Theoretical advances in practical quantum cryptography

Ribeiro, Jérémy

DOI
10.4233/uuid:8f5106ab-9059-4fd6-9448-e4c642362739

Publication date
2020

Document Version
Final published version

Citation (APA)
Ribeiro, J. (2020). *Theoretical advances in practical quantum cryptography*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:8f5106ab-9059-4fd6-9448-e4c642362739

THEORETICAL ADVANCES IN PRACTICAL QUANTUM CRYPTOGRAPHY

THEORETICAL ADVANCES IN PRACTICAL QUANTUM CRYPTOGRAPHY

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus Prof.dr.ir. T.H.J.J. van der Hagen,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op 25 maart 2020 om 15:00 uur

door

Jérémy RIBEIRO

Master of science in Physics,
Univesité Paris-Sud XI, Orsay, France,
geboren te Sainte-Foy-Lès-Lyons, France.

Dit proefschrift is goedgekeurd door de

promotor: prof. dr. S.D.C. Wehner
copromotor: Prof. dr. ir. R. Hanson

Samenstelling promotiecommissie:

Rector Magnificus,	voorzitter
Prof. dr. S.D.C. Wehner,	Technische Universiteit Delft, promotor
Prof. dr. ir. R. Hanson,	Technische Universiteit Delft, copromotor
Onafhankelijke leden:	
Prof. dr. W. Titel	Technische Universiteit Delft
Prof. dr. ir. L.M.K. Vandersypen	Technische Universiteit Delft
Prof. dr. S.O. Fehr,	Universiteit Leiden & CWI Amsterdam
Dr. M. Walter,	Universiteit van Amsterdam

Keywords: quantum, cryptography, two-party cryptography, quantum key distribution, device independence
Printed by: Gildeprint - www.gildeprint.nl
Front & Back: Designed by J. Ribeiro.

ISBN 978-94-6402-160-8

An electronic version of this dissertation is available at
http://repository.tudelft.nl/.

"Philosophy, though unable to tell us with certainty what is the true answer to the doubts which it raises, is able to suggest many possibilities which enlarge our thoughts and free them from the tyranny of custom. Thus, while diminishing our feeling of certainty as to what things are, it greatly increases our knowledge as to what they may be; it removes the somewhat arrogant dogmatism of those who have never travelled into the region of liberating doubt, and it keeps alive our sense of wonder by showing familiar things in an unfamiliar aspect."

– Bertrand Russell. "The Problems of Philosophy."

Curriculum Vitæ

Jérémy Ribeiro

05-07-1992 Born in Sainte-Foy-Lès-Lyons, France.

Education

2003 – 2010	High Scholl Saint Just, Lyon, France
2010 – 2013	Undergraduate in physics Lycée du Parc, Lyon, france Université Paris-Sud, Orsay, France
2013 – 2015	Masters in Condensed Matter Université Paris-Sud, Orsay, France
2015 – 2020	PhD in Quantum Information Delft University of Technology, Delft, The Netherlands *Thesis:* Theoretical advances in practical quantum cryptography *Promotor:* Prof. dr. S.D.C. Wehner

List of Publications

12. **J. Ribeiro**, S. Wehner, *Oblivious-Transfer is harder than Bit-Commitment in realistic Measurement-Device Independent settings*, preprint soon

11. V. Lipinska, **J. Ribeiro**, S. Wehner, *Secure multi-party computation with few qubits*, preprint soon

10. G. Murta, F. Rozpędek, **J. Ribeiro**, D. Elkouss, S. Wehner*Key rates for quantum key distribution protocols with asymmetric noise*, preprint arXiv:2002.07305

9. V. Lipinska, G. Murta, **J. Ribeiro**, S. Wehner, *Verifiable Hybrid Secret Sharing With Few Qubits*, preprint arxiv:1911.09470

8. V. Lipinska, LP Thinh, **J. Ribeiro**, S. Wehner, *Certification of a quantum network functionality.*, prepint arXiv:1910.10004.

7. **J. Ribeiro**, G. Murta, S. Wehner, *Reply to "Comment on 'Fully device-independent conference key agreement'"*, Phys. Rev. A 100, 026302 (2019).

6. G. Murta, SB. van Dam, **J. Ribeiro**, R. Hanson, S. Wehner, *Towards a realization of device-independent quantum key distribution*, Quantum Science and Technology (2019).

5. **J. Ribeiro**, LP. Thinh, J. Kaniewski, J. Helsen, S. Wehner, *Device independence for two-party cryptography and position verification with memoryless devices*, Phys. Rev. 97 (6), 062307 (2018).

4. VC. Vivoli, **J. Ribeiro**, S. Wehner, *High fidelity GHZ generation within nearby nodes*, Physical Review A 100 (3), 032310.

3. F. Rozpędek, K. Goodenough, **J. Ribeiro**, N. Kalb, VC. Vivoli, A. Reiserer, R. Hanson, S. Wehner, D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Science and Technology (2018).

2. **J. Ribeiro**, G. Murta, S. Wehner, *Fully device-independent conference key agreement*, Phys. Rev. 97 (2), 022307 (2018).

1. **J. Ribeiro**, F. Grosshans, *A tight lower bound for the bb84-states quantum-position-verification protocol*, preprint arXiv:1504.07171.

SUMMARY

Most of the mainstream cryptographic protocols that are used today rely on the assumption that the adversary has limited computational power, and that a given set of mathematical problems is hard to solve (on average), *i.e.* that there is no polynomial time algorithm that solves these problems. While these assumptions are reasonable for now they might not be as relevant for long term security. Indeed, all the communication that happens today can be recorded by an adversary who can later – when the technology allows it – break security. There are good reasons to think that technological progress may lead to break the assumptions made today. For example the rapidly increasing computational power of our computer already allows one to break anything that has been encrypted using DES in the 70s and 80s in few days using regular desktop type devices. There is also the constant improvement of the efficiency of the known algorithms that solve a class of problems. Note that, even though the discovery of a polynomial algorithm for a problem we believe to be hard is still possible, much weaker improvements on current algorithms that solve these hard problems, can already be a threat for security.

One of the main goals of quantum cryptography is to make protocols safer. In practice safer means safe for a long period of time. Research in using quantum communication for cryptography has had some big success toward this goal. The best known and mature result is that there exists a quantum protocol called Quantum Key Distribution (QKD), that solves a cryptographic task that cannot be solved without quantum communication.

Despite its potential, quantum cryptography comes with its own challenges. Indeed, beyond all the new infrastructure a quantum network requires in order to run these quantum protocols, the manipulation of quantum systems is very unreliable. Devices that prepare and measure quantum systems are noisy, faulty and in general not very efficient. In order to achieve security in practical implementation, it is important that quantum protocols are designed in a way that their security is tolerant to all these flaws in the devices used. Indeed, it has been proven that these flaws may be exploited by an adversary to bypass the security proofs.

One radical approach to this issue, is to design protocols whose security does not dependent on the behavior of the quantum devices used in the protocol. In particular we can even assume that these devices may behave maliciously. Protocols showing this type of security are said to be device-independent protocols. In the recent years device-independence has successfully been included into security proofs for QKD. However there is very little work in including device-independence in the security proofs of protocol beyond QKD. This it what we propose in this thesis. More specifically, we design protocols for a class of cryptographic tasks called two-party cryptography, or sometimes secure function evaluation. We also improve and extend existing device-independent protocols for QKD.

SAMENVATTING

De meeste gangbare cryptografische protocollen die tegenwoordig worden gebruikt, gaan uit van de veronderstelling dat de kwaadwillende beperkte rekenkracht heeft en dat een bepaald aantal wiskundige problemen bestaat moeilijk (gemiddeld) is op te lossen, *d.w.z.* dat er geen poly-tijd algoritme is dat deze problemen oplost. Terwijl deze veronderstellingen redelijk zijn voor nu zijn ze misschien niet zo relevant voor de beveiliging op lange termijn. Inderdaad, alle communicatie die vandaag plaatsvindt kan worden bevaard door een kwaadwillende die later - wanneer de technologie het toe staat - de beveiliging kan breken. Er zijn goede redenen om te denken dat technologische vooruitgang kan leiden tot het breken van de aannames die vandaag zijn gedaan. Bijvoorbeeld , vanwege de snel toenemende rekenkracht van onze computer kunnen we met behulp van gewone desktopcomputers in enkele dagen alles breken dat in de jaren 70 en 80 is gecodeerd met DES. Er is ook een constante verbetering van de efficiëntie van de bekende algoritmen die een klasse problemen oplossen. Merk op dat, hoewel de ontdekking van een poly-tijd algoritme voor een probleem waarvan wij denken dat het moeilijk is, nog steeds mogelijk is, veel zwakkere verbeteringen op de huidige algoritmen die deze grote problemen oplossen al een bedreiging voor de veiligheid kunnen zijn.

Een van de belangrijkste doelen van kwantumcryptografie is om protocollen veiliger te maken. In de praktijk betekent veiliger voor een lange periode veilig. Onderzoek in het gebruik van kwantumcommunicatie voor cryptografie heeft een groot succes in de richting van dit doel behaald. Het best bekende en het best uitgedachte resultaat is dat er een kwantumprotocol bestaat genaamd Quantum Key Distribution (QKD), dat een cryptografische taak oplost die niet kan worden opgelost zonder kwantumcommunicatie.

Ondanks zijn potentieel heeft kwantumcryptografie zijn eigen uitdagingen. Inderdaad, naast alle nieuwe infrastructuur die een kwantumnetwerk nodig heeft om deze kwantumprotocollen te kunnen gebruiken, is de manipulatie van kwantumsystemen zeer onbetrouwbaar. Apparaten die kwantumsystemen produceren en meten, zijn ruizig, defect en in het algemeen niet zeer efficiënt. Om veiligheid te bereiken in de pratische implementatie is het belangrijk dat kwantumprotocollen zó ontworpen zijn, dat hun veiligheid niet teniet gedaan wordt door fouten in de gebruikte apparaten. Inderdaad, het is bewezen dat deze fouten door een kwaadwillende kunnen worden uitgebuit om de beveiligingsbewijzen te omzeilen.

Een radicale benadering van dit probleem is het ontwerpen van protocollen waarvan de beveiliging niet afhankelijk si van het gedrag van de kwantumapparaten die in het protocol worden gebruikt. We kunnen zelfs aannemen dat deze apparaten zich kwaadaardig gedragen. Er wordt gezegd dat protocollen die dit type beveiliging tonen “device-independent” protocollen zijn. In de afgelopen jaren is “device-independence” met succes opgenomen beveiligingsbewijzen voor QKD. Er is echter heel weinig werk in het toevoegen van “device independence” in de beveiliginsbevewijzen die verder gaan dan QKD

Dit is wat we in dit proefschrift voorstellen. In het bijzonder ontwerpen we protocollen voor een klasse van cryptografische taken genaamd tweepartige cryptografie of soms veilige functie-evaluatie. Wij verbeteren ook bestaande “device-independent” protocollen voor QKD en breiden ze bovendien uit.

CONTENTS

1

INTRODUCTION

1

The intention of garbling messages in a way that makes them understandable by only a very specific person dates back to Antiquity. At the time "cryptographic" schemes were simple and essentially based on substitution of characters as for the famous Caesar cipher. With time these schemes have become more sophisticated. In the years 1800s cryptography started to become more systematically studied even though not yet based on rigorous definitions and security proofs. It is during this period, late 1800s, that the well known principle of cryptography, known as Kerckhoffs's principle, came out. It states, among other things, that security of a scheme should not be based on the secrecy of the scheme but on the secrecy of a "secret key". In the same period, the scheme now known as one-time pad was invented. During World War II, the popularity of mechanical and electromechanical machines allowed to design cipher schemes much more complex than anything done before, like the now very famous Enigma Machine. These schemes, even though very sophisticated were still not based on rigorous definitions and proofs. In the 1940s, Shannon for the first time, defined and rigorously proved that one-time pad gives absolute secrecy, meaning that if one is only given a single cipher, they could never find out what message has been used to produce this cipher. It is in the 70s and 80s that modern cryptography started to use rigorous definitions and security proofs. At the same times the idea of using the unique features of quantum mechanics for cryptography was born [1, 2]. Nowadays, cryptography goes far beyond protecting the content of messages. Among other things, it allows for identification, homomorphic encryption [3], secure multipartite computation [4], secret sharing [5], anonymous communication etc.

The use of quantum communication in cryptography allows to achieve a level of security that cannot be achieved when only using classical communication. The most famous and mature example of this is Quantum Key Distribution [2]. Indeed when using classical communication to implement Key Distribution, one has to assume that an adversary is limited in computational power, and that some mathematical problem is hard to solve. Such assumptions are called computational assumptions. A protocol proven secure under these assumptions is said to be computationally secure. When using Quantum Key Distribution, one can remove these computational assumptions, and the protocol is then said to be statistically secure or information theoretically secure.

However, manipulating and sending quantum information is much harder than manipulating and sending classical information. In practice, this translates into high noise level, high losses etc. Such high level of noise together with the imperfections of the quantum devices used (*e.g.* single photon detectors) can be exploited by a malicious party in order to break implicit assumptions made in the security proofs of the quantum protocols, and thus break their security. For example an adversary can use lasers in order to essentially take (partial) control of the single photon detectors used by the honest parties, and decide which of the detector will click or not [6, 7].

A promising approach to solve this problem consists in trying to design protocols whose security is independent of the inner working of the quantum devices. This way even if the adversary takes control of the quantum devices used by the honest parties, security can be guaranteed. This approach is called device-independence. In this context the quantum devices are modeled as black boxes solely characterized by the probability distribution of their outputs given their inputs. To achieve device-independence, one

somehow needs to test the quality of their devices. In general, this test is performed by using the non-local property of quantum mechanics via the use of Bell's inequality [8, 9]. Indeed if the probability distribution of the inputs and outputs of the devices allows for the violation of Bell's inequality, then the amount by which Bell's inequality is violated can be seen as a constraint the probability distribution has to satisfy [10]. This allows to prove security for several quantum protocols in the DI settings.

1.1. CHALLENGES OF DEVICE-INDEPENDENCE

While device-independence provides strong security guarantees, it is still hard to prove security in this quite generic framework. In particular, device-independent security has only been proven for a handful of protocols, namely protocols implementing Quantum Key Distribution, Randomness Amplification and Randomness Expansion [11–19]. It is still not clear whether this approach can be used for other cryptographic tasks like two-party cryptography. Moreover, device-independent protocols are in general experimentally more demanding than their trusted device counterpart, which makes them challenging to implement in practice. Indeed device-independent protocols in general require a lot more rounds to achieve the same security as their device-dependent counterpart, and in general they tolerate less noise.

In this thesis, we aim at applying this device-independent approach to other cryptographic protocols. We will also improve the efficiency, and benchmark existing device-independent protocols with the intent of easing experimental challenges, and eventually permitting the implementation of these protocols in the near future.

1.2. CHAPTER OVERVIEW

This thesis is divided in 7 chapters. The first two chapters (including this one) are introductory chapters. They provide the reader with essential notation and definitions that will be used throughout the thesis. From chapter 3 to 6 we introduce new protocols and prove their security with diverse degrees of device-independence.

Chapter 2: This chapter is a preliminary chapter which provides the reader with notions of quantum information theory as well as with the cryptographic primitives that we will use in this thesis. The reader will also find in this chapter the notation that will be used across all chapters.

Chapter 3: In this chapter we improve the device-independent security proof provided in [20] for two-party cryptography in the scenario where the devices are assumed to be IID (see IID-Assumption 2.4.2 in Chapter 2). In particular our new proof allows to tolerate a more powerful adversary while using the same amount of resources for the honest party. Moreover we discuss the relation between security of two-party cryptography and the security of an other task called Position Verification.

Chapter 4: In this chapter we propose a new protocol for Conference Key Agreement based on the use of GHZ states. We prove that this protocol is device-independently secure. We compared the key rate achieved by our GHZ-based protocol to the

key rate achieved by protocols based on multiple execution of (bipartite) Device-Independent Quantum Key Distribution, which then only use Bell pairs.

Chapter 5: In this chapter we optimise key rate of the Device-Independent Quantum Key Distribution Protocol (DIQKD) of [11]. We discuss the potential of different platforms on which DIQKD could be implemented, by computing the relevant parameters that have been achieved on each of the platforms. By doing so we assess how far each platform is from an actual implementation of DIQKD.

Chapter 6: In this chapter we present the first protocols that are secure in the measurement-device-independent model. This is a model that is less general than the regular device-independence model. In this model, not all quantum devices are modeled as black boxes, only the measurement-devices are. On the other hand this model allows to have better efficiency. Moreover we discuss how the security of certain protocol can be affected by some types of imperfection of the quantum state sources.

Chapter 7: This chapter provides with the general conclusion of the thesis together with an outlook for future research.

REFERENCES

[1] S. Wiesner, *Conjugate coding,* ACM Sigact News **15**, 78 (1983).

[2] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560, Part 1**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}.

[3] C. Gentry et al., Stoc, Vol. 9 (2009) pp. 169–178.

[4] D. Chaum, C. Crépeau, and I. Damgard, Proceedings of the twentieth annual ACM symposium on Theory of computing (1988) pp. 11–19.

[5] A. Shamir, *How to share a secret,* Communications of the ACM **22**, 612 (1979).

[6] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems,* Phys. Rev. A **74**, 022313 (2006).

[7] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, *Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing,* Phys. Rev. A **91**, 032326 (2015).

[8] J. S. Bell, *On the eintein podolsky rosen paradox,* Physics 1, 195-200 (1964).

[9] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Phys. Rev. Lett. **23**, 880 (1969).

[10] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality,* Rev. Mod. Phys. **86**, 419 (2014).

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation,* Nature Communications **9**, 459 (2018).

[12] U. Vazirani and T. Vidick, *Fully device-independent quantum key distribution,* Phys. Rev. Lett. **113**, 140501 (2014).

[13] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random numbers certified by bell's theorem,* Nature **464**, 1021 (2010).

[14] J. Barrett, R. Colbeck, and A. Kent, *Unconditionally secure device-independent quantum key distribution with only two devices,* Phys. Rev. A **86**, 062326 (2012).

[15] J. Bouda, M. Pawłowski, M. Pivoluska, and M. Plesch, *Device-independent randomness extraction from an arbitrarily weak min-entropy source,* Phys. Rev. A **90**, 032313 (2014).

[16] M. Kessler and R. Arnon-Friedman, *Device-independent randomness amplification and privatization,* arXiv preprint arXiv:1705.04148 (2017).

[17] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, *Full randomness from arbitrarily deterministic events,* Nature Communications **4** (2013), 10.1038/ncomms3654.

[18] C. A. Miller and Y. Shi, *Universal security for randomness expansion from the spot-checking protocol,* SIAM Journal on Computing **46**, 1304 (2017).

[19] R. Colbeck and R. Renner, *Free randomness can be amplified,* Nature Physics **8**, 450 (2012).

[20] J. Kaniewski and S. Wehner, *Device-independent two-party cryptography secure against sequential attacks,* New Journal of Physics **18**, 055004 (2016).

2

PRELIMINARIES

"The language of science is the language of probability, and not of p-values."

– Luis Pericchi

In this chapter we introduce quantum information formalism, the common notation used across all the chapters, as well as the main cryptographic primitives and concepts of this thesis.

NOTATION

In this thesis we will write A_1^n to denote the string $A_1, \ldots, A_n$. We will use $[n]$ as a shorthand notation for the set $\{1, \ldots, n\}$. We denote by "log" the logarithm to base 2 and by "ln" the natural logarithm.

2

2.1. DISCRETE PROBABILITY THEORY

A common ground to all areas of information theory is the use of probabilities. In this section we briefly introduce (discrete) probability theory. We point the reader to [1] for more details on probability theory.

2.1.1. DISCRETE PROBABILITY SPACES

Intuitively, in an "experimental situation", probabilities give a measure of certainty over all the different possible outcomes of the experiment we consider. Note that here, the "experiment" does not have to be an actual concrete physical realisation of an experiment, but may very well be a thought experiment *i.e.* an hypothetical situation. A simple example is a situation in which someone is throwing a dice, in which case the set of possible outcomes is simply the set of faces (or corresponding numbers) of the dice. This set is usually referred as the sample space and is often denoted Ω. In a given experiment one may ask what the probability is that the outcome satisfies a certain condition. For the example of the dice, one may ask what the probability is that the number on the face of the dice is odd, or that it is smaller than 3. Given a certain condition, the set of outcomes satisfying this condition must obviously be a subset of sample space Ω. Each condition will define such a subset of the sample space, so that we can identify the set of all possible questions to a set of subset of Ω. In other words, the set of all questions one can ask about the outcomes is formalized by a set $\mathscr{F} \subseteq 2^\Omega$, where 2^Ω denotes the power set of Ω, *i.e.* the set of subset of Ω. $\mathscr{F}$ is called a σ-algebra. The measure of probability will assign to each of these questions a probability, which is a number in $[0,1]$. As such, a probability measure is a function $\mu : \mathscr{F} \mapsto [0,1]$.

Definition 2.1.1 (Probability space)**.** *We call the triplet $(\Omega, \mathscr{F}, \mu)$ a probability space, if $\Omega, \mathscr{F}$, and μ satisfy the following:*

- *Ω is a set.*
- *$\mathscr{F}$ (the σ-algebra) is a subset of 2^Ω such that:*
  1. *$\Omega \in \mathscr{F}$.*
     This condition simply says that one should be able to ask the trivial question: "What is the probability that the outcome is one of all the possible outcomes?"
  2. *$\forall A \in 2^\Omega$, $(A \in \mathscr{F}) \Rightarrow (A^c \in \mathscr{F})$, where $A^c := \Omega \setminus A$ is the complement of A.*
     This condition can be read as: for every condition A for which one can ask what is the probability that A is satisfied, one should also be able to ask what is the probability that A is not satisfied.

3. *For every countable family of sets* $\left(A_i\right)_{i=1}^{\infty}$ *of* 2^{Ω}, $(\forall i, A_i \in \mathscr{F}) \Rightarrow (\bigcup_{i=1}^{\infty} A_i \in \mathscr{F})$. *This condition states that one can combine different conditions into a single one.*

The elements of $\mathscr{F}$ *are called events.*

- $\mu : \mathscr{F} \mapsto [0,1]$ *is a function, called the probability measure, that satisfies the following.*

  1. $\mu(\Omega)$=*1.*
     This condition is very natural if one wants Ω *to be the set of all outcomes. This conditions can be read as: the probability that the outcome is one of the possible ones is* 1.
  2. *For every countable family of disjoint events* $\left(A_i\right)_{i=1}^{\infty}$, $\mu\left(\bigcup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu\left(A_i\right)$. *This condition generalises the intuition that we can decompose an event into its partition.*

From this definition one can deduce the following properties.

Property 2.1.2.

- *For every countable family* $\left(A_i\right)_{i=1}^{\infty}$ *of sets in* 2^{Ω}, $(\forall i \ A_i \in \mathscr{F}) \Rightarrow (\bigcap_{i=1}^{\infty} A_i \in \mathscr{F})$. *This follows from the fact that* $\cap_i A_i = \left(\cup_i A_i^c\right)^c$.
- *For every event* A, $\mu(A^c) = 1 - \mu(A)$. *This follows from* $1 = \mu(\Omega) = \mu(A \cup A^c) = \mu(A) + \mu(A^c)$.

In this thesis we will mostly use finite or sometimes countable probability theory. This means that we will consider Ω to be a finite (countable) set. For finite (discrete) probability theory it is common to take $\mathscr{F} = 2^{\Omega}$. This combined with the finite (countable) size of Ω simplifies the situation. Indeed we can now, for every event $A \in 2^{\Omega}$, define its probability as $\mu(A) = \sum_{x \in A} \mu(\{x\})$. This means that in the case of finite (countable) sample space one only needs to define the probability measure for every singleton $\{x\} \in 2^{\Omega}$. In this case we will often use p_x to denote $\mu(\{x\})$, $x \in \Omega$, and the tuple $(p_x)_{x \in \Omega}$ is called a probability distribution. Similarly, we will often use $\Pr(A)$ to denote $\mu(A)$, where $A \in 2^{\Omega}$ is an event.

2.1.2. RANDOM VARIABLES

Intuitively, a random variable transforms outcomes into other outcomes. For example let us consider a gambling game in which one has to pay 2€ to participate. In the game, a dice is thrown. The player wins 6€ if and only if the outcome is larger or equal than 5. In this game the sample space can be considered as the the set of faces of the dice. But these faces are then translated into a win or a loss. This translation is formalised by the random variable $X : \Omega \mapsto W$, which is a function from the sample space $\Omega := \{\text{face1}, \text{face2}, \text{face3}, \text{face4}, \text{face5}, \text{face6}\}$, into the "gain set" $W := \{-2, 6\}$.

Definition 2.1.3. *A random variable* $X : \Omega \mapsto E$ *is a measurable function from a probability space* $(\Omega, \mathscr{F}, \mu)$ *into a measurable set* $(E, \mathscr{E})$, *where* $\mathscr{E} \subseteq 2^E$ *denotes a* $\sigma-$*algebra on* E. *We will very often take* E *to be a finite (countable) subset of* $\mathbb{R}$.

Using the same notation as above, we can define the probability distribution of the random variable X as follows. If $B \in \mathscr{E}$ then the probability $\Pr(X \in B)$ that $X \in B$ is given by $\mu(X^{-1}(B))$, where $X^{-1}(B) := \{\omega \in \Omega : X(\omega) \in B\}$ is the preimage of B under X. Since X is measurable we have that $X^{-1}(B) \in \mathscr{F}$ and therefore $\mu(X^{-1}(B))$ is well defined. If $x \in E$, we denote $\Pr(X = x)$ to be $\Pr(X \in \{x\})$. Of course, this is only possible if $\{x\} \in \mathscr{E}$. But since in this thesis we will exclusively consider the case where E is finite (or countable), we will choose $\mathscr{E} = 2^E$, and then we always have $\{x\} \in \mathscr{E}$.

Remark 2.1.4. *When the σ-algebras considered ($\mathscr{F}$ and $\mathscr{E}$) are the power set of there respective set (Ω and E), every function is measurable. Since, in this thesis, we focus on finite (or countable) sets, with their σ-algebra being their power set, all the random variables we will define, will automatically be measurable. For this reason we will omit to mention the probability space on which a random variable is defined.*

When working with a random variable it is often useful to define the conditional probability.

Definition 2.1.5. *Let X be a random variable, and let A be an event such that $\Pr(A) > 0$. Then for any x in the codomain of X, the probability of $X = x$ conditioned on A is defined as*

$$\Pr(X = x|A) = \frac{\Pr(X^{-1}(x) \cap A)}{\Pr(A)}. \tag{2.1}$$

When we consider a random variable taking value in a finite (or countable) subset of the real numbers, we will define its expectation value as follows.

Definition 2.1.6. *Let X be a random variable taking value in the finite (or countable) set $S \subset \mathbb{R}$, then the expectation value of X, denoted $\mathbb{E}(X)$, is defined as,*

$$\mathbb{E}(X) := \sum_{x \in S} x \cdot \Pr(X = x), \tag{2.2}$$

where $\Pr(X = x) := \sum_y \Pr(X = x, Y = y)$.

Very often in this thesis we will consider a set of random variables and say that they are independent. Intuitively, if we consider X and Y being two random variables, then we would like to say that they are independent if for any value y that Y takes, the (conditional) probability of $X = x$ is always the same, *i.e.* independent of the values taken by Y:

$$\forall x, y,\ \Pr(X = x|Y = y) = \Pr(X = x).$$

To avoid problems with the definition of the conditional probability when $\Pr(Y = y) = 0$, we, in general, prefer to rewrite the above inequality as,

$$\forall x, y,\ \Pr(X = x, Y = y) = \Pr(X = x)\Pr(Y = y).$$

This generalizes to n variables as follows.

Definition 2.1.7. *Let us consider $X_1, \ldots, X_n$ be n random variables taking value in some set E. We say that these random variables are independent if $\forall (x_1, \ldots, x_n) \in E^n$,*

$$\Pr(X_1 = x_1, \ldots, X_n = x_n) = \prod_{i=1}^{n} \Pr(X_i = x_i).$$

HOEFFDING INEQUALITY

The Hoeffding inequality is a very useful concentration bound that will be used many times throughout this thesis, and which quantifies how far from its expectation value the sum of independent and bounded random variables can be.

Theorem 2.1.8 ([2])**.** *Let $X_1,\dots,X_n$ to be n discrete independent real random variables such that for any i, $a_i \leq X_i \leq b_i$. Let $\epsilon > 0$, and $X := \sum_i X_i$, then,*

$$\Pr(X - \mathbb{E}(X) \geq n\epsilon) \leq \exp\left(-\frac{2n^2\epsilon^2}{\sum_i (b_i - a_i)^2}\right). \tag{2.3}$$

2.2. BASICS OF QUANTUM INFORMATION THEORY

In this section we will introduce the formalism and notation of quantum information theory that will be used throughout this thesis. In particular, we will only focus on finite dimensional quantum information theory. The content of this section is based on the introductory text book Nielsen and Chuang's *Quantum Computation and Quantum Information* [3], as well as on [4] and [5]. The reader already familiar with quantum information theory may skip this section.

2.2.1. HILBERT SPACES, AND LINEAR OPERATORS

HILBERT SPACES

Let $\mathscr{H}$ be a finite-dimensional vector space over the complex numbers equipped with an inner product $\langle\cdot,\cdot\rangle : \mathscr{H} \times \mathscr{H} \mapsto \mathbb{C}$. Using Dirac's notation, the vectors of $\mathscr{H}$ will be written as "kets". For example, we will write $|v\rangle \in \mathscr{H}$. Let $\mathscr{H}^*$ be the dual space of $\mathscr{H}$, *i.e.* the space of linear forms (we also say linear functionals) on $\mathscr{H}$. Using Dirac's notation, a vector of the dual is denoted with a "bra": $\langle v| \in \mathscr{H}^*$. The action of a linear form $\langle v| \in \mathscr{H}^*$ onto a vector $|w\rangle \in \mathscr{H}$ is denoted $\langle v|w\rangle$. For every vector $|x\rangle \in \mathscr{H}$, its dual $\langle x| \in \mathscr{H}^*$ is defined through the inner product as being the unique linear form such that,

$$\forall |v\rangle \in \mathscr{H},\ \langle x|v\rangle = \big\langle |x\rangle, |v\rangle \big\rangle.$$

As a consequence, from now on, the inner product of vectors $|x\rangle$ and $|y\rangle$ will be denoted as $\langle x|y\rangle$.

The inner product of the space $\mathscr{H}$ has to satisfy the following three conditions:

Conjugate Symmetry: $\forall |x\rangle, |y\rangle \in \mathscr{H}$, $\langle x|y\rangle = \big(\langle y|x\rangle\big)^*$ where here $\forall z \in \mathbb{C}$, z^* denotes for the complex conjugate of z.

Right Linearity: $\forall \alpha, \beta \in \mathbb{C}$ and $\forall |x\rangle, |y\rangle, |z\rangle \in \mathscr{H}$, $\langle z|\big(\alpha|x\rangle + \beta|y\rangle\big) = \alpha\langle z|x\rangle + \beta\langle z|y\rangle$.

Definite Positiveness: $\forall |x\rangle \in \mathscr{H}$, $\langle x|x\rangle \geq 0$ and $\langle x|x\rangle = 0 \Rightarrow |x\rangle = 0$, where 0 is the 0 vector of $\mathscr{H}$.

BASES OF A HILBERT SPACE

A finite family of vectors $\{|v_1\rangle,\dots,|v_n\rangle\}$ is said to be linearly independent if and only if $\forall \alpha_1,\dots,\alpha_n \in \mathbb{C}$,

$$\alpha_1|v_1\rangle + \dots + \alpha_n|v_n\rangle = 0 \ \Rightarrow\ \alpha_1 = \dots = \alpha_n = 0.$$

The span of a family of vectors is defined as,

$$\mathrm{Span}(|v_1\rangle,\ldots,|v_n\rangle) := \Big\{\sum_i \alpha_i |v_i\rangle : \forall i, \alpha_i \in \mathbb{C}\Big\}.$$

2

In a finite-dimensional Hilbert space, the cardinal of a linearly independent family of vectors assumes a maximum value called the dimension of the space $\dim(\mathscr{H})$.

A linearly independent family of vectors that has a cardinal equal to $\dim(\mathscr{H})$ is called a basis of the space. A basis spans the full space $\mathscr{H}$. Moreover, a basis $\{|v_1\rangle,\ldots,|v_{\dim(\mathscr{H})}\rangle\}$ is called orthonormal if and only if $\forall i,j \in \{1,\ldots,\dim(\mathscr{H})\}$,

$$\langle v_i | v_j\rangle = \delta_{ij},$$

where δ_{ij} is the Kronecker symbol.

LINEAR OPERATOR ON HILBERT SPACES

A linear operator L from $\mathscr{H}$ to $\mathscr{H}'$ is a map $L : \mathscr{H} \mapsto \mathscr{H}'$ such that the linearity condition is satisfied: $\forall \alpha,\beta \in \mathbb{C}, \forall |v_1\rangle, |v_2\rangle \in \mathscr{H}$,

$$L\big(\alpha|v_1\rangle + \beta|v_2\rangle\big) = \alpha L\big(|v_1\rangle\big) + \beta L\big(|v_2\rangle\big).$$

The space of linear operators from $\mathscr{H}$ to $\mathscr{H}'$ is denoted $\mathscr{L}(\mathscr{H},\mathscr{H}')$.

The linearity property, together with the fact that a basis spans the whole space, allows one to fully characterize a linear operator L by its action on a basis. This means that by choosing bases for spaces $\mathscr{H}$ and $\mathscr{H}'$, a linear operator L can be represented by a matrix (written in these bases). Let us denote these bases by $\{|e_i\rangle\}$ and $\{|e_j\rangle\}$. If one chooses these bases to be orthonormal, the matrix entry $[L]_{ij}$ of the matrix representing operator L in the bases $\{|e_i\rangle\}$ and $\{|e_j\rangle\}$ is given by $[L]_{ij} = \langle e_i|L|e_j\rangle$.

For every operator $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$, the adjoint operator $L^\dagger \in \mathscr{L}(\mathscr{H}',\mathscr{H})$ is defined such that $\forall |v_1\rangle \in \mathscr{H}$ and $\forall |v_2\rangle \in \mathscr{H}'$

$$\big(\langle v_1|L^\dagger|v_2\rangle\big)^* = \langle v_2|L|v_1\rangle.$$

We define the kernel of an operator $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$ as

$$\mathrm{Ker}(L) := \{|v\rangle \in \mathscr{H} : L|v\rangle = 0\}.$$

The image of L is

$$\mathrm{Im}(L) := \{|v\rangle \in \mathscr{H}' : \exists |v'\rangle \in \mathscr{H},\ L|v'\rangle = |v\rangle\}.$$

The support of L is the subspace of $\mathscr{H}$ orthogonal to $\mathrm{Ker}(L)$. The rank $\mathrm{rank}(L)$ is the dimension of $\mathrm{Im}(L)$.

In the following, we will use $\mathscr{L}(\mathscr{H})$ as a shorthand notation for $\mathscr{L}(\mathscr{H},\mathscr{H})$. A projection is an operator P in $\mathscr{L}(\mathscr{H},\mathscr{H})$ such that $P^2 = P$. A projection P is said to be an orthogonal projection if $\mathrm{Im}(P) = \mathrm{Ker}(P)^\perp$, where $A^\perp$ denotes the subspace orthogonal to subspace $A \subseteq \mathscr{H}$.

We denote by $\mathbb{1}_{\mathscr{H}}$ the identity operator on the space $\mathscr{H}$. Let $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$ be a linear operator. If there exists a linear operator $M \in \mathscr{L}(\mathscr{H}',\mathscr{H})$ such that $ML = \mathbb{1}_{\mathscr{H}}$ and $LM = \mathbb{1}_{\mathscr{H}'}$ then M is the unique operator satisfying these two conditions, and L is said

to be invertible. M will be called the inverse of L and will be denoted L^{-1}. Furthermore, if L^{-1} exists, it must be the case that $\dim(\mathscr{H}) = \dim(\mathscr{H}')$. The generalized inverse of $L \in \mathscr{L}(\mathscr{H}, \mathscr{H}')$ is the unique operator, also denoted L^{-1}, such that $L^{-1}L = P_L$, where P_L denotes the projection on the support of L.

An eigenvalue of an operator $L \in \mathscr{L}(\mathscr{H})$ is a number $\lambda \in \mathbb{C}$ (if it exists) such that $\exists |v_\lambda\rangle \in \mathscr{H}$, $|v_\lambda\rangle \neq 0$ for which $L|v_\lambda\rangle = \lambda|v_\lambda\rangle$. The vector $|v_\lambda\rangle$ is called an eigenvector associated to λ.

The trace is the linear form $\mathrm{tr} : \mathscr{L}(\mathscr{H}) \mapsto \mathbb{C}$, such that

$$\forall L, M \in \mathscr{H},\ \mathrm{tr}(LM) = \mathrm{tr}(ML) \text{ and } \mathrm{tr}(\mathbb{1}) = \dim(\mathscr{H}).$$

The trace can be written in an orthonormal basis $\{|e\rangle\}$ as $\mathrm{tr}(L) = \sum_{|e\rangle} \langle e|L|e\rangle$. Note that this is independent of the choice of the basis $\{|e\rangle\}$.

HERMITIAN, POSITIVE AND DENSITY OPERATORS

A linear operator $H \in \mathscr{L}(\mathscr{H})$ such that $H = H^\dagger$ is called a hermitian operator or a self-adjoint operator. The set of self-adjoint operators will be denoted by $\mathscr{S}_a(\mathscr{H})$. A self-adjoint operator H is orthodiagonializable, meaning that there exists an orthonormal basis in which the matrix of H is diagonal. Equivalently, this means that a matrix representing H can be diagonalized by a unitary transformation. The eigenvalues of a self-adjoint operator are real numbers.

The set of positive semi-definite operators, denoted $\mathscr{P}(\mathscr{H})$, is the set of self-ajoint operators that have non-negative eigenvalues. We will often write $L \geq 0$ for $L \in \mathscr{P}(\mathscr{H})$, and $L \geq M$ for $L - M \in \mathscr{P}(\mathscr{H})$.

The set of density operators on $\mathscr{H}$, denoted by $\mathscr{S}(\mathscr{H})$, is the set of positive operators of trace equal to 1. The set of non-normalized density operators, denoted $\mathscr{S}_\bullet(\mathscr{H})$, is the set of positive semi-definite operators of trace smaller or equal to 1.

Definition 2.2.1. *Let f be an analytical function from $I \subseteq \mathbb{C}$ to $\mathbb{C}$, and let $N \in \mathscr{L}(\mathscr{H})$ be a diagolizable operator whose eigenvalues $\{z_i\}_i$ belong to the set I. Then we define $f(N)$ as the diagonalizable operator that has the same eigenvectors as N, and whose eigenvalues are $\{f(z_i)\}_i$.*

SINGULAR VALUE DECOMPOSITION

For any operator $L \in \mathscr{L}(\mathscr{H}, \mathscr{H}')$ there exists an orthonormal basis $\{|e_i\rangle\}$ of $\mathscr{H}$ and an orthonormal basis $\{|e'_i\rangle\}$ for $\mathscr{H}'$, such that

$$L = \sum_i s_i |e'_i\rangle\langle e_i|, \qquad s_1 \geq \ldots \geq s_{\mathrm{rank(L)}} > 0,$$

where $s_1, \ldots, s_{\mathrm{rank(L)}}$ are called the singular values of L.

The singular values, are also the non-zero eigenvalues of $|L| := \sqrt{L^\dagger L}$, where for any operator $M \geq 0$, $\sqrt{M}$ denotes the unique operator $N \geq 0$, such that $N^2 = M$.

UNITARIES AND ISOMETRIES

A unitary operator is a bijective linear map $U \in \mathscr{L}(\mathscr{H}, \mathscr{H}')$ that preserves the inner product:

$$\forall |v_1\rangle, |v_2\rangle \in \mathscr{H},\ \langle v_1|v_2\rangle = \langle v_1|U^\dagger U|v_2\rangle.$$

This condition is equivalent to $U^\dagger U = \mathbb{1}_{\mathscr{H}}$. Since U is bijective and linear $\dim(\mathscr{H}) = \dim(\mathscr{H}')$, and we also get that $UU^\dagger = \mathbb{1}_{\mathscr{H}'}$. The set of unitary operators acting from space $\mathscr{H}$ to $\mathscr{H}'$ will be denoted as $\mathscr{U}(\mathscr{H}, \mathscr{H}')$, and if $\mathscr{H} = \mathscr{H}'$ we will denote it as $\mathscr{U}(\mathscr{H})$. If a linear operator $V \in \mathscr{L}(\mathscr{H}, \mathscr{H}')$, is not bijective but still preserves the inner product, we say that V is an isometry.

TENSOR PRODUCT OF SPACES

Tensor product of spaces will be used to describe composite systems (see Section 2.2.2). Here, we define the tensor product of two Hilbert spaces in the finite dimensional case.

Let $\mathscr{H}_1$ and $\mathscr{H}_2$ be two finite dimensional Hilbert spaces, and let $\{|e_1^i\rangle\}$ and $\{|e_2^j\rangle\}$ be orthonormal bases of $\mathscr{H}_1$ and $\mathscr{H}_2$ respectively. The tensor product space $\mathscr{H}_1 \otimes \mathscr{H}_2$ can be defined as the space that has for orthonormal basis, the set

$$\mathfrak{B}_{1,2} := \{|e_1^i\rangle\} \times \{|e_2^j\rangle\}, \tag{2.4}$$

where $\{|e_1^i\rangle\} \times \{|e_2^j\rangle\}$ denotes the direct product of the finite set $\{|e_1^i\rangle\}$ and $\{|e_2^j\rangle\}$. The elements of $\mathfrak{B}_{1,2}$ are in general denoted by $|e_1^i\rangle \otimes |e_2^j\rangle$, or sometimes $|e_1^i\rangle|e_2^j\rangle$, or even $|e_1^i, e_2^j\rangle$. Moreover we will impose a "bilinearity constraint" on the space $\mathscr{H}_1 \otimes \mathscr{H}_2$, namely we require that for any $|v_1\rangle, |v_1'\rangle \in \mathscr{H}_1$, $|v_2\rangle, |v_2'\rangle \in \mathscr{H}_2$, and $\alpha \in \mathbb{C}$,

- $\alpha(|v_1\rangle \otimes |v_2\rangle) = (\alpha|v_1\rangle) \otimes |v_2\rangle = |v_1\rangle \otimes (\alpha|v_2\rangle)$
- $|v_1\rangle \otimes |v_2\rangle + |v_1\rangle \otimes |v_2'\rangle = |v_1\rangle \otimes (|v_2\rangle + |v_2'\rangle)$ and
  $|v_1\rangle \otimes |v_2\rangle + |v_1'\rangle \otimes |v_2\rangle = (|v_1\rangle + |v_1'\rangle) \otimes |v_2\rangle$.

By definition, the finite set $\mathfrak{B}_{1,2}$ is an orthonormal basis of $\mathscr{H}_1 \otimes \mathscr{H}_2$, and $\mathscr{H}_1 \otimes \mathscr{H}_2 = \mathrm{Span}(\mathfrak{B}_{1,2})$. The dimension of $\mathscr{H}_1 \otimes \mathscr{H}_2$ satisfies $\dim(\mathscr{H}_1 \otimes \mathscr{H}_2) = \dim(\mathscr{H}_1) \times \dim(\mathscr{H}_2)$.

Note that this definition automatically defines the inner product of the space $\mathscr{H}_1 \otimes \mathscr{H}_2$ in such a way that $\big\langle |v_1\rangle \otimes |v_2\rangle, |v_1'\rangle \otimes |v_2'\rangle \big\rangle = \langle v_1|v_1'\rangle\langle v_2|v_2'\rangle$.

We will often write $A^{\otimes n}$ to denote $\underbrace{A \otimes \ldots \otimes A}_{n \text{ times}}$. Here A can be an operator, a vector a Hilbert space etc.

2.2.2. QUANTUM SYSTEMS AND QUANTUM STATES

In this section we briefly describe what we call a quantum system and a quantum state, and how this relates to the mathematical formalism we have introduced in the previous sections. In this thesis we only consider finite dimensional systems.

Quantum mechanics being a physical theory, talks about real physical systems like electrons or photons. However, in this manuscript, we will abstract the notion of physical system into an abstract object that only inherits the degrees of freedom of the true

physical system. The number of degrees of freedom will be called dimension of the system.[1]

Quantum systems, also called quantum registers, will be denoted by capital letters $A, B, \ldots$. We will often denote $|A|$ for $\log\dim(A)$, where A is an arbitrary quantum or classical system. In particular $|A|$ tells us how many qubits are needed to encode all the information of a quantum system of dimension $\dim(A)$.

Postulate 2.2.2. *A quantum system A of dimension $\dim(A)$ will be modeled by a Hilbert space $\mathscr{H}_A$ of dimension $\dim\mathscr{H}_A = \dim(A)$. The quantum state of system A will be modeled by a density operator ρ_A acting on $\mathscr{H}_A$.*

Intuitively the state should represent everything that can be known about the system. We will usually denote quantum systems by Greek letters $\rho, \sigma, \tau, \ldots$.

When one considers two systems A and B, the composite system AB will be modeled by the tensor space $\mathscr{H}_{AB} := \mathscr{H}_A \otimes \mathscr{H}_B$, and the joint state will be a density operator $\rho_{AB} \in \mathscr{S}(\mathscr{H}_{AB})$.

A state is called pure when it cannot be written as a convex combination of other states. A pure state has rank 1. In this case, there exists a unit vector (unique up to a phase factor) $|\Psi\rangle \in \mathscr{H}$, such that the state $\rho = |\Psi\rangle\langle\Psi|$. The state ρ can then be represented by the corresponding vector $|\Psi\rangle \in \mathscr{H}$.

The set of states, or equivalently the set of density operators, is a convex set, meaning that any convex combination of states is a state. If ρ_A and σ_A are states of a system A, then $p\rho_A + (1-p)\sigma_A$ is also a valid state of A for $p \in [0,1]$.

A state, being a positive semi-definite operator of trace one, can be written in an orthonormal basis $\{|\Psi_i\rangle\}$ (of the underlying space $\mathscr{H}$) as,

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|,$$

where (p_i) are the eigenvalues of ρ, and form a probability distribution. This means that any state can be interpreted as a probability mixture of a set of pure orthogonal states $|\Psi_i\rangle\langle\Psi_i|$.

For a classical (non-quantum) system X, all states of X will be diagonal in a fixed orthonormal basis. They will differ only by their eigenvalues. For example let $\{|x\rangle\}_{x\in\chi}$ be the fixed basis in which the classical states are written. Then a classical state on X can be $\rho_X = \sum_x p_x |x\rangle\langle x|$, and an other one can be $\rho'_x = \sum_x p'_x |x\rangle\langle x|$.

We can now consider a composite system XA in which X is classical and A is quantum, a state of such a system is of the form,

$$\rho_{XA} = \sum_i p_x \, |x\rangle\langle x|_X \otimes \sigma_{A|x},$$

where $\{|x\rangle\}_x$ is the basis associated to the classical system X, and $\{\sigma_{A|x}\}_x$ is a finite set of quantum states on A. These states are called classical-quantum states, or CQ-states or even cq-states.

[1] The dimension of a quantum system can be seen as the maximal number of distinct symbols one can (unambiguously) encode in the system.

In the case when we consider several classical systems, X associated to a basis $\{|x\rangle \in \mathscr{H}_X\}$ and Y associated with a basis $\{|y\rangle \in \mathscr{H}_Y\}$, the state of the composite system will be diagonal in the product basis $\{|x\rangle \otimes |y\rangle\}$, namely,

$$\rho_{XY} = \sum_{xy} p_{xy} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y.$$

SEPARABILITY AND ENTANGLEMENT

Let AB be composite system comprised of subsystem A and subsystem B. Let ρ_{AB} be the state of system AB. The state is said to be separable across A and B if it can be written as,

$$\rho_{AB} = \sum_{ij} p_{ij}\, \sigma_{A|i} \otimes \sigma_{B|j}, \tag{2.5}$$

where $(p_{ij})_{ij}$ is a probability distribution over a finite set, and $\sigma_{A|i}$ is a density operator acting on $\mathscr{H}_A$ and $\sigma_{B|j}$ is a density operator acting on $\mathscr{H}_B$. A state that is not separable across A and B is said to be entangled across A and B. Note that classical states, and CQ-states are always separable.

A separable state $\rho_{AB} \in \mathscr{S}(\mathscr{H}_{AB})$ of the form $\rho_{AB} = \sigma_A \otimes \sigma'_B$ is called a product state. Moreover a state on $\rho_{A_1^n} \in \mathscr{S}(\mathscr{H}_A^{\otimes n})$ is said to be independent and identically distributed (IID) when $\rho_{A_1^n} = \rho_A^{\otimes n}$.

SCHMIDT DECOMPOSITION

Every pure state $|\Psi\rangle_{AB} \in \mathscr{H}_A \otimes \mathscr{H}_B$ of a composite system AB can be decomposed as follows,

$$|\Psi\rangle_{AB} = \sum_i \sqrt{\lambda_i}\, |e_i\rangle_A \otimes |e'_i\rangle_B, \tag{2.6}$$

where $\{|e_i\rangle\}$ is a basis of $\mathscr{H}_A$ and $\{|e'_i\rangle\}$ is a basis of $\mathscr{H}_B$, and where $\sum_i \lambda_i = 1$. Such a state is entangled if and only if the Schmidt decomposition contains more than one term.

FROM MULTIPLE SUBSYSTEMS TO ONE SUBSYSTEM

Let ρ_{AB} be the joint state on composite system AB. Let us say that we are now only interested in system A. In particular, we would like to find a way to transform ρ_{AB} into a state that only describes A. To do so one only has to compute the partial trace as follows. Let $\{|e_i\rangle\}$ be a basis of space $\mathscr{H}_B$, then the marginal state on A will be,

$$\rho_A := \mathrm{tr}_B(\rho_{AB}) := \sum_i \mathbb{1}_A \otimes \langle e_i|_B\, \rho_{AB}\, \mathbb{1}_A \otimes |e_i\rangle_B. \tag{2.7}$$

This definition will be justified in the section 2.2.3, when we will introduce measurements.

EXTENSIONS OF STATES

Let A be a system, and let ρ_A be a state of A. If there exists another system B such that the joint state ρ'_{AB} of AB satisfies,

$$\rho_A = \mathrm{tr}_B(\rho'_{AB}), \tag{2.8}$$

then the state ρ'_{AB} is called an extension of ρ_A.

Note that such a system B always exists. Indeed, let B be a system of the same dimension as A, and let $\{|e'_i\rangle_B\}$ be a basis of space $\mathscr{H}_B$. Let $\{|e_j\rangle_A\}$ be a basis in which ρ_A is diagonal *i.e.* $\rho_A = \sum_i p_i |e_i\rangle\langle e_i|_A$. Consider the following pure state on AB,

$$|\Psi\rangle_{AB} = \sum_i \sqrt{p_i}\, |e_i\rangle_A \otimes |e'_i\rangle_B.$$

One can check that,

$$\rho_A = \mathrm{tr}_B(|\Psi\rangle\langle\Psi|_{AB}),$$

and therefore $|\Psi\rangle\langle\Psi|_{AB}$ is an extension of ρ_A. Moreover the above shows that a state always has an extension that is pure, in which case the extension $|\Psi\rangle\langle\Psi|_{AB}$ is called a purification of ρ_A, and the system B is called the purifying system.

2.2.3. EVOLUTION OF QUANTUM SYSTEMS AND QUANTUM MEASUREMENTS

If one accepts Postulate 2.2.2 about states being described as density operators, one has to describe evolution of such states as maps that transform any density operator acting in some space $\mathscr{H}$ into a density operator acting on some, maybe different, space $\mathscr{H}'$. In particular if $\mathscr{M} : \mathscr{L}(\mathscr{H}) \mapsto \mathscr{L}(\mathscr{H}')$ is such a map, we require that for any state ρ,

$$\mathscr{M}(\rho) \geq 0 \text{ and } \mathrm{tr}\big(\mathscr{M}(\rho)\big) = 1. \tag{2.9}$$

In fact the above should be true, even if $\mathscr{M}(\cdot)$ only act on a subsystem of a larger system, namely, if $\mathscr{M} : \mathscr{L}(\mathscr{H}) \mapsto \mathscr{L}(\mathscr{H}')$, then for any density operator $\rho \in \mathscr{S}(\mathscr{H} \otimes \mathscr{H}'')$ we should have, $\mathscr{M}(\rho) \in \mathscr{L}(\mathscr{H}' \otimes \mathscr{H}'')$ such that eq. (2.9) holds.

Moreover, we have seen in the previous section that a state can be seen as a probabilistic mixture of pure states that form a basis. This gives us a probabilistic interpretation of a state, and it is very natural to require that the evolution of a state is compatible with this interpretation. More precisely, let ρ be a state such that $\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$. This means that with some probability p_i the state ρ is in fact the state $|\Psi_i\rangle\langle\Psi_i|$, in which case, if one applies a map $\mathscr{M}$ on ρ, one in fact applies a map on $|\Psi_i\rangle\langle\Psi_i|$. In other words, for all i, with probability p_i the output states of map $\mathscr{M}$ should be $\mathscr{M}\big(|\Psi_i\rangle\langle\Psi_i|\big)$, *i.e.* we would like that,

$$\forall \rho \in \mathscr{S}(\mathscr{H}),\ \mathscr{M}\big(\rho\big) = \mathscr{M}\Big(\sum_i p_i |\Psi_i\rangle\langle\Psi_i|\Big) = \sum_i p_i \mathscr{M}(|\Psi_i\rangle\langle\Psi_i|). \tag{2.10}$$

The equation (2.10) simply means that we require that the evolution of a state is described by a map that is affine. Note that, since for any affine map $\mathscr{M}$ such that $\mathrm{tr}(L) = 1 \Rightarrow \mathrm{tr}(\mathscr{M}(L)) = 1$, there exists a linear map $\mathscr{N}$ such that $\mathrm{tr}(L) = 1 \Rightarrow \mathscr{M}(L) = \mathscr{N}(L)$,

we can choose evolution maps to be linear without affecting the underlying physics. In this thesis we will only consider linear evolution maps.

Using linearity of such an evolution map $\mathcal{M}$, one can conclude that for any linear operator $L \in \mathcal{L}(\mathcal{H})$ with $\mathrm{tr}(L) \neq 0$,

$$\mathrm{tr}(\mathcal{M}(L)) = \mathrm{tr}\left(\mathrm{tr}(L) \cdot \mathcal{M}\left(L/\mathrm{tr}(L)\right)\right) = \mathrm{tr}(L), \text{ and therefore } \forall L \in \mathcal{L}(\mathcal{H}), \tag{2.11}$$

$$\text{we have } \mathrm{tr}(\mathcal{M}(L)) = \mathrm{tr}(L) \tag{2.12}$$

Equations (2.9),(2.10), and (2.12) motivate the following definition and postulate about transformation (or evolution) of quantum states.

Definition 2.2.3. *Let $\mathcal{H}, \mathcal{H}', \mathcal{H}''$ be three Hilbert spaces. A linear map $\mathcal{M} \in \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}'))$ is called a Completely Positive and Trace Preserving (CPTP) map is it satisfies the following properties,*

Complete Positivity: *For any operator $\rho \in \mathcal{P}(\mathcal{H} \otimes \mathcal{H}'')$, we have $\mathcal{M} \otimes \mathbb{1}_{\mathcal{H}''}(\rho) \geq 0$.*

Trace Preservation: *For any operator $L \in \mathcal{L}(\mathcal{H} \otimes \mathcal{H}'')$, we have $\mathrm{tr}\left(\mathcal{M} \otimes \mathbb{1}_{\mathcal{H}''}(L)\right) = \mathrm{tr}(L)$.*

A map will be simply called Completely Positive (CP) if it only satisfies the Complete Positivity condition, and it will be said to be Completely Positive and Trace Non Increasing (CPTNI) if the Trace Preservation condition is replaced by $\mathrm{tr}\left(\mathcal{M} \otimes \mathbb{1}_{\mathcal{H}''}(\rho)\right) \leq \mathrm{tr}(\rho)$.

Postulate 2.2.4. *Any physical transformation of a quantum state is described by a CPTP map. CPTP maps will also be called quantum channels or simply channels.*

A linear map $\mathcal{M}$ from some operator space $\mathcal{L}(\mathcal{H})$ to another operator space $\mathcal{L}(\mathcal{H}')$ is often called a super operator, and a superoperator $\mathcal{M}$ is an element of $\mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}'))$.

STINESPRING DILATION

Stinespring Dilation relates CPTP maps to unitary evolution in a higher dimensional space.

Lemma 2.2.5 ([6])**.** *Let $\mathcal{M} \in \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}'))$. $\mathcal{M}$ is CPTP if and only if there exists an isometry $V \in \mathcal{L}(\mathcal{H}, \mathcal{H}' \otimes \mathcal{H}'')$ such that, for any $L \in \mathcal{L}(\mathcal{H})$,*

$$\mathcal{M}(L) = \mathrm{tr}_{\mathcal{H}''}(VLV^\dagger). \tag{2.13}$$

Stinespring Dilation is in fact more general, but this version will be sufficient for the purpose of this thesis.

In particular, since for any isometry $V \in \mathcal{L}(\mathcal{H}, \mathcal{H}' \otimes \mathcal{H}'')$ there exists a unitary $U \in \mathcal{U}(\mathcal{H} \otimes \mathcal{H}'', \mathcal{H}' \otimes \mathcal{H}'')$ such that $\forall L \in \mathcal{L}(\mathcal{H})$,

$$VLV^\dagger = U\,(L \otimes |0\rangle\langle 0|)\,U^\dagger, \tag{2.14}$$

Stinespring Dilation relates any physical evolution of a quantum system to a unitary evolution of a bigger system containing the initial system. The extension added to the initial system can be interpreted as being part of the environment.

KRAUS DECOMPOSITION

It is sometimes convenient to decompose a CPTP into its Kraus form.

Lemma 2.2.6. *Let $\mathcal{M} \in \mathcal{L}(\mathcal{L}(\mathcal{H}), \mathcal{L}(\mathcal{H}'))$. $\mathcal{M}$ is CPTP if and only if there exists a finite family of operators $\{K_k\}$ in $\mathcal{L}(\mathcal{H}, \mathcal{H}')$, such that for any $L \in \mathcal{L}(\mathcal{H})$,*

$$\mathcal{M}(L) = \sum_k K_k L K_k^\dagger. \quad \textit{and} \tag{2.15}$$

$$\sum_k K_k^\dagger K_k = \mathbb{1}_{\mathcal{H}}. \tag{2.16}$$

The operators $\{K_k\}_k$ are called Kraus operators.

Proof. This follows from Stinespring Dilation Lemma 2.2.5. Indeed, using notation from Lemma 2.2.5, one can choose $K_k = (\mathbb{1} \otimes \langle k|)V$, where $\{|k\rangle\}$ forms an orthonormal basis of space $\mathcal{H}''$. □

The Kraus Decomposition comes very handy, for example, when it comes to relate CPTP maps and measurements as we explain in the next section.

MEASUREMENTS

Since from Postulate 2.2.4 every transformation has to be described by a CPTP map, the action of making a measurement should also be described by a CPTP map. In particular, since measurement outcomes are classical values, a measurement will be modeled by a CPTP map $\mathcal{M}$ from some space $\mathcal{L}(\mathcal{H}_A)$ (of a system A) to $\mathcal{L}(\mathcal{H}_X \otimes \mathcal{H}_{A'})$ (of a CQ-system XA'). $\mathcal{H}_X$ denotes the Hilbert space of a classical system X that stores the measurement outcomes (that belong to finite alphabet χ), and $\mathcal{H}_{A'}$ denotes the space a potential quantum system A'.

From Lemma 2.2.6 such a channel must have a Kraus decomposition. Moreover, since one of the output registers is classical, the Kraus operator must have have the following form: $K_k = |x_k\rangle \otimes K'_k$, where K'_k is an operator in $\mathcal{L}(\mathcal{H}_A, \mathcal{H}_{A'})$ such that, $\sum_k {K'_k}^\dagger K'_k = \mathbb{1}_A$. We can, thus, write the state after measurement as,

$$\begin{aligned}
\rho_{XA'} = \mathcal{M}(\rho_A) = \sum_k K_k \rho_A K_k^\dagger &= \sum_k |x_k\rangle\langle x_k| \otimes K'_k \rho_A {K'_k}^\dagger \\
&= \sum_{x \in \chi} |x\rangle\langle x| \otimes \sum_{k:x_k = x} K'_k \rho_A {K'_k}^\dagger \\
&= \sum_{x \in \chi} p_x |x\rangle\langle x| \otimes \sum_{k:x_k = x} (K'_k \rho_A {K'_k}^\dagger)/p_x,
\end{aligned} \tag{2.17}$$

where

$$p_x := \mathrm{tr}\left(\sum_{k:x_k = x} K'_k \rho_A {K'_k}^\dagger \right).$$

Therefore, the outcome x occurs with probability p_x and the post-measurement state for this given outcome is

$$\rho_{A'|x} := \sum_{k:x_k = x} (K'_k \rho_A {K'_k}^\dagger)/p_x.$$

Sometimes one is only interested in describing the probability distribution of the measurement outcomes without having to describe the post-measurement state $\rho_{A'|x}$. In this case, one can simplify the measurement, description as follows. In the above we have seen that for any measurement the probability distribution is given by,

$$p_x = \mathrm{tr}\left(\sum_{k:x_k=x} K'_k \rho_A {K'_k}^\dagger\right),$$

so by using cyclicity and linearity of the trace this is equivalent to

$$p_x = \mathrm{tr}\left(\sum_{k:x_k=x} {K'_k}^\dagger K'_k \, \rho_A\right).$$

Let us define

$$P_x := \sum_{k:x_k=x} {K'_k}^\dagger K'_k.$$

One can check that $\forall x \in \chi,\ P_x \geq 0$, and $\sum_x P_x = \mathbb{1}_A$. This motivates the following definition of POVM measurements, which are the most general description of measurements if we are only interested in the probability distribution of the outcome.

Definition 2.2.7 (Positive Operator Valued Measure (POVM))**.** *A POVM is a (finite) set of operators $\{P_x\}_{x\in\chi}$ in $\mathscr{L}(\mathscr{H}_A)$, such that $\forall x,\ P_x \geq 0$, and $\sum_x P_x = \mathbb{1}_A$. Moreover, if $\forall x, x' \in \chi,\ P_x P_{x'} = \delta_{x,x'} P_x$, then the measurement is said to be a projective measurement. The probability of getting outcome x, while performing a measurement given by POVM $\{P_x\}_{x\in\chi}$ on some state ρ, is given by,*

$$p_x := \mathrm{tr}(P_x \rho). \tag{2.18}$$

Lemma 2.2.8. *For any POVM $\{P_x \in \mathscr{L}(\mathscr{H})\}_{x\in\chi}$, there exists an isometry $V \in \mathscr{L}(\mathscr{H}, \mathscr{H} \otimes \mathscr{H}')$ and a projective measurement $\{\Pi_x \in \mathscr{L}(\mathscr{H} \otimes \mathscr{H}')\}_{x\in\chi}$, such that for any state $\rho \in \mathscr{S}(\mathscr{H})$ and for any outcome x,*

$$p_x = \mathrm{tr}(P_x \rho) = \mathrm{tr}(\Pi_x V \rho V^\dagger) \tag{2.19}$$

Proof. Choose $V := \sum_x |x\rangle \otimes \sqrt{P_x}$, and $\Pi_x := |x\rangle\langle x|_{\mathscr{H}'} \otimes \mathbb{1}_{\mathscr{H}}$. □

Using the definition of a general measurement (Def. 2.2.7), we can retrospectively justify eq. (2.7), in which it is stated that the marginal state of a system A, where A is a subsystem of system AB, is given by the partial trace of the joint state ρ_{AB}, namely,

$$\rho_A = \mathrm{tr}_B(\rho_{AB}). \tag{2.20}$$

Indeed, intuitively we want that any two states which always lead to the same outcome distribution to be equal. This means that for any two states ρ_A^1 and ρ_A^2 of system A, we wish that

$$\rho_A^1 = \rho_A^2 \iff \forall \{P_x\}_x,\ \mathrm{tr}(P_x^A \rho_A^1) = \mathrm{tr}(P_x^A \rho_A^2), \tag{2.21}$$

where $\{P_x\}_x$ are POVMs. (We will see in the next section that eq. (2.21) is indeed true. It is due to the fact that the trace distance (Def. 2.2.15) is a distance and therefore satisfies the indiscerniblility property (Def. 2.2.10))

Moreover, according to Def. 2.2.7, if system AB is in state ρ_{AB}, then for any POVM $\{P_x^A\}_x$ measuring subsystem A, the probability distribution of any outcome x is given by,

$$p_x = \mathrm{tr}\left(P_x^A\ \rho_{AB}\right) = \mathrm{tr}\left(P_x^A\ \mathrm{tr}_B(\rho_{AB})\right). \tag{2.22}$$

If one computes the same probability distribution using directly the marginal state ρ_A of subsystem A, one gets,

$$p_x = \mathrm{tr}\left(P_x^A\ \rho_A\right), \tag{2.23}$$

Therefore for any POVM $\{P_x^A\}_x$ and for any outcome x we have $\mathrm{tr}(P_x^A\rho_A) = p_x = \mathrm{tr}\left(P_x^A\ \mathrm{tr}_B(\rho_{AB})\right)$, and therefore, from eq. (2.21) we must have $\rho_A = \mathrm{tr}_B(\rho_{AB})$.

Given a POVM $M = \{P_x\}_x$, one can define an observable as,

$$O = \sum_x x\ P_x. \tag{2.24}$$

The observable is an operator that allows us to compute the expectation values of the measurement outcome of M when evaluated on a quantum state. Let X be the random variable modeling the outcome of the measurement, then

$$\mathbb{E}(X) = \sum_x x p_x = \sum_x x\,\mathrm{tr}(P_x\rho) = \mathrm{tr}(O\rho). \tag{2.25}$$

2.2.4. NORMS AND DISTANCE MEASURES

In this section we will introduce different norms and distances that we use in this thesis. First we remind the reader of the definitions of a norm and a distance.

Definition 2.2.9 (Norm)**.** *A norm $\|\cdot\|$ is a function from a vector space V (over field $K \in \{\mathbb{R},\mathbb{C}\}$) to real numbers such that,*

- *(**Positive definitness**). $\forall |v\rangle \in V$, $\||v\rangle\| \geq 0$ and $\||v\rangle\| = 0 \Rightarrow |v\rangle = 0$.*
- *(**Absolute homogeneity**). $\forall \lambda \in K$, and $\forall |v\rangle \in V$, $\|\lambda|v\rangle\| = |\lambda| \cdot \||v\rangle\|$, where $|\cdot|$ denotes the absolute value of field K.*
- *(**Triangle inequality**). $\forall |v\rangle, |w\rangle \in V$, $\||v\rangle + |w\rangle\| \leq \||v\rangle\| + \||w\rangle\|$.*

Definition 2.2.10 (Distance)**.** *Let $\mathscr{E}$ be a set. A distance $d(\cdot,\cdot)$ on $\mathscr{E}$, is a function from $\mathscr{E} \times \mathscr{E}$ to the real numbers such that,*

- *(**Non-negativity and indiscernibility**). $\forall a, b \in \mathscr{E}$, $d(a,b) \geq 0$ and $d(a,b) = 0 \Leftrightarrow a = b$.*
- *(**Symmetry**). $\forall a, b \in \mathscr{E}$, and $d(a,b) = d(b,a)$.*
- *(**Triangle inequality**). $\forall a, b, c \in \mathscr{E}$, $d(a,b) \leq d(a,c) + d(c,b)$.*

Note that a norm on a vector space induces a distance defined as $\forall |v\rangle, |w\rangle \in \mathscr{H}$, $d(|v\rangle, |w\rangle) := \||v\rangle - |w\rangle\|$.

INDUCED NORMS

The inner product of a Hilbert space induces a norm. Namely $\forall |v\rangle \in \mathscr{H}$, $\||v\rangle\|_2 := \sqrt{\langle v|v\rangle}$.

Remark 2.2.11. *Note that the space $\mathscr{L}(\mathscr{H},\mathscr{H}')$ is also a Hilbert space with inner product (the Hilbert-Schmidt product) defined for all $L, M \in \mathscr{L}(\mathscr{H},\mathscr{H}')$ as,*

$$\langle L, M\rangle := \mathrm{tr}\left(L^\dagger M\right). \tag{2.26}$$

As a consequence, the Hilbert-Schmidt product induces a norm called the Hilbert-Schmidt norm.

One can use the norm on a Hilbert spaces $\mathscr{H}$ and $\mathscr{H}'$ to induce a norm on the space of linear operators $\mathscr{L}(\mathscr{H},\mathscr{H}')$ called the induced norm. This norm intuitively tells us by how much an operator can stretch a vector.

Definition 2.2.12. *Let $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$ be a linear operator. The induced norm of operator L is defined as,*

$$\|L\|_I := \sup_{|v\rangle\in\mathscr{H},|v\rangle\neq 0} \frac{\|L|v\rangle\|_2}{\||v\rangle\|_2} \tag{2.27}$$

SCHATTEN NORMS

Schatten norms, or Schatten p-norms are a family of norms indexed by a parameter p that are defined as follows.

Definition 2.2.13. *Let $p \in [1,\infty[$, and let $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$, then*

$$\|L\|_p := \left(\sum_i s_i(L)^p\right)^{1/p}, \tag{2.28}$$

where $s_i(L)$ are the singular values of L.

When $p \to \infty$, the Schatten $p-$norm tends to the operator norm $\|\cdot\|_\infty$, where $\|L\|_\infty := \max_i s_i(L)$. Note that the operator norm equals the induced norm $\|L\|_\infty = \|L\|_I$.

Property 2.2.14. *Let us here list some of the properties of the Schatten $p-$norms that will be useful in this thesis.*

Monotonicity: *For all $p, p' \in [1,\infty]$ such that $p' \leq p$, we have, $\|\cdot\|'_p \geq \|\cdot\|_p$.*

Isometry invariance: *Let $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$, and $p \in [1,\infty]$. For any isometries $V \in \mathscr{L}(\mathscr{H}',\mathscr{H}'')$ and $V' \in \mathscr{L}(\mathscr{H}''',\mathscr{H})$ we have $\|V L V'\|_p = \|L\|_p$.*

Hölder's inequality: *Let $p \in [1,\infty]$ and q such that $\frac{1}{p}+\frac{1}{q}=1$, then for any operators $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$, $M \in \mathscr{L}(\mathscr{H}'',\mathscr{H}')$*

$$\|LM\|_1 \leq \|L\|_p \|M\|_q \tag{2.29}$$

Duality: *Let $p \in [1,\infty]$ and q such that $\frac{1}{p}+\frac{1}{q}=1$, then for any $L \in \mathscr{L}(\mathscr{H},\mathscr{H}')$*

$$\|L\|_p = \sup_{M:\|M\|_q=1} |\langle L, M\rangle|, \tag{2.30}$$

where $\langle\cdot,\cdot\rangle$ is the Hilbert-Schmidt product. Note that this duality condition implies that $\|\cdot\|_2$ equals the Hilbert-Schmidt norm.

TRACE DISTANCE

In this section we will introduce the trace distance. This is a distance that is used a lot for "measuring" the distance between states, because it has an operational interpretation. Imagine a one-player guessing game in which the player receives from a black-box a state ρ with probability $1/2$ or a state σ with a probability $1/2$, and where he has to guess which of the two states he has received from the box. If the player randomly guesses the state without performing any measurement on the system he receives, his guess will be correct with probability $1/2$. If he measures the system he increases the probability that his guess will be correct: For example, for a given measurement, he may get a correct guess with probability $1/2+\delta$, where $\delta > 0$ is called the "distinguishing probability advantage". The trace distance is directly related to the best "distinguishing probability advantage" the player can obtain, by optimizing over all the possible measurements he can perform on the state.

Definition 2.2.15 (Trace Distance)**.** *Let L and M be operators in $\mathscr{L}(\mathscr{H})$, then we define the trace distance between L and M as,*

$$\Delta(L,M) := \sup_{0\leq P\leq \mathbb{1}} \big|\operatorname{tr}\big(P(L-M)\big)\big|. \tag{2.31}$$

It is not hard to check that the trace distance is a distance according to Def. 2.2.10. In particular the trace distance satisfies the indiscerniblility property of a distance, which justifies why a quantum state is fully characterized by the set of probability distribution induced by all the possible POVM measurements (see eq. (2.21)).

If L and M are self-adjoint then one can write their trace distance as,

$$\Delta(L,M) = \frac{1}{2}\|L-M\|_1 + \frac{1}{2}|\operatorname{tr}(L-M)|, \tag{2.32}$$

where $\|\cdot\|_1$ is the Schatten $1-$norm.

We will often write $\sigma \approx_\epsilon \rho$ if the trace distance between state ρ and state σ is $\Delta(\rho,\sigma)\leq \epsilon$.

Let us now see how the trace distance relates to the best distinguishing probability advantage in the above mentioned guessing game. The best guessing probability the player can have in the guessing game can be written as,

$$P_{\text{guess}} = \sup_{\{P_\rho,P_\sigma\}} \frac{1}{2}\operatorname{tr}(P_\rho\,\rho) + \frac{1}{2}\operatorname{tr}(P_\sigma\,\sigma), \tag{2.33}$$

where $\{P_\rho,P_\sigma\}$ is a POVM. But since $\{P_\rho,P_\sigma\}$ is a POVM, we can rewrite P_σ as $\mathbb{1}-P_\rho$ and thus, the guessing probability becomes,

$$P_{\text{guess}} = \sup_{0\leq P_\rho\leq \mathbb{1}} \frac{1}{2}\operatorname{tr}(P_\rho\,\rho) + \frac{1}{2}\operatorname{tr}((\mathbb{1}-P_\rho)\,\sigma) \tag{2.34}$$

$$= \frac{1}{2}\Big(1+\sup_{0\leq P_\rho\leq \mathbb{1}} |\operatorname{tr}(P_\rho\,(\rho-\sigma))|\Big) \tag{2.35}$$

$$= \frac{1}{2}\big(1+\Delta(\rho,\sigma)\big). \tag{2.36}$$

□

The last equation shows that the best distinguishing probability advantage δ the player can have is bounded by $1/2\,\Delta(\rho,\sigma)$.

Let us spell out one last property of the trace distance. The trace distance contracts under the action of a CPTNI map, namely for any CPTNI map $\mathcal{M}$ and any operator $L, M \in \mathcal{L}(\mathcal{H})$,

$$\Delta\big(\mathcal{M}(L),\mathcal{M}(M)\big) \leq \Delta(L,M). \tag{2.37}$$

This can be interpreted as: "Transformation can only erase information." They cannot allow to increase the distinguishability of two states.

PURIFIED DISTANCE

The purified distance is another distance that is very often used. Indeed, it is directly related to the fidelity. Fidelity is a measure of closeness between states that is relatively easy to estimate in an implementation, and thus relevant for experiments. In a more theoretical perspective, a property that makes the fidelity interesting is that it behaves nicely under extension of states, and in particular under purification. One other property is that for pure states fidelity is linear for one of the state: If ρ, σ_1, and σ_2 are states and ρ is pure, then $F(\rho, \alpha\sigma_1 + \beta\sigma_2) = \alpha F(\rho,\sigma_1) + \beta F(\rho,\sigma_2)$.

Definition 2.2.16 (Purified Distance)**.** *Let ρ and σ be non-normalized states in $\mathcal{S}_\bullet(\mathcal{H})$, then their purified distance is defined as*

$$\nabla(\rho,\sigma) := \sqrt{1 - F(\rho,\sigma)}, \tag{2.38}$$

where $F(\rho,\sigma)$ is the fidelity defined as,

$$F(\rho,\sigma) := \left(\mathrm{tr}\left(|\sqrt{\rho}\sqrt{\sigma}|\right) + \sqrt{(1-\mathrm{tr}(\rho))(1-\mathrm{tr}(\sigma))}\right)^2. \tag{2.39}$$

The purified distance is related to the trace distance by the following Fuchs-Van de Graaff inequality. For any states $\rho, \sigma \in \mathcal{S}_\bullet(\mathcal{H})$,

$$\Delta(\rho,\sigma) \leq \nabla(\rho,\sigma) \leq \sqrt{2\Delta(\rho,\sigma)}. \tag{2.40}$$

As for the trace distance, the purified distance contracts under the action of a CPTNI (see eq. (2.37)).

For any two states ρ_A and σ_A on system A their fidelity can be expressed as a function of their purification. In particular, let $|\rho\rangle_{AB}$ be any purification of ρ_A. Then,

$$F(\rho_A,\sigma_A) = \max_{|\sigma\rangle_{AB}} F\big(|\rho\rangle, |\sigma\rangle\big) = \max_{|\sigma\rangle_{AB}} |\langle\sigma|\rho\rangle|^2, \tag{2.41}$$

where we have used that fidelity for any pure states $|v\rangle$ and $|w\rangle$ is simply $|\langle v|w\rangle|^2$, and the maximum is taken over all purifications $|\sigma\rangle_{AB}$ of σ_A.

Note that for pure states ρ and σ we have that the purified distance and the trace distance are equal: $\Delta(\rho,\sigma) = \nabla(\rho,\sigma)$. Combining this with equation (2.41) we get that for any two statess ρ_A and σ_A on syatem A,

$$\nabla(\rho_A,\sigma_A) = \min_{|\sigma\rangle_{AB}} \Delta(|\rho\rangle_{AB}, |\sigma\rangle_{AB}), \tag{2.42}$$

where $|\rho\rangle_{AB}$ is a purification of ρ_A, and where the minimisation is taken over the purifications $|\sigma\rangle_{AB}$ of σ_A.

2.2.5. NON LOCALITY AND CHSH INEQUALITY

In this thesis, we will be interested in non-local features of quantum mechanics, and in particular, in the CHSH inequality. Indeed, one can use an observed violation of the CHSH inequality in order to lower-bound some entropic quantities [7, 8]. We will use this in many of the security proofs presented in this thesis.

We provide in this section a very short introduction to the notion of non-locality, local hidden variables, and to the CHSH inequality. We refer a curious reader to [9] for more information.

NON-LOCALITY

Non-locality states that space-like separated systems can influence each other. In other words, it says that a system A can influence a system B instantaneously, no matter how far from each other they are. Note that this does not necessarily imply that the systems are sending a signal to each other. Non-locality should be understood as a statement on the probability distributions of measurement outcomes of a set of local measurements $\{M_x^A\}_x$ and $\{M_y^B\}_y$. $\{M_x^A\}_x$ denotes a POVM $M_x^A := \{P_a^x : \forall a,\, P_a^x \geq 0 \,\&\, \sum_a P_a^x = \mathbb{1}\}$and $\{M_y^B\}_y$ performed on systems A, and similarly M_y^B is a POVM performed on system B. As such, and as a first approximation, non-locality states that the joint probability distribution $p(a,b|x,y)$ of the outcomes a and b for any given two local measurements M_x^A and M_y^B performed on systems A and B respectively cannot necessarily be factorized *i.e.* in general,

$$p(a,b|x,y) \neq p(a|x,y)p(b|x,y). \tag{2.43}$$

This means that given any measurement labeled by x on A and y on B, the outcomes a and b are not necessarily independent; they influence each other. This does not imply that one can use this non-locality in order to send a message. To do so, one would need that the output a depends on which measurement y as been performed on B, or reciprocally, that b depends on the measurement choice x. That is, one would need that,

$$\exists y, y', \exists x,\ p(a|x,y) \neq p(a|x,y') \quad \text{or,} \tag{2.44}$$

$$\exists x, x', \exists y,\ p(b|x,y) \neq p(b|x',y). \tag{2.45}$$

Since the non-local condition eq. (2.43) does not imply the "signaling" condition eq. (2.44) or (2.45), one can have a non-local theory that does not violate the non-signaling principle stating that no signal can travel faster than the speed of light. Quantum mechanics is such a theory; it is a non-local and non-signaling theory (for space-like separated systems).

The condition eq. (2.43) is not exactly what a non-local condition should be. Indeed, if both systems A and B carry some shared (classical) information λ, that can be for example a bit string, it is not very surprising that the outcomes a and b are correlated. Such extra information will be called a local hidden variable. In this thesis, we will therefore called a theory non-local if it is not a local hidden variable theory, which we define below.

Definition 2.2.17 ([10])**.** *A local hidden variable theory, is a theory in which the outcome statistics of any set of local measurements $\{M_x^A\}_x$ on systems A and local measurements*

$\{M_y^B\}_y$ on systems B, are such that there exists a random variable Λ taking values in some set $\{\lambda\}_\lambda$, such that, for all x, y, a, b, and λ,

$$p(a,b|x,y,\lambda) = p(a|x,\lambda)\,p(b|y,\lambda), \tag{2.46}$$

where a and b are the outputs of the measurements performed on A and B respectively. The random variables Λ is called the "local hidden variable".

Note that in the above definition we write $p(a|x,\lambda)$ and $p(b|y,\lambda)$ and not $p(a|x,y,\lambda)$ and $p(b|x,y,\lambda)$, because we also require that a local hidden theory is non-signaling.

Definition 2.2.18. *A non-local theory, is a theory that is not a local hidden variable theory. Such a theory can be non-signaling, which is the case for example for quantum mechanics.*

CHSH INEQUALITY

One of the big questions of the 20$^{\text{th}}$ century in physics [11] was to know whether physical quantum systems could be described by a local hidden variable theory, or, as suggested by the theory of quantum mechanics, whether physics is inherently non-local.

In 1964 Bell [10] formalized the notion of local hidden variables as in Definition 2.2.17, and he showed that local theories must satisfy some constraint which non-local theories (like quantum mechanics) do not necessarily satisfy. This constraint can be observed by a statistical test. In other words, Bell found a test that can tell whether our physical world is local or not. The constraint he found, and all the constraints that were found after him are now called Bell inequalities. In this Thesis we will focus on one of the simplest of them, namely, we will mostly talk about the Clauser–Horne–Shimony–Holt (CHSH) inequality [12].

The simplest way to express the CHSH inequality, is by expressing it as a bound on the winning probability of a game called the CHSH game. Let Alice and Bob be the two players of this game. They receive independent random bits x and y respectively. After receiving these bits they have to output bits a and b respectively. They win the game if and only if their output bits satisfy the following equality,

$$a + b = xy \pmod 2. \tag{2.47}$$

From the moment they receive their input bits x and y to the moment they both output their bits a and b, they are not allowed to communicate at all. They can however agree on an arbitrary strategy beforehand. The CHSH inequality simply states that if their strategy can be modeled by a local hidden variable theory, then their winning probability P_w^{CHSH} is bounded as,

$$P_w^{\text{CHSH}} \leq 3/4. \tag{2.48}$$

Quantum mechanics predicts that if Alice and Bob's strategy is based on quantum systems then they can achieve a winning probability up to $\cos(\pi/8)^2 \approx 0.85 > 3/4$. This means that quantum mechanics cannot be modeled by local hidden variables. Bell experiments show that quantum mechanics gives the correct predictions of a violation of the CHSH inequality (the observed $P_w^{\text{CHSH}} > 3/4$). Therefore, quantum systems exhibit a

non-local behavior. Note that quantum mechanics predicts that the states that achieve a winning probability higher than 3/4 are necessarily entangled states. Separable states do not violate the CHSH inequality and they show a local behavior.

The CHSH inequality is often expressed as an inequality on "two-body correlators". Let us consider that Alice and Bob, instead of outputting bits as in the CHSH game, they output $A_x \in \{-1,1\}$ and $B_y \in \{-1,1\}$ when given as inputs bit x and y respectively. Then the CHSH inequality (2.48) can be re-expressed as,

$$S := \mathbb{E}\left(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\right) \leq 2. \tag{2.49}$$

The value $S \in [-4,4]$ taken by $\mathbb{E}\left(A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1\right)$ is called the CHSH value. In fact, any strategy between Alice and Bob that gives them some CHSH value of S, leads to a winning probability P_w^{CHSH} of the CHSH game given by,

$$P_w^{\text{CHSH}} = \frac{1}{2} + \frac{S}{8}. \tag{2.50}$$

From there one can recover that if $P_w^{\text{CHSH}} \leq 3/4$ then $S \leq 2$. If, as for quantum mechanics, $P_w^{\text{CHSH}} \leq \cos(\pi/8)^2 = \frac{1}{2} + \frac{1}{2\sqrt{2}}$ then $S \leq 2\sqrt{2}$. To see more precisely how P_w^{CHSH} relates to the CHSH value S, we point the reader to Ref. [9].

2.3. ENTROPIES

In this section we will introduce the entropic quantities that will be used throughout this thesis as well as some of their properties. This section heavily uses definitions and results from [5], and we point to reader to this book for more extensive discussions about entropies.

VON NEUMANN ENTROPY

The easiest and the most know entropy for quantum states is the Von Neumann entropy which generalizes Shannon entropy to the quantum case.

Definition 2.3.1 (Von Neumann entropy)**.** *Let ρ_A be a state on system A. The Von Neumann entropy of ρ_A is defined as,*

$$H(A)_\rho := -\operatorname{tr}(\rho_A \log(\rho_A)). \tag{2.51}$$

Intuitively, this entropy measures how mixed the state ρ_A is. The more the state is mixed the less one has information about system A.

Let us now consider two systems A and B in a joint state ρ_{AB}. We expect that giving system B to some individual will increase his knowledge about system A *i.e.* the entropy conditioned system B is smaller than the entropy of A alone. To more formally encompass this intuition we define the conditional Von Neumann entropy by analogy to the classical conditional Shannon entropy as,

Definition 2.3.2. *Let ρ_{AB} be a state on system AB. Then the Von Neumann entropy of A conditioned on B is defined as*

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho. \tag{2.52}$$

Using the fact that Von Neumann entropy is additive under tensor product, we have that if $\rho_{AB} = \rho_A \otimes \rho_B$ then $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho = H(A) + H(B)_\rho - H(B)_\rho = H(A)_\rho$. This simply means that if A and B are not correlated then B does not bring any information about A.

2.3.1. MIN- AND MAX-ENTROPY

In this thesis we will also use (smooth) min- and max-entropies [5], which are useful to characterize the "amount of information" in the finite regime. This is in contrast to the Von Neumann entropy which is mostly useful to characterise the amount of information in the asymptotic limit when one is assumed to be able to repeatedly use some resource many times independently (see 2.3.8).

Definition 2.3.3 ([5])**.** *Let ρ_{AB} be a quantum state. The min-entropy on A conditioned on B is,*

$$H_{\min}(A|B)_\rho := -\inf_{\sigma_B \in \mathscr{S}_\bullet(\mathscr{H})} \inf\{\eta \in \mathbb{R} : \rho \leq 2^\eta \mathbb{1}_A \otimes \sigma_B\}, \tag{2.53}$$

$$= -\min_{\sigma_B \in \mathscr{S}_\bullet(\mathscr{H})} \log \left\| \sigma_B^{-1/2} \rho_{AB} \sigma_B^{-1/2} \right\|_\infty \tag{2.54}$$

where σ_B is a non-normalized density operator on system B.

When register A is classical, the min-entropy can be interpreted as $-\log$ of the best guessing probability of the value of A for a party having access to system B [13]. The best guessing probability is obtained by maximizing the probability that the outcome equals the value of A, over all measurements on system B,

$$P_{\text{guess}}(A|B) := \max_{\{P_a\}_a} \sum_a \Pr(A = a) \operatorname{tr}(P_a \rho_{B|a}) = 2^{-H_{\min}(A|B)_\rho}, \tag{2.55}$$

where the maximization is taken over all POVM $\{P_a\}_a$.

We will sometimes also use the max-entropy defined as,

Definition 2.3.4 ([5])**.** *Let ρ_{AB} be a state. Then the max entropy of A conditioned on B is,*

$$H_{\max}(A|B)_\rho := \max_{\sigma_B \in \mathscr{S}_\bullet(\mathscr{H})} \log \left\| \sigma_B^{1/2} \rho_{AB} \sigma_B^{1/2} \right\|_{1/2}, \tag{2.56}$$

where σ_B is a non-normalized density operator on system B.

CONDITIONING ON CLASSICAL INFORMATION

For any qqc-state ρ_{ABY}, if one conditions the min- and max-entropies with the classical system Y, then one can expand the expression of these entropies as follows,

$$H_{\min}(A|BY)_\rho = -\log\left(\sum_y p_y 2^{-H_{\min}(A|BY=y)_{\rho_{|y}}}\right), \tag{2.57}$$

$$H_{\max}(A|BY)_\rho = \log\left(\sum_y p_y 2^{H_{\max}(A|BY=y)_{\rho_{|y}}}\right). \tag{2.58}$$

SMOOTH ENTROPIES

On many occasions it will be easier to use smoothed versions of the min- and max-entropies.

Definition 2.3.5 ([5])**.** *Let ρ_{AB} be a non-normalized state. Let $\epsilon \in \left[0, \sqrt{\mathrm{tr}(\rho_{AB})}\right]$, then the $\epsilon-$smooth min- and max-entropies are defined as,*

$$H_{\min}^{\epsilon}(A|BY)_{\rho} = \sup_{\hat{\rho}\in\mathscr{B}(\rho,\epsilon)} H_{\min}(A|BY)_{\hat{\rho}}, \tag{2.59}$$

$$H_{\max}^{\epsilon}(A|BY)_{\rho} = \inf_{\hat{\rho}\in\mathscr{B}(\rho,\epsilon)} H_{\max}(A|BY)_{\hat{\rho}}, \tag{2.60}$$

where $\mathscr{B}(\rho,\epsilon)$ denotes the ball of non-normalized state centered in ρ_{AB} and of radius ϵ. The radius is defined with respect to the purified distance. If $\epsilon = 0$ then the smoothed min-entropy is simply the min-entropy.

In particular, some chain rules hold for the smooth entropies, but not for the non-smooth versions.

2.3.2. SOME ADDITIONAL PROPERTIES

When A is classical, the smooth min-entropy can be interpreted as the amount of nearly random bits that can be extracted from A with respect to B.

Lemma 2.3.6 (Leftover Hash Lemma with smooth min-entropy [14, 15])**.** *Let $\rho_{A_1^n B}$ be a classical-quantum state, where A_1^n denotes the string of binary random variables $A_1,\ldots,A_n$, and let H be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^l$, that maps the classical n-bit string A_1^n into K_A, and let $\epsilon \geq 0$. Then*

$$\|\rho_{K_A HB} - \tau_{K_A}\otimes\rho_{HB}\|_1 \leq 2^{-\frac{1}{2}\left(H_{\min}^{\epsilon}(A_1^n|B)_{\rho}-l\right)} + 2\epsilon, \tag{2.61}$$

where τ_{K_A} is maximally mixed, i.e. $\tau_{K_A} := \frac{\mathbb{1}_{K_A}}{\dim K_A}$.

One possible operational interpretation of the smooth max entropy we will use in this thesis, is that it gives the amount of information one needs to get, in order to correct a string in which some errors have been introduced.

Theorem 2.3.7 (Max entropy [16] and [17] Lemma 18)**.** *Let X and Y be random variables held by Alice and Bob respectively. Let $\ell^{\epsilon}(X|Y)$ be the minimum amount of information in bits (let denote this information by O, then $|O| = \ell^{\epsilon}(X|Y)$) that Alice needs to send to Bob, such that there exists a function f such that with probability at least $1-\epsilon$ $X = f(Y,O)$. Let $\epsilon' + \epsilon'' = \epsilon$, then*

$$\ell^{\epsilon}(X|Y) \leq H_{\max}^{\epsilon'/2}(X|Y) + \log(8/\epsilon'^2 + 2/(2-\epsilon')) + \log(1/\epsilon''). \tag{2.62}$$

These theorems state that smooth min- and max-entropies have operational interpretation in the finite regime, *i.e.* for finite n. On the other hand, using the next theorem, one can recover the fact that the operational asymptotic behavior (when $n\to\infty$) is given at first order by the Von Neumann entropy.

Theorem 2.3.8 (Asymptotic Equipartition Property (AEP)[18]). *Let $\rho = \rho_{AB}^{\otimes n}$ be an IID state. Then for $n \geq \frac{8}{5}\log\frac{2}{\epsilon^2}$*

$$H_{\min}^{\epsilon}(A_1^n|B_1^n)_{\rho_{AB}^{\otimes n}} \geq nH(A|B)_{\rho_{AB}} - \sqrt{n}\,\delta(\epsilon,\eta) \tag{2.63}$$

and similarly

$$H_{\max}^{\epsilon}(A_1^n|B_1^n)_{\rho_{AB}^{\otimes n}} \leq nH(A|B)_{\rho_{AB}} + \sqrt{n}\,\delta(\epsilon,\eta) \tag{2.64}$$

where $\delta(\epsilon,\eta) = 4\log\eta\sqrt{\log\frac{2}{\epsilon^2}}$ and $\eta = \sqrt{2^{-H_{\min}(A|B)_{\rho_{AB}}}} + \sqrt{2^{H_{\max}(A|B)_{\rho_{AB}}}} + 1$.

Many times we will use a chain rule on min-entropy stating that a conditioning quantum register cannot decrease the entropy more than by its size expressed in qubits.

Theorem 2.3.9 (min-entropy chain rule ([14] or [19],eqs. (2.6))). *Let ρ_{XKQ} be classical on XK, and $\epsilon \geq 0$. Then we have*

$$H_{\min}^{\epsilon}(X|KQ) \geq H_{\min}^{\epsilon}(X|K) - \log\dim(Q). \tag{2.65}$$

2.3.3. ENTROPY ACCUMULATION THEOREM (EAT)

One of the main tools that we will use in Chapters 4 and 5 of this thesis is the Entropy Accumulation Theorem (EAT) developed relatively recently in [20, 21]. We point the reader to [22] for a discussion about the EAT. Roughly speaking the EAT generalizes the AEP (Theorem 2.3.8) to the case where the state $\rho_{A_1^nB_1^n}$ is not IID. However, it requires that the state on which the EAT is applied, satisfy a Markov condition.

Definition 2.3.10 (Markov Condition). *Let ρ_{ABC} be a state in $\mathcal{S}(\mathcal{H}_{ABC})$. We say that ρ_{ABC} satisfies the Markov condition $A \leftrightarrow B \leftrightarrow C$ if and only if*

$$I(A:C|B)_{\rho} = 0, \tag{2.66}$$

where $I(A:C|B)_{\rho} := H(A|B)_{\rho} + H(C|B)_{\rho} - H(AC|B)_{\rho}$ is the mutual information between A and C conditioned on B for the state ρ_{ABC}.

This condition becomes trivial when A, B and C are independent random variables. For more details on the definition of the Markov condition see [23, section 2.2 & appendix C].

To be more precise, the EAT applies to states of the form,

$$\rho_{C_1^nA_1^nB_1^nE} := (\mathrm{tr}_{R_n} \circ \mathcal{M}_n \circ \ldots \circ \mathcal{M}_1 \otimes \mathbb{1}_E)(\rho_{R_0E}), \tag{2.67}$$

for some arbitrary initial state $\rho_{R_0E} \in \mathcal{S}(\mathcal{H}_{R_0E})$ and, $\forall i \in [n]$, $\mathcal{M}_i$ is a EAT channel defined as follows.

Definition 2.3.11 (EAT channels (from [20])). *For $i \in [n]$ we call $\mathcal{M}_i$ a EAT channel if $\mathcal{M}_i$ is a CPTP map from R_{i-1} to $C_iA_iB_iR_i$ such that $\forall i \in [n]$:*

1. *A_i, B_i, C_i are finite dimensional systems, C_i is classical and R_i is an arbitrary quantum system.*

2. *For any state $\sigma_{R_{i-1}R}$, where R is isomorphic to R_{i-1}, the output state $\sigma_{R_iA_iB_iC_iR} := (\mathcal{M}_i \otimes \mathbb{1}_R)\sigma_{R_{i-1}R}$ is such that the classical register C_i can be measured from $\sigma_{A_iB_i}$.*

3. *Any state defined as in (2.67) satisfies the following Markov conditions,*

$$\forall i \in [n],\ A_1^{i-1} \leftrightarrow B_1^{i-1}E \leftrightarrow B_i. \tag{2.68}$$

To state EAT we also need the notion of min- and max-tradeoff functions. Let $\mathbb{P}(\mathscr{C})$ be the set of distributions on the alphabet $\mathscr{C}$ of C_i. For any $q \in \mathbb{P}(\mathscr{C})$ we define the set of states

$$\Sigma_i(q) := \{\sigma_{C_iA_iB_iR_iR} = (\mathcal{M}_i \otimes \mathbb{1}_R)(\sigma_{R_{i-1}R}) : \sigma_{R_{i-1}R} \in \mathscr{S}(\mathscr{H}_{R_{i-1}R}) \ \&\ \sigma_{C_i} = q\}. \tag{2.69}$$

Definition 2.3.12. *A real function f_i on $\mathbb{P}(\mathscr{C})$ is called a min-tradeoff function for a map $\mathcal{M}_i$ if*

$$f_i(q) \leq \inf_{\sigma \in \Sigma_i(q)} H(A_i|B_iR)_\sigma, \tag{2.70}$$

and max-tradeoff function for a map $\mathcal{M}_i$ if

$$f_i(q) \geq \sup_{\sigma \in \Sigma_i(q)} H(A_i|B_iR)_\sigma. \tag{2.71}$$

If $\Sigma_i(q) = \varnothing$, the infimum is taken to be $+\infty$ and the supremum $-\infty$.

Definition 2.3.12 states that the min-(max-)tradeoff function is a lower (upper) bound on the conditional von Neumann entropy $H(A_i|B_iR)_\sigma$ of a final state $\sigma_{C_iA_iB_iR_iR}$, for all states that result from the action of the channel $\mathcal{M}_i$ on an arbitrary initial state and exhibit a particular distribution q over the classical variable C_i, where R is a side information. Typically, when analysing protocols we will use the CPTP map $\mathcal{M}_i$ to model the set of operations performed in a protocol at round i. In particular, this means that the EAT fundamentally requires a protocol to be sequential[2]. Note that in the protocols we will analyze in this thesis, C_i will be the variable that encodes the wins or the losses of a CHSH game (or a similar game) performed in the test rounds of these protocols. Therefore, in this thesis, the set $\Sigma_i(q)$ can be seen as the set of states that achieve certain statistics in the Bell test. This means that the min-tradeoff function is a lower-bound on the Von Neumann entropy for all states which achieve some CHSH value.

Let $\mathsf{freq}(C_1^n)$ be the vector in $\mathbb{P}(\mathscr{C})$ that contains the frequency of apparition of each of the elements of $\mathscr{C}$ in C_1^n. We can now state the EAT.

Theorem 2.3.13 (EAT from [20])**.**
Let $\mathcal{M}_1, \ldots, \mathcal{M}_n$ be EAT channels and $\rho_{C_1^nA_1^nB_1^nE}$ be a state as defined in (2.67), let $h \in \mathbb{R}$, f be an affine min-tradeoff function for all the maps $\mathcal{M}_i$, $i \in [n]$, and $\epsilon \in]0,1[$. For any event $\Omega \subseteq \mathscr{C}^n$ such that $f(\mathsf{freq}(C_1^n)) \geq h$,

$$H_{\min}^\epsilon(A_1^n|B_1^nE)_{\rho_{|\Omega}} \geq nh - v\sqrt{n}, \tag{2.72}$$

[2] In fact, it requires that the state produced by the studied protocol can also be produced by some sequential protocol

where $v = 2(\log(1+2d_A) + \lceil \|\nabla f\|_\infty \rceil)\sqrt{1-2\log(\epsilon \cdot p_\Omega)}$, *where* d_A *is the maximum dimension of the system* A_i. *On the other hand we have,*

$$H^\epsilon_{\max}(A_1^n|B_1^n E)_{\rho|\Omega} \leq n\tilde{h} + v\sqrt{n}, \tag{2.73}$$

where we replace f *by an affine max-tradeoff function* $\tilde{f}$, *such that the event* Ω *implies* $\tilde{h} \geq \tilde{f}(\text{freq}(C_1^n))$.

2.4. CRYPTOGRAPHY

2.4.1. DEVICE INDEPENDENCE (DI)

Many quantum protocols have been proven to be secure implicitly by assuming that the preparation device – which prepares quantum states – or the measurement devices used during the protocol, work as expected. However, in real implementations, measurement devices use photon detectors that do not have 100% efficiency, and many photons are lost in fibers etc. This may allow the adversary to tamper with these devices to get advantage and break security. This is what has been shown in [24, 25].

In order to remedy these issues, one could, each time a security flaw is discovered, try to fix it. On the other hand, a more satisfactory approach is that one could try to fix all possible flaws at once. Even though the latter approach may seem surprising at first, this is the path taken by many, and it has lead to the notion of device-independence (DI) [7, 26, 27].

The device-independent scenario models the underlying system and measurement devices as black boxes where the only relevant information is the statistics of inputs and outputs. In particular, we often rely on the ability of these devices to violate a Bell inequality. In this thesis we will focus on the CHSH inequality or some variant of it. To check whether a set of devices can achieve Bell violation, DI protocols include some test rounds in which the parties play a CHSH game. This will allow to collect some statistics and test the quality of the device. Therefore, no assumptions on the dimension of the quantum systems or the particular measurements performed by the devices are required. This represents a significant relaxation of the assumptions present in an implementation of, for example, the BB84 protocol [28]. However, it is important to remark which assumptions remain present in any implementation of a DI protocol.

Assumptions 2.4.1 (Device-Independent model)**.** *In the device-independent model we assume:*

1. *Isolated labs: no information is leaked from or enters Alice's and Bob's labs, apart from the state distribution before the measurements and the public classical information dictated by the protocol.*
2. *Isolated source: the preparation of states is independent of the measurements.*
3. *Trusted classical post-processing: the local classical computations are trusted.*
4. *Classical authenticated channel*[3] *: all the public classical communication is performed using an authenticated channel.*

[3] This condition only applies when it makes sense, *i.e.* when at least two parties trust each other and defend again an external adversary.

5. *Trusted Random Number Generators: If the parties use a Random Number Generator, we will assume that the honest parties possess independent and trusted random number generators.*

It is sometimes hard to work with this level of generality, and the protocols that are device-independent may be much less efficient than their "trusted devices" counterpart, which may lead one to assume further conditions.

Assumptions 2.4.2 (IID-Assumption)**.** *It is often assumed that, even if the behavior of the devices used during the protocol can deviate arbitrarily form their honest behavior, the devices used behave in the exact same way for each use of theses devices, independently of the other uses:*

IID-Source: *If the device is a quantum state preparation device (also called source), the state produced across the n uses of this device will have the IID form:* $\rho_{A_1^n} = \rho_A^{\otimes n}$.

IID-Measurement Device: *For all of the uses of the measurement device, each setting of the device can be modeled by a single POVM measurement. In particular, these POVMs only depend on the settings, not on the use of the device, so that for a fixed setting, the POVM for the first use is the same as for any other use of the device.*

In practice, the IID-Assumption is not always satisfied, and therefore, if one wants to prove security for a practical set-up, then they would need to remove this assumption. However, the techniques used to prove security with the IID-Assumption are often very useful for the more general case. As such, proofs with the IID-Assumption can be seen as first step towards full Device-Independent security.

Assumptions 2.4.3 (Measurement-Device Independence (MDI))**.** *Sometimes, one may still trust the preparation devices but not the measurement devices used in a protocol. In this case we talk about Measurement-Device Independence, and only the measurement devices are treated as black boxes, while the preparation devices are assume to be sufficiently well characterized so that we know which state is produced every time it is used.*

One of the reason why one would like to prove security in the MDI settings, is that protocols in the MDI settings are often easier to implement and more efficient than DI protocols, while providing with sufficiently good security guarantees.

2.4.2. KEY DISTRIBUTION/AGREEMENT

Key distribution, or key agreement, is the task that consists in giving to two or more parties a random key in such a way that any external party is ignorant about the key[4], even if the external party is spying over all available communication performed during the protocol.

If no assumption is made on the power of the external party – usually called adversary, or eavesdropper – then there is no secure protocol implementing key distribution using only classical communication. However, if one uses quantum communication, then there exist protocols that achieve this task [28]. For historical reasons, in the case

[4] Being ignorant about the key, roughly speaking, means that the maximum probability of guessing the key is $2^{-\text{length of key}}$

where only two parties want to share a key, these protocols are referred to as Quantum Key Distribution (QKD) protocols, and the multyparty case is called Conference Key Agreement (CKA).

Let K_A and $K_{B_1},\dots,K_{B_{N-1}}$ denote the final key held by Alice and $\text{Bob}_1,\dots,\text{Bob}_{N-1}$, respectively, after they perform a QKD protocol. A QKD protocol is secure if it is correct and secret. Correctness is the statement that Alice and Bob share the same key at the end of the protocol, *i.e.*, $K_A = K_{B_1} = \dots = K_{B_{N-1}}$. Secrecy is the statement that the eavesdropper is totally ignorant about the final key.

More formally, the security definition we will use in this thesis goes as follows.

Definition 2.4.4. *(Correctness) We will call a Device-Independent Conference Key Agreement (DICKA) protocol ϵ_{corr}-correct for an implementation, if Alice's and Bobs' keys, K_A, $K_{B_{(1)}},\dots,K_{B_{(N-1)}}$, are all identical with probability at least $1-\epsilon_{\text{corr}}$.*

Definition 2.4.5. *(Secrecy) We say that a DICKA protocol is ϵ_{sec}-secret for an implementation, if conditioned on not aborting Alice's key K_A is ϵ_{sec}-close to a key that Eve is ignorant about. More formally for a key of length l, we want*

$$p_{\hat{\Omega}} \cdot \frac{1}{2} \left\| \rho_{K_A E|\hat{\Omega}} - \frac{\mathbb{1}_A}{2^l} \otimes \rho_{E|\hat{\Omega}} \right\|_1 \leq \epsilon_{\text{sec}},$$

where $\hat{\Omega}$ is the event of the protocol not aborting, and $p_{\hat{\Omega}}$ is the probability for $\hat{\Omega}$.

Note that if a protocol is ϵ_{corr}-correct and ϵ_{sec}-secret then it is ϵ^s-correct-and-secret for $\epsilon^s \geq \epsilon_{\text{corr}} + \epsilon_{\text{sec}}$.

Definition 2.4.6 (Security)**.** *A Key Distribution/Agreement protocol is called $(\epsilon^s, \epsilon^c, l)$-secure if:*

1. *(Soundness) For any implementation of the protocol, either it aborts with probability greater than $1-\epsilon^s$ or it is ϵ^s-correct-and-secret.*
2. *(Completeness) There exists an honest implementation of the protocol, such that the probability of aborting the protocol is less than ϵ^c, that is $1-p_{\hat{\Omega}} \leq \epsilon^c$.*

Note that in the trusted device scenario, this definition provides very strong security guarantees. In particular, a protocol that satisfies this definition can be composed with other arbitrary protocols while preserving security. The protocol is then said to be universally composable. In the device-independent settings, the situation is more complicated. Indeed, in order to guarantee composibility with the DI definition one has to destroy the devices used after each execution of a protocol and replace them by new ones [29]. Some works address this issue [30] by using secure multi-party computation techniques.

2.4.3. TWO-PARTY CRYPTOGRAPHY

Two party cryptography allows two parties – *e.g.* Alice and Bob – to jointly compute a function $f(\cdot,\cdot)$ on their respective inputs a and b, in a way that these inputs remain private with regard to the other party (Fig. 2.1). We stress that in a two-party protocol Alice and Bob cannot trust each other, as opposed to a QKD protocol.

The generality of two-party cryptography allows for many different tasks. One simple example is called private identification. Let's say Alice is a server, and Bob is a client who wants to connect to the server. The server (Alice) will only allow Bob to connect if Bob inputs the good password K. Alice knows the password (or maybe some hash of it). The two-party function they then want to implement is the following. Alice's input a password K'', and Bob$'$ input his guess of the password K', the function $f(K,K')$ outputs 1 to both Alice and Bob if $K = K'$ and 0 otherwise. Of course, if Bob is a legitimate user who knows the password, there is no problem, he will always input $K' = K$, and the function will always output 1. But maybe some non-authorised client Bob$'$ tries to impersonate Bob and tries to connect while not knowing the password. Of course, we do not want that Bob$'$ to get any information about K while interacting with the server Alice. On other hand, if a fake server Alice$'$ who does not know K and tries to impersonate Alice, then we do not want Alice$'$ to get any information about K either.

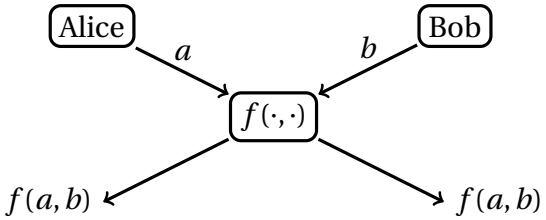


Figure 2.1: Schematic of a two-party computation. Each of the parties has an input, and they must compute the function f on these inputs, in a way that Alice never learns Bob's input and *vice versa*.

It has been shown [31] that any two party protocol can be build upon of a much simpler task called Oblivious Transfer (OT) (see the next section). For this reason we say that OT is universal. This makes OT a central and well-studied task in two-party cryptography. Another well studied task is Bit Commitment (BC) (see details below). If we limit the parties to classical communication, it can be shown that BC is not universal, since it cannot be used to get OT [32]. However, many protocols implementing two-party cryptographic tasks use BC as a subroutine, even thought BC is not universal in purely classical protocols. Interestingly, when quantum communication is used in a protocol, Bit Commitment becomes universal [33].

Unfortunately, it is well known that neither of these two tasks – OT and BC – can be secure against an arbitrarily powerful adversary, even using quantum mechanics [34–36]. This sharply contrasts with QKD and other Key Agreement tasks, in which there is no information theoretically secure classical protocol, but for which using quantum systems allows to achieve such security. These no-go results motivate the use of assumptions on the power of the adversary. In particular, one popular assumption is the Bounded Quantum Storage Model (BQSM) or its generalization, the Noisy Quantum Storage Model (NQSM). In the BQSM the adversary is assumed to be unable to store more than a certain amount of quantum information. In other words, the size of the adversary's quantum memory is bounded. On the other hand, in the NQSM the adversary is assumed to have a quantum memory that is not perfect; it is noisy. The BQSM can be viewed as a particular case of the NQSM, where the noise erase all the information beyond a certain storage

capacity. The NQSM allows to prove the security of protocols for OT and BC [37–41]. For all the Chapters treating of two-party cryptography protocols we will work in the NQSM.

In the two next sections we present the variants of OT and BC that we will use in this thesis, as well as an other primitive called Weak String Erasure (WSE). The formal definitions we will use for these tasks are based on [39].

OBLIVIOUS TRANSFER

OT, or rather its variant called Randomized 1-out-2 Oblivious String Transfer, is a task in which Alice receives two random strings (S_0, S_1), and Bob receives one of these strings S_C together with its corresponding index C (see Fig. 2.2). As explained in [39], Randomised OT can be transformed into a non-randomised version, in which Alice can chose the strings she "receives".

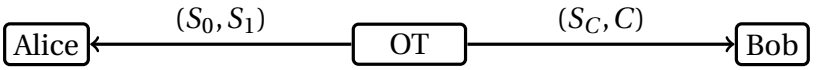


Figure 2.2: In a Randomized 1-out-2 Oblivious String Transfer, Alice should get two random l-bit strings (S_0, S_1) and Bob should receive a random bit C together with S_C which is one of the two strings Alice has received. Alice should never learn C and Bob should remain ignorant about at least one of the two bit-strings Alice receives.

Informally, we say a protocol implementing this Randomized 1-out-2 Oblivious String Transfer is secure for honest Alice, if dishonest Bob is ignorant about one of the two strings S_0 or S_1 that Alice obtained. On the other hand, the protocol is secure for honest Bob if dishonest Alice is ignorant about which string honest Bob received.

In this thesis we will use the security definition of Oblivious Transfer from [39] stated below.

Definition 2.4.7 (Randomized 1-out-2 (l,ϵ)-Oblivious String Transfer (OST))**.**
Let τ_R denote the maximally mixed state on register R.

A fully randomized 1-out-2 (l,ϵ)-Oblivious String Transfer scheme is a protocol between two parties, Alice and Bob, that satisfies the following three conditions.

Correctness *If both parties are honest there exists an ideal state $\sigma_{S_0S_1CS_C}$, where $S_1, S_1 \in \{0,1\}^l$ and $C \in \{0,1\}$, such that:*

- *The distribution over S_0, S_1 and C is uniform:*

$$\sigma_{S_0S_1C} = \tau_{S_0} \otimes \tau_{S_1} \otimes \tau_C. \tag{2.74}$$

- *The real state ρ produced by the protocol is ϵ-close (in the trace distance) to the ideal state:*

$$\rho_{S_0S_1C\hat{S}_C} \approx_\epsilon \sigma_{S_0S_1CS_C}. \tag{2.75}$$

Security for Bob *If Bob is honest, there exists an ideal state $\sigma_{AS_0S_1C}$ such that:*

- *Alice is ignorant about C:*

$$\sigma_{AS_0S_1C} = \sigma_{AS_0S_1} \otimes \tau_C. \tag{2.76}$$

- *The real state ρ produced by the protocol is $\epsilon-$close (in the trace distance) to the ideal state:*

$$\rho_{AC\hat{S}_C} \approx_\epsilon \sigma_{ACS_C}. \tag{2.77}$$

Security for Alice *If Alice is honest, there exists an ideal state $\sigma_{S_0S_1BC}$ such that:*

- *Bob is ignorant about S_{1-C}:*

$$\sigma_{S_0S_1BC} = \sigma_{S_CBC} \otimes \tau_{S_{1-C}}. \tag{2.78}$$

- *The real state ρ is $\epsilon-$close (in the trace distance) to the ideal state:*

$$\rho_{S_0S_1B} \approx_\epsilon \sigma_{S_0S_1B}. \tag{2.79}$$

BIT COMMITMENT

Bit Commitment is a two-phase task between two parties, Alice and Bob, where in the first phase Alice commits to a bit of her choice to Bob. Later they can run the second phase (the "Open" phase) where Alice reveals the bit to which she committed. Importantly, Alice should not be able to open a bit different than the one to which she committed. We also require that Bob cannot learn the value of the committed bit before Alice opens it. The case in which Alice commits to a bit-string rather than a single bit is called String Commitment. In the following we give a definition for a randomized version of String Commitment, in which Alice does not get to choose the string she commits to. This string will be chosen uniformly at random by the protocol. Note that a Randomized String Commitment can be turned into a String Commitment scheme as explained in [39].

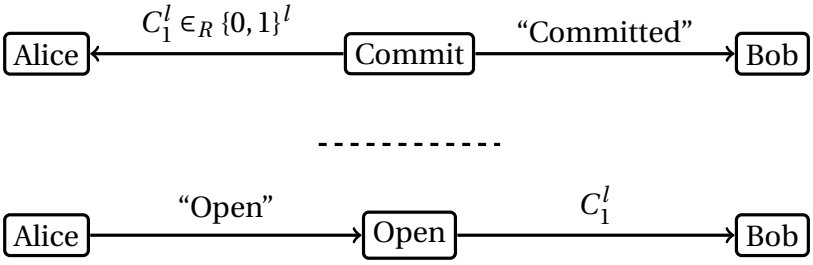


Figure 2.3: Ideal Randomized String Commitment. In the first part Alice gets a random l-bit string $C_1^l \in \{0,1\}^l$, and Bob is notified that the string is committed. In the second phase, Alice asks "the box" to reveal the string to Bob.

Informally, a protocol implementing Randomized String Commitment is said to be secure for honest Alice, if before the Open phase, dishonest Bob is ignorant about the committed string. It is said to be secure for honest Bob, if after the Commit phase, there exists only a single string to which dishonest Alice can open while honest Bob accepts.

In this thesis we will use the security definition of String Commitment from [39] stated below.

Definition 2.4.8 (Randomized String Commitment)**.** *Let τ_R denote the maximally mixed state on a register R.*

A (l,ϵ)-Randomized String commitment scheme is a protocol between Alice and Bob that satisfies the following three properties.

Correctness *When both parties are honest, then there exists a state $\sigma_{C_1^l C_1^l F}$, called the ideal state that is defined as:*

- $\sigma_{C_1^l F} := \tau_{C_1^l} \otimes |accept\rangle\langle accept|_F$,
- *The real state produced by the protocol $\rho_{C_1^l \tilde{C}_1^l F}$ is ϵ-close (in the trace distance) to the ideal state $\sigma_{C_1^l C_1^l F}$,*

$$\rho_{C_1^l \tilde{C}_1^l F} \approx_\epsilon \sigma_{C_1^l C_1^l F}.$$

Security for Alice (against dishonest Bob) *When Alice is honest, Bob is ignorant about C_1^l before the Open phase:*

$$\rho_{C_1^l B} \approx_\epsilon \tau_{C_1^l} \otimes \rho_B.$$

The protocol is then said to be ϵ-hidding.

Security for Bob (against dishonest Alice) *After the Commit phase and before the pen phase, there exists an ideal state $\sigma_{C_1^l AB}$ such that for any Open algorithm, describe by the CPTP maps $\mathcal{O}_{\mathcal{AB}}$, in which Bob is honest, we have:*

- *Bob almost never accepts $\tilde{C}_1^l \neq C_1^l$:*
  for $(\mathbb{1}_{C_1^l} \otimes \mathcal{O}_{AB})(\sigma_{C_1^l AB})$ we have $\Pr(\tilde{C}_1^l \neq C_1^l \text{ and } F = accept) \leq \epsilon$.
- *The real state produced in the commitment phase is close (in the trace distance) to the ideal state:*

$$\rho_{AB} \approx_\epsilon \sigma_{AB}.$$

The protocol is then said to be ϵ-binding.

WEAK STRING ERASURE (WSE)

Weak String Erasure (WSE) is a primitive that allows one to get OT and BC using only classical post-processing (see [39] or see Chapter 6: in all the protocols presented, the "preparation phase" of OT and BC protocols in fact corresponds to a protocol that implements WSE). As a consequence, it is also impossible to have a protocol implementing WSE that is secure against an all powerful adversary, even using quantum communication. Therefore, we will also treat WSE (in particular in Chapter 3) in the NQSM.

WSE is a two-party primitive, such that if Alice and Bob are honest then at the end of its execution Alice holds a random bit string $X_1^n \in \{0,1\}^n$ and Bob holds a random substring $X_{\mathcal{I}}$ of X_1^n where $\mathcal{I}$ is a random subset of $\{1,2,\ldots,n\}$. WSE is secure for honest Bob if Alice cannot guess the set $\mathcal{I}$ better than random chance, and for honest Alice if it is hard for Bob to guess the entire Alice's string, *i.e.* if the probability that $X_1^n = \tilde{X}_1^n$ is low,

where X_1^n is the random variable corresponding to Alice's output measurement and $\tilde{X}_1^n$ is the random variable corresponding to Bob's guess, that is

$$\begin{aligned} &\exists \alpha > 0 : \; H_{\min}(X_1^n|\text{Bob}) \geq \alpha n \\ \Leftrightarrow\; &\exists \alpha > 0 : \; P_{\text{guess}}(X_1^n|\text{Bob}) = 2^{-H_{\min}(X_1^n|\text{Bob})} \leq 2^{-\alpha n}. \end{aligned} \tag{2.80}$$

In this thesis, we will use the definition from [39] stated below.

Definition 2.4.9 ($(\alpha,\epsilon)-$Weak String Erasure)**.**

Correctness: *If both Alice and Bob are honest, then the state $\rho_{X_1^n(X_{\mathscr{J}},\mathscr{I})}$ produced at the end of the protocol, where Alice holds X_1^n and Bob holds $(X_{\mathscr{J}},\mathscr{I})$, is such that the marginal $\rho_{X_1^n,\mathscr{J}}$ is $\epsilon-$close (in the trace distance) to $\tau_{X_1^n}\otimes\tau_{\mathscr{J}}$, where τ denotes the maximally mixed state.*

Security for Alice: *If Alice is honest, then the state $\rho_{X_1^n B}$ produced at the end of the protocol, where Alice holds X_1^n and Bob holds B, is such that,*

$$\exists \alpha > 0 : \; H_{\min}^{\epsilon}(X_1^n|B)_{\rho} \geq \alpha n. \tag{2.81}$$

Security for Bob: *If Bob is honest, then there exists an ideal state $\sigma_{X_1^n A(X_{\mathscr{J}},\mathscr{I})}$ such that the marginal $\rho_{A\mathscr{J}}$ of the real the state $\rho_{A(X_{\mathscr{J}},\mathscr{I})}$ produced at the end of the protocol is $\epsilon-$close (in the trace distance) to $\sigma_{A,\mathscr{J}}$, and where the ideal state $\sigma_{X_1^n A(X_{\mathscr{J}},\mathscr{I})}$ is such that $\sigma_{X_1^n A\mathscr{J}} = \sigma_{X_1^n A}\otimes\sigma_{\mathscr{J}}$.*

2.4.4. POSITION VERIFICATION (PV)

In most cryptographic protocols, the credential used by the users or by the end nodes, is something they "know": A secret key, a password etc. Position-Based Cryptography (PBC) [42–44] provides another paradigm in which the only credential used is the physical position of the user/process. A central task in PBC is Position Verification (PV). In this section, we informally describe PV.

Position Verification (PV) has three protagonists in the honest scenario, namely two verifiers V_1 and V_2, and one prover P. For simplicity, we restrict to position verification in one spatial dimension. The prover claims to be at some geographical position, and the PV protocol permits to prove to the verifiers whether this is true. The protocol is then secure, if the probability that one or more dishonest provers impersonate a real prover in the claimed position, decays exponentially with the number of qubits exchanged in the protocol.

When the devices are trusted and the prover is honest, a protocol implementing PV can be as follows [45–49] (see Fig. 2.4). V_1 prepares n EPR entangled pairs, measures half of all the pairs in some bases $\Theta_1^n \in \{0,1\}^n$ to get outcomes $X_1^n \in \{0,1\}^n$, and sends the other half to the prover P. V_2 sends Θ_1^n to P; this random string can be preshared between the verifiers before the protocol begins. When the prover receives all the information, he measures the halves of the EPR pairs he received in the bases Θ_1^n to get X_1^n and sends it back to both verifiers. Then the verifiers check whether the prover's answer

is correct, and measure the time it took between the moment they sent information and the moment they receive the answer from the prover. If the answer is correct and if the prover replies within a predefined time Δt, then the execution of the protocol is considered successful.

A protocol implementing PV is said secure if, for any group of dishonest prover in which none of them is at the claimed position, the probability that the verifiers accept is decaying exponentially in the number of messages sent by the verifiers to the the provers.

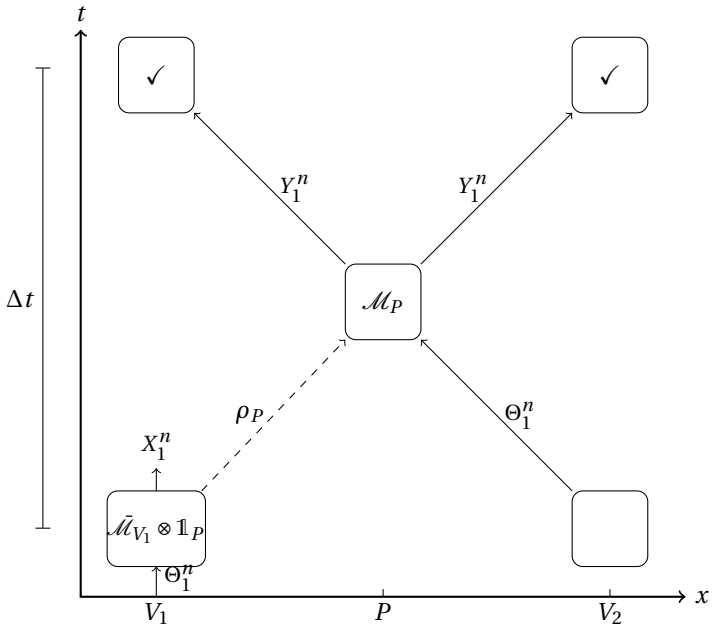


Figure 2.4: V_1 uses Θ_1^n as an input to his device, which creates a bipartite state ρ_{AP} and sends the part ρ_P to the prover P, and measures the other part ρ_A to produce $X_1^n \in \{0,1\}^n$ as output. At the same time V_2 sends Θ_1^n to P. When P receives the state and Θ_1^n, he makes a measurement on the state and obtains $Y_1^n \in \{0,1\}^n$. He sends Y to both verifiers. The verifiers check if $Y_1^n = X_1^n$ (or if Y_1^n is "close enough" to X_1^n), and measure the time it took to get back an answer from P.

A single dishonest prover cannot cheat, because he cannot reply on time to both verifiers. More than one dishonest prover is required and, without loss of generality (in one dimension), we can consider at most two dishonest provers whose goal is to impersonate one honest prover who would be at the claimed position. In this case there exists a general attack on the protocol [47, 50]. This attack, however, requires an exponential amount of entanglement with respect to the amount of quantum information received from the verifiers. Hence, it is natural to ask if security is possible when the adversaries hold a limited amount of entanglement. In this thesis we will work in this framework of dishonest provers.

REFERENCES

[1] G. Grimmett and D. Welsh, Probability: an introduction (Oxford University Press, 2014).

[2] W. Hoeffding, *Probability inequalities for sums of bounded random variables,* Journal of the American Statistical Association **58**, 13 (1963), https://amstat.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830 .

[3] M. A. Nielsen and I. Chuang, Quantum computation and quantum information (AAPT, 2002).

[4] M. Tomamichel, A framework for non-asymptotic quantum information theory, Ph.D. thesis (2012).

[5] M. Tomamichel, Quantum Information Processing with Finite Resources - Mathematical Foundations, SpringerBriefs in Mathematical Physics, Vol. 5 (Springer International Publishing, 2016).

[6] W. F. Stinespring, *Positive functions on c*-algebras,* Proceedings of the American Mathematical Society **6**, 211 (1955).

[7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks,* Phys. Rev. Lett. **98**, 230501 (2007).

[8] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-independent quantum key distribution secure against collective attacks,* New Journal of Physics **11**, 045021 (2009).

[9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality,* Rev. Mod. Phys. **86**, 419 (2014).

[10] J. S. Bell, *On the eintein podolsky rosen paradox,* Physics 1, 195-200 (1964).

[11] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev. **47**, 777 (1935).

[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Phys. Rev. Lett. **23**, 880 (1969).

[13] R. Konig, R. Renner, and C. Schaffner, *The operational meaning of min- and max-entropy,* IEEE Transactions on Information Theory **55**, 4337 (2009), http://dx.doi.org/10.1109/TIT.2009.2025545 .

[14] R. Renner, Security of Quantum Key Distribution, Ph.D. thesis, PhD Thesis, 2005 (2005).

[15] M. Tomamichel and A. Leverrier, *A largely self-contained and complete security proof for quantum key distribution,* Quantum **1**, 14 (2017).

[16] R. Renner and S. Wolf, Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 199–216.

[17] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information,* IEEE Transactions on Information Theory **57**, 5524 (2011).

[18] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition property,* IEEE Transactions on Information Theory **55**, 5840 (2009).

[19] C. Schaffner, Cryptography in the Bounded-Quantum-Storage Model, Ph.D. thesis, BRICS, University of Aarhus (2007).

[20] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation,* Nature Communications **9**, 459 (2018).

[21] R. Arnon-Friedman, R. Renner, and T. Vidick, *Simple and tight device-independent security proofs,* SIAM Journal on Computing **48**, 181 (2019).

[22] R. Arnon-Friedman, *Reductions to iid in device-independent quantum information processing,* (2018).

[23] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation,* arXiv:1607.01796 (2016), arXiv:1607.01796 [quant-ph] .

[24] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems,* Phys. Rev. A **74**, 022313 (2006).

[25] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, *Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing,* Phys. Rev. A **91**, 032326 (2015).

[26] D. Mayers and A. Yao, Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS '98 (IEEE Computer Society, Washington, DC, USA, 1998) pp. 503–.

[27] J. Barrett, L. Hardy, and A. Kent, *No signaling and quantum key distribution,* Phys. Rev. Lett. **95**, 010503 (2005).

[28] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560, Part 1**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}.

[29] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography,* Phys. Rev. Lett. **110**, 010503 (2013).

[30] M. Curty and H.-K. Lo, *Foiling covert channels and malicious classical post-processing units in quantum key distribution,* npj Quantum Information **5**, 14 (2019).

[31] J. Kilian, *Founding cryptography in oblivious transfer,* Theory of Computing (1988).

[32] T. Moran and M. Naor, Automata, Languages and Programming, edited by L. Caires, G. F. Italiano, L. Monteiro, C. Palamidessi, and M. Yung (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 285–297.

[33] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, Annual International Cryptology Conference (2009) pp. 408–427.

[34] D. Mayers, *Unconditionally secure quantum bit commitment is impossible,* Phys. Rev. Lett. **78**, 3414 (1997).

[35] H.-K. Lo and H. F. Chau, *Is quantum bit commitment really possible?* Phys. Rev. Lett. **78**, 3410 (1997).

[36] H.-K. Lo and H. F. Chau, *Why quantum bit commitment and ideal quantum coin tossing are impossible,* Physica D Nonlinear Phenomena **120**, 177 (1998), quant-ph/9711065 .

[37] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005. (2005) pp. 24–27.

[38] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Advances in Cryptology - CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) Chap. Secure Identification and QKD in the Bounded-Quantum-Storage Model, pp. 342–359.

[39] R. Konig, S. Wehner, and J. Wullschleger, *Unconditional security from noisy quantum storage,* IEEE Transactions on Information Theory **58**, 1962 (2012).

[40] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner, *Experimental implementation of bit commitment in the noisy-storage model,* Nature Communications **3**, 1326 (2012), arXiv:1205.3331 [quant-ph] .

[41] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, *An experimental implementation of oblivious transfer in the noisy storage model,* Nature Communications **5**, 3418 (2014), arXiv:1308.5098 [quant-ph] .

[42] A. Kent, *Quantum tagging for tags containing secret classical data,* Phys. Rev. A **84**, 022335 (2011).

[43] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Advances in Cryptology - CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings, edited by S. Halevi (Springer Berlin Heidelberg, Berlin, Heidelberg, 2009) pp. 391–407.

[44] H.-K. Lau and H.-K. Lo, *Insecurity of position-based quantum-cryptography protocols against entanglement attacks,* Phys. Rev. A **83**, 012322 (2011).

[45] A. Kent, W. J. Munro, and T. P. Spiller, *Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints,* Phys. Rev. A **84**, 012326 (2011).

[46] R. A. Malaney, *Location-dependent communications using quantum entanglement,* Phys. Rev. A **81**, 042319 (2010).

[47] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *Position-based quantum cryptography: Impossibility and constructions,* SIAM Journal on Computing **43**, 150 (2014), http://dx.doi.org/10.1137/130913687 .

[48] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, *A monogamy-of-entanglement game with applications to device-independent quantum cryptography,* New Journal of Physics **15**, 103002 (2013).

[49] J. Ribeiro and F. Grosshans, *A tight lower bound for the BB84-states quantum-position-verification protocol,* arXiv:1504.07171 (2015).

[50] S. Beigi and R. Koenig, *Simplified instantaneous non-local quantum computation with application to position-based cryptography,* arXiv:1101.1065 (2011).

3

DEVICE-INDEPENDENCE FOR TWO-PARTY CRYPTOGRAPHY AND POSITION VERIFICATION WITH MEMORYLESS DEVICES

Jérémy RIBEIRO, LE PHUC Thinh, Jędrzej KANIEWSKI, Jonas HELSEN, Stephanie WEHNER

I am easily satisfied with the very best.

Winston Churchill

Quantum communication has demonstrated its usefulness for quantum cryptography far beyond Quantum Key Distribution. One domain is Two-Party Cryptography, whose goal is to allow two parties who may not trust each other to solve joint tasks. Another interesting application is Position-Based Cryptography whose goal is to use the geographical location of an entity as its only identifying credential. Unfortunately, security of these protocols is not possible against an all powerful adversary. However, if we impose some realistic physical constraints on the adversary, there exist protocols for which security can be proven, but these so far relied on the knowledge of the quantum operations performed during the protocols. In this chapter we improve the device-independent security proofs of [1] for Two-Party Cryptography (with memoryless devices) and we add a security proof for device-independent Position Verification (also memoryless devices) under different physical constraints on the adversary. We assess the quality of the devices by observing a Bell violation and as for [1] security can be attained for any violation of the Clauser-Holt-Shimony-Horne inequality.

Parts of this chapter have been published in Phys. Rev. A, **97:022307**, 2018.

3.1. INTRODUCTION

In this chapter we will improve results from [1]. In particular we show that the Device-Independent (DI) quantum protocol for the Two-Party Cryptography (2PC) primitive called Weak String Erasure (WSE) is secure against an adversary holding a quantum memory twice as big as what is shown in [1]. We will then use this result to prove security of Position Verification (PV) by using the construction of [2].

As stated in Chapter 2 neither WSE not PV can be securely implemented if no assumption is made on the adversary. We will therefore work in the Noisy Quantum Storage Model (NQSM) [3–7] Here, the adversary is allowed to have an unlimited amount of classical storage, but his ability to store quantum information is limited. This is a relevant assumption since reliable storage of quantum information is challenging. Significantly, however, security can always be achieved by sending more qubits than the storage device can handle. Specifically, if we assume that the adversary can store at most r qubits, then security can be achieved by sending n qubits, where $r \leq n - O(\log n)$ [6], which is essentially optimal since no protocol can be secure if $r \geq n$ [8, 9]. The corresponding quantum protocols require only very simple quantum states and measurements – and no quantum storage – to be executed by the honest parties, and their feasibility has been demonstrated experimentally [10, 11]. It is known that the Noisy Quantum Storage Model allows protocols for tasks such as oblivious transfer, bit commitment, as well as Position-Based Cryptography [2, 12–15].

In all these security proofs, however, one assumes perfect knowledge of the quantum devices used in the protocol. In other words, we know precisely what measurements the devices make, or what quantum states they prepare. Here, we present a general method to prove security for 2PC and PV, in the Device-Independent (DI) model. There is a large body of work in DI QKD (see e.g. [16–18]), but in contrast there is hardly any work in DI 2PC. A protocol has been proposed by Silman [19] for bit commitment which does not make physical assumptions, and hence only achieved a weak primitive. First steps towards DI PV have also been made in [20], and for one-sided DI QKD in [14].

Achieving DI security for 2PC [1] and PV presents us new with challenges which require a different approach than what is known from QKD.

1. In QKD Alice and Bob trust each other, while Eve is an eavesdropper trying to break the protocol. As in DI QKD we will assume that the devices used in the protocol are made by the dishonest party.

2. In QKD, after Eve has prepared and given the devices – which she might be entangled with – to Alice and Bob, there is no more direct communication between them and Eve. On the contrary in two party cryptography, the dishonest party, who prepared the devices, will receive back quantum communication from these devices. This feature leads to different security analysis between DI QKD and DI 2PC, and also requires us to develop new proof techniques.

In this chapter, we present a method for improving the device-independent security of Two-Party Cryptography presented in [1] and add the device independent analysis of position-verification. We accomplish that by first reusing the device independent model of [1] (in particular they also use the memoryless device assumption for Alice's devices),

	[1]	**This chapter**
IID assumption on Alice's devices	yes	yes
Bound on P_{guess} (cf. (2.80))	$d\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n$	$\left(1-o(1)\right)\cdot\sqrt{d}\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n$
Memory size $r := \log(d)$ (in qubits) for which security can be achieved for a maximal Bell violation	$r \lesssim 0.22n$	$r \lesssim 0.45n$
Security for PV	no	yes
Adversary memory	reduction to classical adversary	deals with the memory directly
Jordan's Lemma	not used	reduction of dimensionality thanks to Jordan's Lemma
Absolute effective anti-commutator	used	used

Table 3.1: Comparison of the proof techniques used in [1] with those of this chapter. This chapter relates the security directly to the entanglement cost of the adversary's storage channel, however, we borrow concepts on how to test our quantum devices from the earlier work. Security is possible whenever $P_{\text{guess}} \leq 2^{-\alpha n}$ (see equation (2.80)) for some $\alpha > 0$, which depends on the dimension d of the adversary's storage device as well as the parameter ζ estimated during the Bell test. Our new analysis allows to prove security for a storage device that is at least twice as large as the one allowed by the previous results. We also know that an optimal bound on $r := \log(d)$ must satisfy $\frac{r}{n} \lesssim 1$ since attacks on WSE can be found if an adversary has a memory of $r = n + O(1)$ qubits.

and where to obtain DI security, Alice performs a Bell test on a subset of the quantum systems used in the protocol. It is an appealing feature of this analysis that security can be attained for any violation of the Clauser-Holt-Shimony-Horne (CHSH) inequality [21]. We then follow their reduction of the security of DI-WSE onto bounding the cheating probability on a "guessing game" (see Sec. 3.1.3).

In order to analyze the bound on the probability of winning the "guessing game" that we developed new techniques. The previous analysis [1] permitted to prove a bound on the cheating probability proportional to the dimension d of the adversary's quantum storage (see Table 3.1). To do so, the authors first reduced the dishonest party to a classical adversary thanks to an entropy inequality. Then they used the absolute effective anti-commutator to prove some uncertainty relations and finally lower bound some min-entropy (which is equivalent to upper-bound the cheating probability).

Here we deal directly with a quantum adversary, which permits us to prove security for an adversary quantum memory (of size r qubits) that is at least twice as large as in the previous analysis (see Table 3.1). We do not know if our new bound is optimal, we know however that the bound must satisfy $\frac{r}{n} \lesssim 1$. We would like to highlight the fact that finding an optimal bound is highly non trivial: even in the trusted scenario, it took several years to go from the first security proof for WSE [7] to a tight bound on the adversary memory size [6], and the techniques used cannot, as far as we know, be extended to the device independent scenario.

To overcome the difficulties induced by dealing directly with the adversary quantum

memory we had to use different tools (see Table 3.1). While the adversary can be fully general during the course of the protocol, we assume in this chapter that the devices he prepared earlier are memoryless (see IID-Assumption 2.4.2 of Chapter 2), which means that the devices behave in the same manner every time they are used. By analogy to classical random variables such devices are often referred to as IID devices (which stands for independent and identically distributed).

3.1.1. WEAK STRING ERASURE

To analyze 2PC protocols, we focus on a simpler primitive, namely Weak String Erasure (WSE) [7]. In this chapter we will use the formal security definition of (α,ϵ)-WSE proposed in [7] which we already give in Chapter 2 Definition 2.4.9.

One possible implementation of WSE [7] in case of honest parties and trusted devices is as follows. Alice prepares n EPR entangled pairs, measures randomly half of all the pairs in BB84 [22] bases $\Theta \in \{0,1\}^n$ and gets $X \in \{0,1\}^n$. At the same time, she sends the other half to honest Bob who measures it in some random bases $\Theta' \in \{0,1\}^n$ and gets $Z \in \{0,1\}^n$. As Bob does not know Θ, he has measured some of his states in the wrong basis, so the outcome bits corresponding to these measurements provide no information about Alice's outcome. At this stage, Bob does not know which of his measurement were done in the good basis and which were done in the wrong one. After Alice and Bob have waited for a duration Δt, Alice sends Θ to Bob. Bob can now compare Θ with Θ' and deduce the set $\mathscr{I} := \{k \in \{0,\dots,n\} : \Theta_k = \Theta'_k\}$ of indexes where Bob's bases are the same as Alice's ones. For these indexes we have $Z_k = X_k$ and Bob erases all the other bits. At this stage Bob holds $(\mathscr{I}, X_{\mathscr{I}})$, where $X_{\mathscr{I}}$ is the substring of X corresponding to the set $\mathscr{I}$.

In the device-independent version of the protocol Alice holds two devices: the main device and the testing device. Alice uses the main device to prepare and measure states, and the testing device to measure states. In the honest scenario, Alice first tests her devices by proceeding to a Bell test following Protocol 3.2.2 (in section 3.2.1), i.e. Alice checks that the states produced and measurements performed by the main device can be used to violate the CHSH inequality. Then Alice and Bob proceed as in the trusted device protocol.

In the dishonest Alice scenario, Alice is allowed to create Bob's measurement device, but we assume that the device is IID . If one hopes to be able to compose WSE to get other protocols such as Oblivious Transfer or Bit Commitment the above security condition is not enough. A stronger one (against dishonest Alice) is given by the following: Let $\hat{\rho}_{A'B}$ be the state after the execution of WSE, where $B := (\mathscr{I}, X_{\mathscr{I}})$ (X is the random variable for the bit string X and $X_{\mathscr{I}}$ is the random variable for the substring $X_{\mathscr{I}}$ of X) is held by Bob and A' is an arbitrary quantum register held by Alice. WSE is secure for an honest Bob if it exists a state $\tau_{A'\hat{X}\mathscr{I}}$ such that $\tau_{A'\hat{X}\mathscr{I}} = \tau_{A'\hat{X}} \otimes \frac{\mathbb{1}}{|\mathscr{I}|}$ and that for any given set $\mathscr{I}$, $\tau_{A'\hat{X}_{\mathscr{I}}\mathscr{I}} = \hat{\rho}_{A'X_{\mathscr{I}}\mathscr{I}}$. We leave open the question of whether this definition is strong enough to get any composability statement in the Device Independent setting [23].

In the dishonest Bob scenario, we can assume that it is Bob who created Alice's devices to gain extra information and compromise Alice's security. Consequently, at the very beginning of the protocol, Alice needs to test her devices (thanks to a Bell test). She

then uses the device n times to produce a bipartite state $\rho_{AB} = \sigma_{AB}^{\otimes n}$ (IID assumption), where σ_{AB} is an unknown but fixed state, measures the ρ_A part to get $X \in \{0,1\}^n$ and sends the ρ_B part to Bob. Bob can proceed to any kind of operation not necessarily IID on ρ_B and stores the outcome for the duration Δt to get a cq-state $\rho_{KB'}$. When he receives Θ from Alice he performs a general measurement on his cq-state which produces the guess $\tilde{X}$. Bob's cheating is considered successful if $\tilde{X} = X$. However, as his quantum storage is assumed to be bounded (or noisy) which impose a restriction on the possible state Bob can hold, and permits us to show that,

- **WSE is secure:** for Alice against dishonest Bob who holds a bounded (or noisy) storage device of size up to $r \lesssim 0.45n$ (n being the number rounds of the protocol) and is allowed to create the honest party's devices (but these devices have to be memoryless), and for Bob against dishonest Alice. This improves the previous known security proof [1] where security was shown for $r \lesssim 0.22n$.

To establish this result we proceeded in a similar way as in [1], that's to say we reduce the security of WSE to a bound on the probability of winning what we call a "guessing game". The main difference between our approach and the one presented in [1] is that we introduce new techniques to analyze this guessing game (more details about the guessing game are provided in section 3.1.3). As mentioned above our analysis improves the size of (dishonest) Bob's quantum memory that can be securely tolerated by a DI-WSE protocol. More precisely we show that the protocol is secure as long as the size (measured in qubits) r of Bob's quantum memory is $r \lesssim 0.45n$ (where n the number of round of the protocol), while [1] shows security for $r \lesssim 0.22n$.

The detailed Weak String Erasure protocol is presented in section 3.3.1 (Protocol 3.3.1). The precise formal result is presented in the Corollary 3.3.3 in section 3.3.1.

3.1.2. POSITION VERIFICATION

We use the security proof of WSE together with the security reduction of [2] to show device independent security for PV.

Note that to make the security reduction from PV to WSE we use a model introduced in [2] where the dishonest provers do not have access to quantum channels but only to limited entanglement and arbitrary classical communication. However they can use teleportation with their entanglement to recreate a quantum channel. Therefore this model is in fact equivalent as to considering dishonest provers having access to limited entanglement and limited quantum channels (and arbitrary classical communication). Moreover if the dishonest provers have access to arbitrary quantum channels they can use them to prepare and store an arbitrary amount of entanglement before the protocol starts as shown in Fig. 3.4 in Technical Details section 3.5.3 which would lead to known attacks.

As security of PV can be reduced to the security of WSE, we prove that

- **PV is secure** against adversaries who share a "noisy" entangled state and who cannot use quantum communication but are allowed to create the honest party's devices (these devices have to be memoryless).

The precise formal result is presented in Lemma 3.3.11, and this follows from a technical result informally presented in the next section.

3.1.3. METHODS

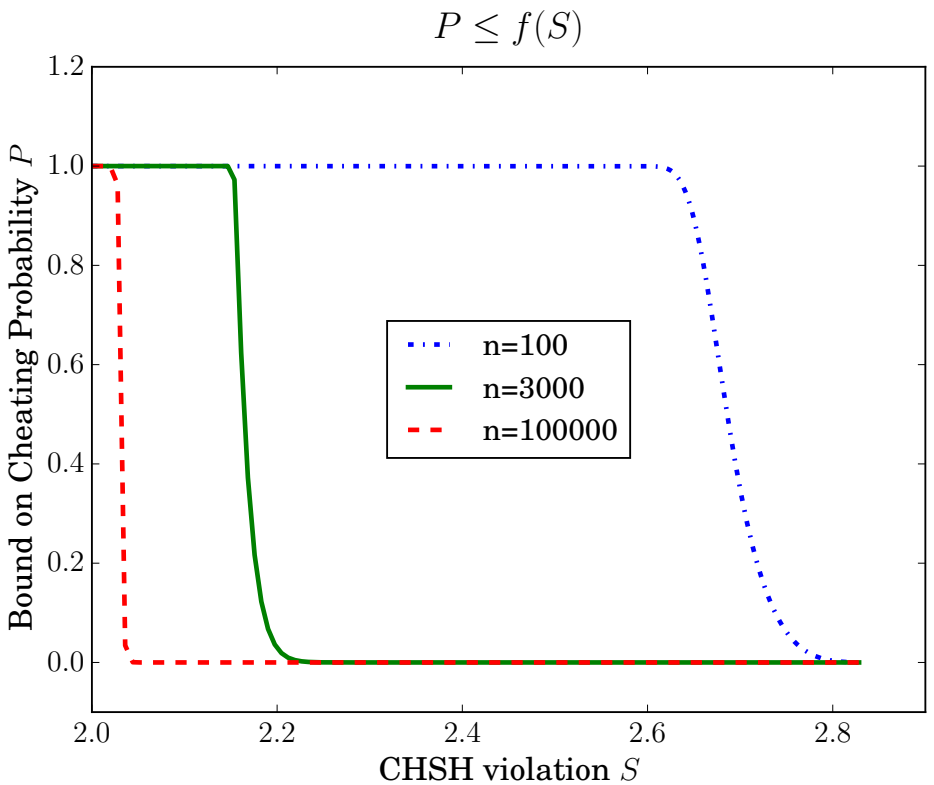


Figure 3.1: Security is possible for any violation of the CHSH inequality, but depending on the violation we need to send a larger number of qubits n.

In order to prove DI security for Weak String Erasure and Position Verification, we analyze a related task known as the post-measurement guessing game. This is a two-player game where Alice plays against Bob. Alice inputs a bit string into her main device and receives an output string; Bob wins the game if he guesses correctly the output of Alice's device given his knowledge of Alice's input.

In the DI version, Alice demands that she has another test device different from her main device and dishonest Bob is allowed to create these two devices of Alice (Fig. 3.2). Alice can use these two devices to perform a Bell test (CHSH game), which certifies the quality of the devices. Having tested her devices, Alice uses the main device to prepare a bipartite (arbitrary) state and measures half of it by inputting $\Theta \in \{0,1\}^n$ in her main device, gets an outcome $X \in \{0,1\}^n$, and sends the other part of the quantum system to Bob. Later she sends him the input she used to perform her measurements. Once Bob has received all information he has to guess Alice's measurement outcome X.

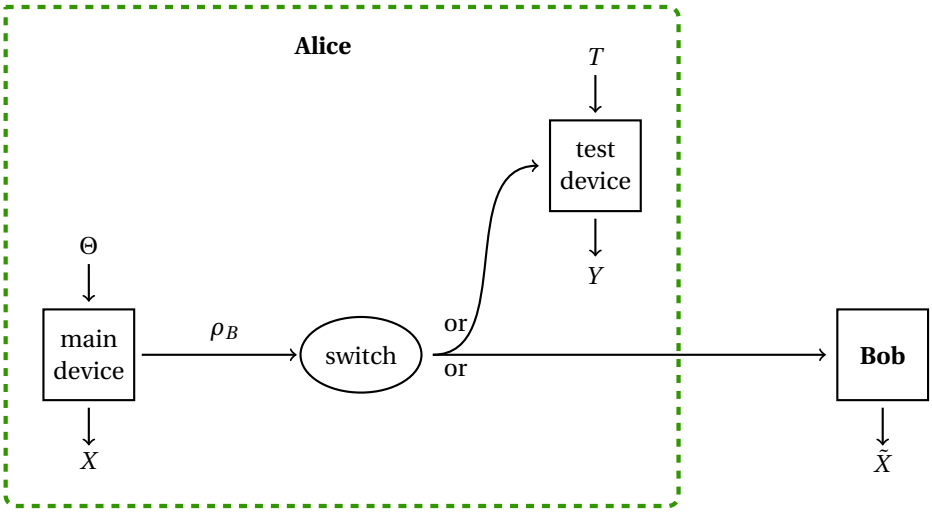


Figure 3.2: Alice is in possession of two devices prepared by Bob: The "main device" permits Alice to prepare a bipartite state ρ_{AB} and measure the ρ_A part of it according to a list of bases $\Theta \in \{0,1\}^n$. The "testing device" measures according to a list of bases $t \in \{0,1\}^m$. These two devices are assumed to be memoryless (or IID). A dishonest Bob is assumed to be only limited by the dimension of his quantum memory, so he is allowed to make arbitrary measurements on states of dimension at most d.

The main device prepares a bipartite state $\rho_{AB} = \sigma_{AB}^{\otimes n}$ (the tensor form follows the IID assumption), one part ρ_A is measured by the main device, with the measurement settings specified by a random bit string $\Theta \in \{0,1\}^n$, to produce the bit string $X \in \{0,1\}^n$. The other part ρ_B of the state is sent to a switch that Alice controls. As the devices are memoryless, Alice can first test her devices, and so sets her switch such that the system B is sent to the testing device. She then repeatedly performs the CHSH test to estimate the violation. After that she sets her switch so that the system B is sent to Bob. Bob's goal is to guess Alice's output X, i.e. he wants to achieve $\tilde{X} = X$.

To find a bound on Bob's winning probability, we have to assume that Bob has limited quantum storage or else he wins with certainty: he would just have to store the quantum system until he receives the bases Θ and then he can measure his system in those bases. As a first step towards security against fully uncharacterized devices, we assume for now that all devices used by Alice are memoryless or IID, so they behave in the same way each time Alice uses them. This implies that Alice's measurement operators are a tensor product of binary measurement operators, and the state she prepares is also of product form. This memoryless assumption also permits Alice to perform the Bell test before the actual guessing game, and from this test, to estimate an upper bound $\zeta := \frac{S}{4}\sqrt{8-S^2}$ on a quantity we call the effective absolute anti-commutator of Alice's measurement denoted ϵ_+ [1], where S is the left hand side of the CHSH inequality. Since ϵ_+ is always larger than the effective anti-commutator, one can show that it gives rise to strong uncertainty relations [24].

Despite the memoryless assumption (on Alice side only), the problem remains hard. Indeed, we cannot use techniques coming from DI QKD, since in QKD the honest parties do not send back quantum information to the eavesdropper, in contrast to the guessing

game. The analysis must be different. As we do not know what Alice's measurements are, there is no limitation on the dimension on which Alice's devices act, so we cannot use bounds depending on the dimensionality of Alice's states or measurements. Moreover we have to express the absolute anti-commutator ϵ_+ of Alice's measurement, in a way that allows us to relate it to Bob's guessing probability. In the previous work on DI-WSE [1], the authors reduced the problem to proving security against a classical adversary (see Table 3.1 for a more detailed comparison between the works). This reduction leads to a bound which is proportional to d, the dimension of the adversary's quantum memory. To improve this bound we must deal with Bob's measurement, which are fully general though acting on a space of dimension at most d.

We overcome these difficulties thanks to Jordan's Lemma [25, 26], which permits to block diagonalize Alice's measurement and reduces the dimensionality of these measurements into a list of qubit measurements. The price to pay is that we lose the "identically distributed" part of the IID assumption on these qubit measurements. Jordan's Lemma permits us to express the absolute effective anti-commutator in an adapted form, such that we can link it to the guessing probability of Bob. Finally we prove the following.

- **Main technical result:** Assuming Alice's devices are memoryless, and Bob has a noisy storage device, there is a DI upper-bound on the success probability of Bob in the guessing game, which decays exponentially in n, the length of Alice's measurement outcomes $X \in \{0,1\}^n$ which coincides here with the number of qubits exchanged in the honest execution protocol. This bound scales as $\sqrt{d}$ (where d is the dimension of the quantum system Bob can store) and holds for *any* CHSH violation, *i.e.* $\forall S \in]2, 2\sqrt{2}]$ (see Fig. 3.1). This improves the previous known bound by a factor $\sqrt{d}$.

The precise formal statement is given in Theorem 3.2.8.

From this result follows the DI security of WSE and PV. Indeed any attack on WSE can be viewed as a guessing game where Bob tries to guess Alice's complete string X. Likewise in the case of PV we can see any attack as a guessing game: the dishonest provers have to guess V_1's outcome, and one can map the operations they used to the guessing game and hence show that these operations would permit Bob to win the guessing game. This implies that the cheating probability in PV is lower than that of the guessing game. This statement has been shown in [2] (the remapping was done between attacks on PV and attacks on WSE, but it is essentially the same since any attack on WSE can be seen as a guessing game).

3.2. DEVICE-INDEPENDENT GUESSING GAME

3.2.1. PRELIMINARIES

In this chapter, because we heavily use the operator norm (Schatten ∞-norm) $\|\cdot\|_\infty$ we will simply denote it by $\|\cdot\|$ without any subscript. Some useful properties of the operator norms are $\|L\|^2 = \|L^\dagger L\| = \|LL^\dagger\|$ for all $L \in \mathscr{L}(\mathscr{H})$ and if $A, B \in \mathscr{P}(\mathscr{H})$ such that $A \geq B$ then $\|A\| \geq \|B\|$. Moreover, whenever $A, B, L \in \mathscr{L}(\mathscr{H})$ and $A^\dagger A \geq B^\dagger B$ then $\|AL\| \geq \|BL\|$ [14, Lemma 1].

Vector p-norms induce the corresponding operator p-norms, which we denote as $\|\cdot\|_p^{\mathrm{I}}$ to distinguish them from Schatten p-norms. They are defined as

$$\|A\|_p^{\mathrm{I}} = \sup_{x\neq 0} \frac{\|Ax\|_p}{\|x\|_p}. \tag{3.1}$$

In the proof of a technical Lemma in the Technical Details section, we will need the induced 1-norm and ∞-norm

$$\|A\|_1^{\mathrm{I}} = \max_{1\leq j\leq n} \sum_{i=1}^{m} |a_{ij}| \qquad \text{and} \qquad \|A\|_\infty^{\mathrm{I}} = \max_{1\leq i\leq m} \sum_{j=1}^{n} |a_{ij}| \tag{3.2}$$

which can be seen as the maximum absolute column sum and maximum absolute row sum, respectively, and where m and n are the maximum row and column indexes respectively. Note that the induced 2-norm and the operator norm are the same $\|\cdot\|_2^I = \|\cdot\|$.

For a bit string $x \in \{0,1\}^n$, $|x|$ denotes its length n and the Hamming weight $w_H(x)$ is the number of 1's in x. For $x, y \in \{0,1\}^n$ the Hamming distance is defined as $d_H(x,y) := w_H(x \oplus y)$.

If $\mathscr{I}$ is a subset of $[n]$ then by $x_{\mathscr{I}}$ we mean the substring of x with indices $\mathscr{I}$.

$E^{(1)}_{\mathrm{C,LOCC}}(\rho_{AB})$ is the one shot entanglement cost to create a bipartite state ρ_{AB} from a maximally entangled state using only local operations and classical communication. It is formally defined as

$$E^{(1)}_{\mathrm{C,LOCC}}(\rho) := \min_{M,\Lambda} \left\{ \log(M) : \Lambda(\Psi_M^{\bar{A}\bar{B}}) = \rho_{AB}, \Lambda \in \mathrm{LOCC}, M \in \mathbb{N} \right\}, \tag{3.3}$$

where $\Psi_M^{\bar{A}\bar{B}}$ is a maximally entangled state of dimension M

$$\Psi_M^{\bar{A}\bar{B}} := |\Psi_M^{\bar{A}\bar{B}}\rangle\langle\Psi_M^{\bar{A}\bar{B}}|, \qquad |\Psi_M^{\bar{A}\bar{B}}\rangle := \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |i^{\bar{A}}\rangle |i^{\bar{B}}\rangle. \tag{3.4}$$

Similarly, we have $E_C^{(1)}(\mathscr{E})$ [27, Definition 10] is the one shot entanglement cost to simulate a channel $\mathscr{E} : \mathscr{L}(\mathscr{H}_A) \to \mathscr{L}(\mathscr{H}_B)$ using LOCC and preshared entanglement:

$$E_C^{(1)}(\mathscr{E}) := \min_{M,\Lambda} \left\{ \log(M) : \forall \rho_A \in \mathscr{L}(\mathscr{H}_A),\ \Lambda(\rho_A \otimes \Psi_M^{\bar{A}\bar{B}}) = \mathscr{E}(\rho_A) \right\} \tag{3.5}$$

where Λ is a LOCC with $A\bar{A} \to 0$ (no output) on Alice's side and $\bar{B} \to B$ on Bob's side, and $M \in \mathbb{N}$. Note that we require a single LOCC map to simulate the effect of the channel $\mathscr{E}$ so Λ must be independent of ρ_A.

In this chapter, we will call binary observable any hermitian operator A such that $A^2 \leq \mathbb{1}$.

MODELS AND ASSUMPTIONS

In this section we explain in detail the assumptions imposed on the model, which are motivated by considerations on the WSE and PV protocols and our IID constraint.

Assumptions 3.2.1. *These are the assumptions on our device-independent guessing game:*

1. *In device-independent protocols, the security cannot rely on the knowledge we have about the devices used by the honest party (the inner workings are unknown). These devices may even be maliciously prepared by the dishonest party to compromise security.*

   - *Thus in this context, dishonest Bob is allowed to create the two devices of honest Alice: the main device and the testing device. These devices are assumed to be memoryless (or IID), which means that they behave in the same way every time Alice uses them. In other words, the measurements made by the devices in one round of usage depend only on Alice's input in this round (and not on previous rounds), and the state $\rho_{AB} = \sigma_{AB}^{\otimes n}$ created by her device has a tensor product form where σ_{AB} may be chosen by Bob. The testing device is used in the testing protocol 3.2.2.*
   - *Similarly dishonest Alice can prepare honest Bob's measurement device. It is also assumed to be IID .*

2. *When Bob receives his state ρ_B from Alice, we allow him to perform any quantum operation on it. After the operation the global state can be written as $\rho_{AB'K}$ where Alice's part ρ_A has a tensor product form, and $\rho_{B'K}$ is an arbitrary qc-state held by Bob such that $|B'| \leq d$ (see assumptions 3.2.5).*

3. *Alice can test her devices before using them in the protocol as they are memoryless. We describe the testing procedure in detail in the following Protocol 3.2.2.*

The testing procedure aims to estimate how much the two binary measurements made by Alice's main device are incompatible given the prepared state. This is accomplished by measuring how much the main and test devices can violate the CHSH inequality.

Protocol 3.2.2. *Let A_0, A_1 be the two binary observables of Alice's main measurement device, and T_0, T_1 be the two binary observables of her testing device.*

1. *Alice creates a bipartite state ρ_{AB} using her main device.*
2. *She sends the B subsystems in state ρ_B to her testing device and statistically estimates $S := \mathrm{tr}(W\rho_{AB})$, where W is the CHSH operator defined as*

$$W := A_0 \otimes T_0 + A_0 \otimes T_1 + A_1 \otimes T_0 - A_1 \otimes T_1. \tag{3.6}$$

The test is said to be successful if $S > 2$.

The following Lemma 3.2.4 shows that this testing procedure permits Alice to estimate the absolute effective anti-commutator defined as follows.

Definition 3.2.3. *Let ρ_{AB} be a bipartite state then for two binary measurements with POVM elements $\{P_0^0, P_1^0\}$ and $\{P_0^1, P_1^1\}$, we define the absolute effective anti-commutator*

$$\epsilon_+ := \frac{1}{2}\,\mathrm{tr}(|\{A_0, A_1\}|\rho_A) \tag{3.7}$$

where $A_0 := P_0^0 - P_1^0$ and $A_1 := P_0^1 - P_1^1$, $\{A_0, A_1\} := A_0A_1 + A_1A_0$, and $\rho_A := \mathrm{tr}_A(\rho_{AB})$.

Lemma 3.2.4 (Proposition 2 of [1])**.** *Let $\rho_{AT} \in \mathscr{S}(\mathscr{H}_{AT})$ and let A_0, A_1 and T_0, T_1 be binary observables on subsystem A and T, respectively, achieving $\mathrm{tr}(W\rho_{AT}) =: S$ for $S \geq 2$ with W being the* CHSH *operator. The absolute effective anti-commutator on Alice's side satisfies*

$$\epsilon_+ \leq \frac{S}{4}\sqrt{8 - S^2} =: \zeta \in [0, 1]. \tag{3.8}$$

This estimation ζ of ϵ_+ is central to our proof. Indeed the security bounds we derive below rely on the fact that $\zeta < 1$, which means that any Bell violation in the testing procedure leads to security on WSE and PV. In other words it is enough for Alice to estimate $\zeta < 1$ in the testing procedure to be sure that her devices permit her to execute the protocols (PV or WSE) securely under

Assumptions 3.2.5. *We assume that the adversarial or dishonest party cannot have access to an unlimited and perfect quantum memory or quantum entanglement. More specifically,*

1. *In the guessing game and in WSE, the adversary will either have a bounded storage or a noisy storage.*

2. *In PV, the adversary will either have access to bounded entanglement or noisy entanglement.*

3.2.2. GUESSING GAMES AND RESULTS

In this section, we describe and analyze the perfect and imperfect guessing games. As the name suggests, the winning condition of the perfect guessing game is more strict than that of the imperfect guessing game. Bounding the probability that Bob wins the perfect guessing game is the first step to bounding the probability that he wins the more general imperfect guessing game. The motivation behind the analysis of the imperfect guessing game is to prove security of WSE and PV even if the protocol is made robust to noise, which is inherent to any experimental implementation.

PERFECT GUESSING GAME

We state here a formal description of the perfect guessing game.

Protocol 3.2.6. *(Perfect guessing game)*
Alice runs Protocol 3.2.2, if the devices pass the test successfully then she gets an estimate $\zeta < 1$ that upper bounds the effective anti-commutator associated with her measurement device and the state produced by the source. If the devices do not pass the test Alice aborts. After this testing phase Alice and Bob proceed as follows.

1. *Alice creates n identical bipartite states, chooses uniformly at random a string $\Theta \in \{0,1\}^n$ and measures her k^{th} register using her main device with input Θ_k to obtain an outcome X_k. This measurement produces an outcome string $X \in \{0,1\}^n$. At the same time she gives all the B parts to Bob.*
2. *Alice waits for a duration Δt before sending her string Θ to Bob.*
3. *Bob tries to guess X using Θ and all his available information. In other words, Bob produces an output Y and the (perfect) winning condition is $Y = X$.*

Let us analyze this game from the perspective of quantum theory and under the IID assumption 3.2.1. We will go through each step of the protocol again but with added descriptive comments. In the first step of the protocol, using the device n times, Alice produces a bipartite state $\rho_{AB} = \sigma_{AB}^{\otimes n}$, and chooses the measurement setting Θ to measure $\rho_A = \sigma_A^{\otimes n}$ with the POVM $\{P_x^\theta = \bigotimes_k P_{x_k}^{\theta_k} : x \in \{0,1\}^n\}$. This measurement can be seen as a tensor product of two binary measurements $\{P_0^0, P_1^0\}$ and $\{P_0^1, P_1^1\}$ because of the IID assumption. At the same time, Alice sends to Bob a state which has IID form $\rho_B = \sigma_B^{\otimes n}$ due to our assumption. Then, the waiting time enforces the Noisy Quantum Storage Model: Bob is allowed to perform any quantum operation to transform B to $B'K$ where B' is his quantum memory of dimension d and K is his (unbounded) classical memory. Bob is allowed to perform any measurement on his system B', as advised by K and Θ and his information about the state (since he prepares the devices), in order to guess X. Note that for an honest implementation of the protocol, Alice does not need quantum memory, which makes the protocol easy to implement.

As the security of the protocols WSE and PV are expressed in terms of cheating probability (or equivalently in terms of min-entropy), we are here interested in the probability that Bob wins the guessing game. Indeed if this probability is low, then it means that the probability that the two protocols PV and WSE can be cheated is low as well. To win the guessing game Bob needs first to pass the testing phase of Protocol 6 described in Protocol 2. Therefore we will consider that Bob passes the tests with some value $\zeta < 1$. This value ζ constrains the possible measurement devices and source that Alice can have. Let $\mathfrak{P}(\zeta)$ be the set of possible main measurement device and source Alice can have conditioned on the fact that Bob has successfully passed the testing procedure with value $\zeta < 1$. More formally,

$$\mathfrak{P}(\zeta) := \left\{\left(\sigma_{AB}, \{P_0^0, P_1^0\}, \{P_0^1, P_1^1\}\right) \in \mathscr{S}(\mathscr{H}_{AB}) \times \mathscr{P}(\mathscr{H}_A)^2 \times \mathscr{P}(\mathscr{H}_A)^2 : \forall i \in \{0,1\},\, P_0^i + P_1^i = \mathbb{1}_A, \epsilon_+ \leq \zeta\right\}.$$

Then under Assumptions 3.2.1 and 3.2.5, and for devices $\Gamma \in \mathfrak{P}(\zeta)$, Bob's guessing prob-

ability is defined as,

$$\lambda(n,d,\Gamma) := \max_{\substack{\rho_{AB'K} \\ \text{qqc} \\ \dim(\mathscr{H}_{B'})\leq d}} \max_{\{\mathscr{F}^\theta\}} \operatorname{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} P_x^\theta \otimes F_x^\theta \quad \rho_{AB'K}\right), \tag{3.9}$$

where the first maximization is over all qqc-states $\rho_{AB'K}$ such that $\operatorname{tr}_{B'K}(\rho_{AB'K}) = \operatorname{tr}_B(\rho_{AB}) = \rho_A$, where $\rho_{AB} = \sigma_{AB}^{\otimes n}$ is the initial state as defined above and P_x^θ are the measurement operators of Alice as mentioned above. F_x^θ are arbitrary measurement operators of Bob acting on $B'K$ register. Note that the state $\rho_{B'K} := \operatorname{tr}_A(\rho_{AB'K})$ is the qc-state that Bob gets after a quantum operation on the initial state $\rho_B = \sigma_B^{\otimes n}$ sent to him by Alice. The second maximization is a short hand for 2^n separate maximizations: for each θ we pick the POVM $\mathscr{F}^\theta = \{F_x^\theta : x \in \{0,1\}^n\}$ which maximizes the sum over x.

The following Lemma, whose proof is presented in the Technical Details section, gives a bound on the probability $\lambda(n,d,\Gamma)$.

Lemma 3.2.7 (Key Lemma)**.** *In a perfect guessing game where the adversary holds a bounded quantum memory of dimension at most d, we have*

$$\lambda(n,d,\Gamma) \leq \sqrt{d}\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n - \sum_{k=0}^{t}\binom{n}{k}2^{-n}\left(\sqrt{d}\left(\frac{1+\zeta}{2}\right)^{k/2}-1\right) =: B(n,d,\zeta) \tag{3.10}$$

where t is defined as

$$t = \left\lfloor -\log d \cdot \left[\log\left(\frac{1+\zeta}{2}\right)\right]^{-1}\right\rfloor, \tag{3.11}$$

which implies that,

$$\forall k\colon\ 0\leq k\leq t,\ \left(\sqrt{d}\left(\frac{1+\zeta}{2}\right)^{k/2}-1\right)\geq 0.$$

Observe that by forgetting the second term of $B(n,d,\zeta)$ that is always negative, one can check that when the size of Bob's memory $r := \log(d) = \kappa n$ the bound $B(n,2^r,\zeta)$ decays exponentially when $n\to\infty$ (and for constant $\zeta<1$) as long as $\kappa < -2\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)\underbrace{\approx 0.45}_{\text{for }\zeta=0}$ which is an improvement of a factor 2 for the size of Bob's memory compare to [1].

IMPERFECT GUESSING GAME

The consideration of imperfect guessing game is motivated by noise in experimental realizations of any protocols. Allowing noise between provers and verifiers in WSE or PQV allows these protocols to be implemented with current state-of-the-art quantum technologies.

Formally, the imperfect guessing game consists of exactly the same steps as the guessing game discussed in the previous section, except for the winning condition of Bob. Unlike the guessing game's strict winning condition $y = x$, in the imperfect guessing game

Bob wins if his guess y is such that $d_H(x,y) \leq \gamma n$ for $\gamma \in [0,1[$, where $d_H(\cdot,\cdot)$ is the Hamming distance. Formally

$$\lambda_{\text{ip}}(n,d,\Gamma,\gamma) := \max_{\substack{\rho_{AB'K} \\ \text{qqc} \\ \dim(\mathscr{H}_{B'})\leq d}} \max_{\{\mathscr{F}^\theta\}} \text{tr}\Big(2^{-n} \sum_{\theta,x\in\{0,1\}^n} \sum_{\substack{y\in\{0,1\}^n \\ d_H(x,y)\leq\gamma n}} P_x^\theta \otimes F_y^\theta \quad \rho_{AB'K}\Big), \tag{3.12}$$

where $\Gamma \in \mathfrak{P}(\zeta)$ (see eq. (3.9)), and γ can be understood as the maximum quantum bit error rate (QBER) allowed in the protocol. We recover the perfect guessing game by taking $\gamma = 0$.

One of our main results in this chapter is the following

Theorem 3.2.8 (Main Theorem)**.** *For an imperfect guessing game with the maximum "QBER" allowed $\gamma \in [0,1/2]$, where Bob holds a noisy storage device $\mathscr{E}$ such that $E_C^{(1)}(\mathscr{E}) \leq \log(d)$, the winning probability of Bob*

$$\lambda_{\text{ip}}(n,d,\Gamma,\gamma) \leq 2^{h(\gamma)n} B(n,d,\zeta) =: B'(n,d,\zeta,\gamma) \tag{3.13}$$

where $h(\cdot)$ is the binary entropy and $B(n,d,\zeta)$ is the bound defined in Lemma 3.2.7.

Proof. (sketch) We first look at the imperfect guessing game in the Bounded Quantum Storage Model where the dimension of B' is bounded by d. To obtain an upper bound on $\lambda_{\text{ip}}(n,d,\Gamma,\gamma)$ we note that

$$\text{tr}\Big(\sum_{x\in\{0,1\}^n} \sum_{\substack{y\in\{0,1\}^n \\ d_H(x,y)\leq\gamma n}} P_x^\theta \otimes F_y^\theta \quad \rho_{AB'K}\Big) = \text{tr}\Big(\sum_{x\in\{0,1\}^n} \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} P_x^\theta \otimes F_{x\oplus z}^\theta \quad \rho_{AB'K}\Big) \tag{3.14}$$

$$= \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} \text{tr}\Big(\sum_{x\in\{0,1\}^n} P_x^\theta \otimes F_{x\oplus z}^\theta \quad \rho_{AB'K}\Big). \tag{3.15}$$

Then combining the previous remark with (3.12) we have,

$$\lambda_{\text{ip}}(n,d,\Gamma,\gamma) \leq \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} \max_{\substack{\rho_{AB'K} \\ \text{qqc} \\ \dim(\mathscr{H}_{B'})\leq d}} \max_{\{\mathscr{F}^\theta\}} \text{tr}\Big(\sum_{x\in\{0,1\}^n} P_x^\theta \otimes F_{x\oplus z}^\theta \quad \rho_{AB'K}\Big) \tag{3.16}$$

where the first maximization is over all qqc-states compatible with the marginal on Alice. Note that all the trace terms in the sum are equivalent since z only permutes Bob's measurement operators. Then by using the Key Lemma 3.2.7 to bound each term of the sum over z we can write,

$$\lambda_{\text{ip}}(n,d,\Gamma,\gamma) \leq B(n,d,\zeta) \times \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} 1 \tag{3.17}$$

$$= B(n,d,\zeta) \times \sum_{k=0}^{\lfloor\gamma n\rfloor} \binom{n}{i} \tag{3.18}$$

To proceed further, we assume that $\gamma < 1/2$ so $\lfloor \gamma n \rfloor$ is bounded by $\lfloor n/2 \rfloor$ and therefore by Lemma 25 of [6] we can bound the binomial sum by the binary entropy function $h(\cdot)$ so that,

$$\lambda_{\text{ip}}(n,d,\Gamma) \leq 2^{h(\gamma)n} \cdot B(n,d,\zeta) =: B'(n,d,\zeta,\gamma). \tag{3.19}$$

It remains to extend this bound to an adversary who holds a noisy memory $\mathscr{E}$ such that the one-shot entanglement cost satisfies $E_C^{(1)}(\mathscr{E}) \leq \log(d)$. Indeed, by definition of the one-shot entanglement cost [27], the above condition means that $\mathscr{E}$ can be simulated by the identity channel $\mathbb{1}_d$. Then all strategies achievable with $\mathscr{E}$ are achievable with $\mathbb{1}_d$, particularly the strategy which maximizes the probability of winning in the Bounded Quantum Storage Model. This proves the Theorem. □

The bound on the winning probability of the imperfect guessing game also decays exponentially in n for suitably chosen parameters.

Lemma 3.2.9. *If the maximum QBER allowed γ satisfies the following conditions*

$$\gamma \leq 1/2 \tag{3.20}$$

$$h(\gamma) < -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right) \tag{3.21}$$

then $B'(n,d,\zeta,\gamma)$ decays exponentially in n, when $n \to \infty$ and d,ζ are fixed.

Note that it is always possible to have a γ which satisfies these conditions since the right hand sides of the inequalities are strictly positive.

Proof. First note that $B'(n,d,\zeta,\gamma) = 2^{h(\gamma)n} B(n,d,\zeta)$. According to Lemma 3.2.7, $B(n,d,\zeta) = \sqrt{d}\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n - O(n^t \cdot 2^{-n})$ It is now straightforward to see that the condition on γ implies the exponential decay of $B'(n,d,\zeta,\gamma)$. □

3.3. APPLICATIONS

Following the analysis of [1] the bound on the winning probability of the guessing game can be applied to prove the security of several two-party cryptographic protocols. Here we will apply it to prove the security of Weak String Erasure and Position Verification. For the first protocol, we can directly consider an attack on WSE as an attack on the guessing game. For the second protocol, as the security of PV can be reduced to the security of WSE [2], we also get a security proof for PV.

3.3.1. DEVICE-INDEPENDENT WEAK STRING ERASURE

This section is divided into two subsections.

1. In the first we prove security of DI-WSE in the Noisy Quantum Storage Model (see Corollary 3.3.3).

2. The second part aims to make the transition between WSE and PV since security of (DI) PV can be derived easily from the security of (DI) WSE in the "noisy entanglement" model [6]. Therefore we explain the (DI) WSE protocol in the "noisy entanglement" model that is a variant of WSE in the Noisy Quantum Storage Model, and we show security in this model.

(α,ε=0)-WSE IN THE NOISY QUANTUM STORAGE MODEL

Let the two protagonists of (α,ϵ)-WSE be Alice and Bob. The goal of this cryptographic primitive is that at the end of its execution Alice holds a random bit string X and Bob holds a random substring of X called $X_{\mathscr{I}}$. We can view this $X_{\mathscr{I}}$ as X where we have randomly erased some bits, hence the name WSE (Protocol 3.3.1). For a formal definition of (α,ϵ)-WSE we refer to [7].

Protocol 3.3.1 (Weak String Erasure)**.** *In the case where Alice and Bob are honest, the protocol is executed as follows:*

1. *Alice tests her devices following the testing protocol 3.2.2 and obtains ζ, an estimate of an upper bound on the absolute effective anti-commutator.*
2. *Alice creates n identical bipartite states σ_{AB}. She chooses uniformly at random a string $\Theta \in \{0,1\}^n$ and measures her part of the k^{th} register by inputting it and Θ_k to her measurement device to get an outcome X_k. This process generates an outcome string $X \in \{0,1\}^n$. At the same time she sends all the B registers of σ_{AB} to Bob.*
3. *Bob chooses uniformly at random $\Theta' \in \{0,1\}^n$, and measures his registers in the same manner as Alice to get an outcome string $X' \in \{0,1\}^n$.*
4. *Alice waits for a duration Δt before sending Θ to Bob.*
5. *Bob determines the index set $\mathscr{I} := \{k \in [n] : \Theta'_k = \Theta_k\}$, and obtains the corresponding substring $X'_{\mathscr{I}}$.*

At the end of the protocol Alice holds X and Bob holds $(\mathscr{I}, X'_{\mathscr{I}})$. It can be easily checked that in the ideal implementation, $X'_{\mathscr{I}}$ is a substring of X so Bob does not know the full X and Alice does not know $\mathscr{I}$.

SECURITY FOR HONEST BOB

Let ρ_{AB} be the state that dishonest Alice produces at the beginning of the protocol, $\hat{\rho}_{A'B}$ the state after the execution of WSE, where $B := (\mathscr{I}, X_{\mathscr{I}})$ (X is the random variable for the bit string X and $X_{\mathscr{I}}$ is the random variable for the substring $X_{\mathscr{I}}$ of X) is held by Bob and A is an arbitrary quantum register held by Alice.

WSE is secure for an honest Bob if it exists a (ideal) state $\tau_{A\hat{X}\mathscr{I}}$ such that $\tau_{A'\hat{X}\mathscr{I}} = \tau_{A\hat{X}} \otimes \frac{\mathbb{1}}{|\mathscr{I}|}$ and for any given $\mathscr{I}$, $\tau_{A\hat{X}_{\mathscr{I}}\mathscr{I}} = \hat{\rho}_{A'X_{\mathscr{I}}\mathscr{I}}$.

Let us now take $\tau_{A'\hat{X}\mathscr{I}}$ as being the state we would obtain after the protocol 3.3.1 if Bob (in some imaginary scenario), instead of measuring the B part of state ρ_{AB} in his chosen bases Θ', measured it in Alice's bases Θ while Alice performs her "cheating" operations (an arbitrary CPTP map from A to A') on the A system (all the other part of the protocol being the same).

We show in the following theorem that this definition for the state $\tau_{A\hat{X}_{\mathscr{I}}\mathscr{I}}$ satisfies the two properties described above, and hence that the protocol 3.3.1 implements a secure WSE for Bob.

Theorem 3.3.2. *The protocol 3.3.1 realizes a secure WSE for Bob. Indeed the state $\tau_{A'\hat{X}\mathscr{I}}$ defined above satisfies the two required relations:*

- $\tau_{A'\hat{X}_{\mathscr{I}}\mathscr{I}} = \hat{\rho}_{A'X'_{\mathscr{I}}\mathscr{I}}$,
- $\tau_{A'\hat{X}\mathscr{I}} = \tau_{A'\hat{X}} \otimes \frac{\mathbb{1}}{|\mathscr{I}|}$,

where $\hat{\rho}_{A'X'_{\mathscr{I}}\mathscr{I}}$ is the real state produced after the excution of WSE.

Proof. Let us first see why $\tau_{A'\hat{X}\mathscr{I}} = \tau_{A'\hat{X}} \otimes \frac{\mathbb{1}}{|\mathscr{I}|}$. For that let us consider the hypothetical scenario. By definition of $\mathscr{I}$, Alice is ignorant about $\mathscr{I}$ if and only if she is ignorant about $\Theta \oplus \Theta'$. Because she knows Θ, she is ignorant about $\mathscr{I}$ if and only if she is ignorant about Θ'. But Bob choses Θ' uniformly at random and independently of everything. Moreover he does not even use Θ' to produce $\hat{X}$ (we are in the hypothetical scenario). So even giving $\hat{X}$ to Alice keeps her uncorrelated to Θ' and so to $\mathscr{I}$. This means that the state $\tau_{A'\hat{X}\mathscr{I}}$ is such that

$$\tau_{A'\hat{X}\mathscr{I}} = \tau_{A'\hat{X}} \otimes \frac{\mathbb{1}}{|\mathscr{I}|}.$$

Let us now compare the operations performed during the real protocol, where Bob measures in his own bases Θ', with the ones performed in the hypothetical scenario where Bob choses the bases Θ' but measures in Alice's bases Θ.

In both scenarios Alice produces the state ρ_{AB}. In both scenarios apply the map $\mathscr{M}_{A\hookrightarrow A'} \otimes \mathbb{1}_B$ ($A' = \Theta T$ where Θ is the register for the bit string Θ and T is an arbitrary quantum register) to ρ_{AB} and send the B part to Bob. In both scenarios Bob choses uniformly at random a bit string Θ'. Now Bob will apply two different measurement depending on the scenario:

- In the real scenario Bob applies a measurement modeled by a CPTP map $\mathscr{M}_B^{\text{real}}$ going from B to $X'\mathscr{I}$. The correspond to the choice of basis Θ'.
- In the hypothetical scenario Bob applies a measurement modeled by a CPTP map $\mathscr{M}_B^{\text{hyp}}$ going from B to $\hat{X}\mathscr{I}$. The correspond to the choice of basis Θ.

Because Bob's device is memoryless, Bob's map has a tensor product form across all rounds. In particular we can write $\mathscr{M}_B^{\text{real}} = \mathscr{M}_{B_{\mathscr{I}}}^{\text{real}} \otimes \mathscr{M}_{B_{\mathscr{I}^c}}^{\text{real}}$, the first map acting on the rounds in $\mathscr{I}$ and the second on the ones in the complementary. For the same reason we can do the same in the hypothetical scenario $\mathscr{M}_B^{\text{hyp}} = \mathscr{M}_{B_{\mathscr{I}}}^{\text{hyp}} \otimes \mathscr{M}_{B_{\mathscr{I}^c}}^{\text{hyp}}$.

Because the device are memoryless and because on the rounds in $\mathscr{I}$ the bits of Θ and Θ' agree, the measurement on $B_{\mathscr{I}}$ are equal in both scenario, meaning that $\mathscr{M}_{B_{\mathscr{I}}}^{\text{real}} =$

$\mathcal{M}^{\text{hyp}}_{B_{\mathcal{J}}} =: \mathcal{M}_{B_{\mathcal{J}}}$. Then we can write $\tau_{A'\hat{X}_{\mathcal{J}}} = \left(\mathcal{M}_{A\mapsto A'} \otimes \mathcal{M}_{B_{\mathcal{J}}} \otimes \mathcal{M}^{\text{hyp}}_{B_{\mathcal{J}^c}}\right)(\rho_{AB})$. Moreover because Bob will trace out (in both scenarios) all the outcomes of the rounds in $\mathcal{J}^c$, the fact that the measurement are different on these rounds do not affect the outcomes in $\mathcal{J}$, meaning that,

$$\text{tr}_{X'_{\mathcal{J}^c}}\left((\mathbb{1}_{A'} \otimes \mathcal{M}_{B_{\mathcal{J}}} \otimes \mathcal{M}^{\text{real}}_{B_{\mathcal{J}^c}})(\rho_{A'B})\right) = \text{tr}_{\hat{X}_{\mathcal{J}^c}}\left((\mathbb{1}_{A'} \otimes \mathcal{M}_{B_{\mathcal{J}}} \otimes \mathcal{M}^{\text{hyp}}_{B_{\mathcal{J}^c}})(\rho_{A'B})\right) \quad (3.22)$$

$$\iff \hat{\rho}_{A'X'_{\mathcal{J}}\mathcal{J}} = \tau_{A'\hat{X}_{\mathcal{J}}\mathcal{J}}\,. \quad (3.23)$$

□

SECURITY FOR HONEST ALICE

According to Definition 2.4.9, to prove security for Alice we only need to lower bound the smooth min-entropy of X (where X is the random variable representing Alice's measurement output) condition on Bob's register. Therefore it is sufficient to lower bound the min-entropy as follows,

$$\exists \alpha > 0 :\ H_{\min}(X|BK\Theta)/n \geq \alpha.$$

This is equivalent as to show that the probability $\lambda_{\text{WSE}}(n,d,\Gamma)$ that Bob guesses x, and so that he succeeds to cheat, decays exponentially with n, where,

$$\lambda_{\text{WSE}}(n,d,\Gamma) := \max_{\rho_{ABK}} \max_{\{\mathcal{F}^\theta\}} \text{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} P^\theta_x \otimes F^\theta_x \quad \rho_{ABK}\right), \quad (3.24)$$

and where the first maximization is over all qqc-states compatible with the marginal on Alice.

If Bob is dishonest, we can look at any attack strategy of Bob as a guessing strategy in the guessing game where Bob has to guess Alice's bit string x. Thus we have the following:

Corollary 3.3.3. *For $(\alpha, \epsilon = 0)$-WSE in the Noisy Quantum Storage Model, under the assumption 3.2.1, if Alice's memoryless device is such that $\zeta < 1$ then the cheating probability $\lambda_{\text{WSE}}(n,d,\Gamma)$ of Bob is upper bounded by $B'(n,d,\zeta,\gamma)$, where $B'(n,d,\zeta,\gamma)$ is defined in Theorem 3.2.8.*

Proof. We can directly apply Theorem 3.2.8 on $(\alpha, \epsilon = 0)$-WSE by considering Bob's cheating strategy as a guessing game. □

$(\alpha,\varepsilon{=}0)$-WSE IN NOISY ENTANGLEMENT MODEL

In order to make the link between WSE and PV, we describe briefly WSE in the noisy entanglement model (see [2] for more details). The protocol is the same as before but now there are two Bobs, called Bob1 and Bob2, who share an entangled state $\rho_{B_1B_2}$ such that $E^{(1)}_C(\rho_{B_1B_2}) \leq \log(d)$ (which replaces Bob's channel $\mathcal{E}$ used in the Noisy Quantum Storage Model), and can only communicate classically from Bob1 to Bob2. It is Bob2 who is asked to get the pair $(\mathcal{J}, X_{\mathcal{J}})$, while Alice sends ρ_B to Bob1 and Θ to Bob2. If the Bobs are cheaters, Bob1 will try to send ρ_B to Bob2 using their entanglement and classical communication, in order to enable Bob2 to guess the full outcome string $X \in \{0,1\}^n$ of Alice in the perfect case (or at least $(1-\gamma)n$ bits in the imperfect case).

The Bobs play the role of the malicious provers in PV, called M_1 and M_2 who both want to guess X. The fact that in PV they both have to guess X to be able to cheat the protocol makes PV harder to cheat than WSE in the noisy-entangled model where only one Bob (Bob2) needs to guess X. Because it is harder to cheat in PV, proving the security on this model of WSE proves the result for PV [2]. Again we say that WSE in the noisy-entangled model is secure if the cheating probability denoted by λ_{NE} decays exponentially with n. In the two following Lemmas we first prove the security of WSE for the bounded-entanglement model, and then extend it to noisy-entanglement model.

Definition 3.3.4. *For $(\alpha, \epsilon = 0)$-WSE in the bounded-entanglement model, the probability $\lambda_{BE}(n,d,\Gamma)$ that Bob2 perfectly guesses Alice's output string $X \in \{0,1\}^n$ is,*

$$\lambda_{\mathrm{BE}}(n,d,\Gamma) := \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta, x\in\{0,1\}^n} P_x^\theta \otimes F_x^\theta \quad \rho_{AB_2K}\right) \tag{3.25}$$

where the first maximization is over all qqc-states compatible with the marginal on Alice (which are constraint by the value ζ measured in the testing procedure). Here the state ρ_{B_2} is of dimension at most d.

In the following Lemma 3.3.5 we look at the special case where $\rho_{B_1B_2}$ is a maximally entangled state of local dimension d (this case is WSE in the bounded entanglement model). This Lemma is a variant of Lemma 3.2.7.

Lemma 3.3.5. *For WSE in the bounded-entanglement model, where the two Bobs share a perfect entangled state $\rho_{B_1B_2}$ of dimension at most d^2, the probability $\lambda_{BE}(n,d,\Gamma)$ that Bob2 perfectly guesses Alice's output string $X \in \{0,1\}^n$ is*

$$\lambda_{\mathrm{BE}}(n,d,\Gamma) \leq B(n,d,\zeta) \tag{3.26}$$

where $B(n,d,\zeta)$ is defined in Lemma 3.2.7.

Proof. The guessing probability of Bob2 in this model is given by

$$\lambda_{\mathrm{BE}}(n,d,\Gamma) := \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta, x\in\{0,1\}^n} P_x^\theta \otimes F_x^\theta \quad \rho_{AB_2K}\right) \tag{3.27}$$

where the first maximization is over all qqc-states compatible with the marginal on Alice. Note that this is the same expression as $\lambda(n,d,\Gamma)$ except that the state $\rho_{AB'K}$ is replaced by ρ_{AB_2K}. We can then invoke Lemma 3.2.7 since Bob2's measurements are also acting jointly on d-dimensional quantum register B_2 and an arbitrary large classical register K. □

We now want to extend the result to the case where the adversary holds noisy entanglement and must guess Alice's string up to some error tolerance γ.

Definition 3.3.6. *For $(\alpha, \epsilon = 0)$-WSE in the noisy-entanglement model, the probability $\lambda_{NE}(n,d,\zeta,\gamma)$ that Bob2 guesses Alice's output string $x \in \{0,1\}^n$ with an error rate, as de-*

fined in the paragraph before equation (3.12)*, at most* γ *is,*

$$\lambda_{\mathrm{NE}}(n,d,\Gamma,\gamma) := \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} \sum_{\substack{y\in\{0,1\}^n \\ d_H(x,y)\leq\gamma n}} P_x^\theta \otimes F_y^\theta \quad \rho_{AB_2K} \right) \tag{3.28}$$

where the first maximization is over all qqc-states compatible with the marginal on Alice. Here we assume that the state shared by the two Bobs $\rho_{B_1B_2}$ *is such that* $E_C^{(1)}(\rho_{B_1B_2}) \leq \log(d)$.

3

Now we tackle the general case where $\rho_{B_1B_2}$ is a noisy-entangled state such that $E_C^{(1)}(\rho_{B_1B_2}) \leq \log(d)$.

Lemma 3.3.7. *Consider* $(\alpha, \epsilon = 0)$*-WSE in the noisy-entanglement model, where the two Bobs share a noisy entangled state* $\rho_{B_1B_2}$ *such that* $E_C^{(1)}(\rho_{B_1B_2}) \leq \log(d)$*. If Alice's device is such that* $\zeta < 1$*, then the probability* $\lambda_{\mathrm{NE}}(n,d,\Gamma)$ *that Bob2 produces a guess* $y \in \{0,1\}^n$ *and* $d_H(x,y) \leq \gamma n$ *with* $x \in \{0,1\}^n$ *being Alice's output string, is upper bounded as follows*

$$\lambda_{\mathrm{NE}}(n,d,\Gamma,\gamma) \leq B'(n,d,\zeta,\gamma) \tag{3.29}$$

where $B'(n,d,\zeta,\gamma)$ *is defined in Theorem* 3.2.8*.*

Proof. We first look at the imperfect guessing game in the bounded entanglement model, where Bob1 and Bob2 share a maximally entangled state of dimension $M \leq d$:

$$\left|\Psi_M^{B_1B_2}\right\rangle := \frac{1}{\sqrt{M}} \sum_{i=1}^{M} \left|i^{B_1}\right\rangle \left|i^{B_2}\right\rangle \tag{3.30}$$

Denote $\Psi_M := \left|\Psi_M^{B_1B_2}\right\rangle \left\langle\Psi_M^{B_1B_2}\right|$. Note that the fact that the local dimension Ψ_M is at most d implies that Bob2's quantum state ρ_{B_2} has a dimension bounded by d. Hence it is easy to see that

$$\lambda_{\mathrm{NE}}(n,d,\Gamma,\gamma) := \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} \sum_{\substack{y\in\{0,1\}^n \\ d_H(x,y)\leq\gamma n}} P_x^\theta \otimes F_y^\theta \quad \rho_{AB_2K} \right) \tag{3.31}$$

$$\leq \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} P_x^\theta \otimes F_{x\oplus z}^\theta \quad \rho_{AB_2K} \right) \tag{3.32}$$

$$\leq \sum_{\substack{z\in\{0,1\}^n \\ w_H(z)\leq\gamma n}} \max_{\rho_{AB_2K}} \max_{\{\mathscr{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} P_x^\theta \otimes F_{x\oplus z}^\theta \quad \rho_{AB_2K} \right) \tag{3.33}$$

where the first maximization is over all qqc-states compatible with the marginal on Alice, can be bounded by the techniques in the proof of the Theorem 3.2.8 since the register B_2 has bounded dimension. We have

$$\lambda_{\mathrm{NE}}(n,d,\Gamma,\gamma) \leq 2^{h(\gamma)n} \times B(n,d,\zeta) \leq B'(n,d,\zeta,\gamma). \tag{3.34}$$

We can extend this bound against an adversary who holds a noisy entangled state $\rho_{B_1B_2}$ such that $E^{(1)}_{\mathrm{C,LOCC}}(\rho_{B_1B_2}) \leq \log(d)$. Indeed by definition (eq. (3.3)) of the one shot entanglement cost of the state $\rho_{B_1B_2}$ denoted $E^{(1)}_{\mathrm{C,LOCC}}(\rho_{B_1B_2})$ [28], saying that $E^{(1)}_{\mathrm{C,LOCC}}(\rho_{B_1B_2}) \leq \log(d)$ means that $\rho_{B_1B_2}$ can be created from a perfectly entangled state Ψ_M of dimension $M \leq d$. Thus, all strategies achievable with $\rho_{B_1B_2}$ are achievable with Ψ_M. In particular the strategy which maximizes the probability of winning with respect to $\rho_{B_1B_2}$ is achievable with Ψ_M which proves the Lemma. □

If γ in the protocol is such that it satisfies the condition of Lemma 3.2.9, the previous bound proves the security of $(\alpha, \epsilon = 0)$-WSE since it decays exponentially.

3.3.2. DEVICE-INDEPENDENT POSITION VERIFICATION

In the following we will prove that PV in the noisy entanglement model (NE) is device-independently secure. Indeed the attacks on PV in the NE model can be mapped to attacks on WSE in the NE model [2, Theorem 14]. As we have proved in Lemma 3.3.7 that WSE in the NE model is device-independently secure, PV in the NE model must be secure.

Here we only speak about the one dimensional position verification protocol. In PV there are three protagonists in the honest case: two verifiers (V_1 and V_2) and one prover (P). The prover claims to be at some geographical position, and the PV protocol permits to check whether this is true.

Protocol 3.3.8 (Position Verification)**.** *Let us assume P has claimed his position to be in the middle of both verifiers (Fig. 2.4). The verifiers check this claim by the following procedure:*

1. *V_1 tests his devices as described in the testing protocol 3.2.2*
2. *At the beginning of the protocol, the two verifiers V_1 and V_2 share a random bit string $\Theta \in \{0,1\}^n$.*
3. *V_1 prepares a bipartite state (which is ideally a maximally entangled state) $\rho_{V_1P} = \sigma^{\otimes n}_{V_1P}$ which has a tensor product structure, and sends the part $\rho_P := \mathrm{tr}_{V_1}(\rho_{V_1P})$ to the prover.*

   V_2 sends the string Θ to the prover, such that the prover receives Θ and ρ_P at the same time.

   V_1 applies the measurement $\mathcal{M}^\theta = \{P^\theta_y := \bigotimes_{j\in[n]} P^{\theta_j}_{y_j}, y \in \{0,1\}^n\}$ to his part of the state ρ_{V_1P} and gets X.
4. *The prover applies a projective measurement $\mathcal{M}^\theta$, and gets a bit string $Y \in \{0,1\}^n$. Then he sends Y to both verifiers.*
5. *Then V_1 compares (using the Hamming distance) his outcome X with the string Y he receives from the prover, and measures how much time passed between the moment he sent the state to P and the moment he receives Y from P.*

6. *V_1 sends X to V_2 so V_2 can also compare Y and X. V_2 also measures how long it took for the message to come back.*

7. *If $X = Y$ (or $d_H(X,Y) \leq \gamma n$) and the time measured by the verifiers is lower than a certain fixed bound Δt then the prover passes the protocol, which means that the verifiers accept that the prover is at his claimed position.*

As mentioned in Chapter 2, if the prover is dishonest, it suffices to consider the scenario where there are two dishonest provers B_1 and B_2 who impersonate being at some claimed location. The protocol is secure against adversaries holding an entangled state $\rho_{B_1B_2}$ with one shot entanglement cost bounded by d if the probability that the adversaries cheat the protocol decays exponentially with the length n of x (which is also the number of quantum system the verifiers send to the prover).

Definition 3.3.9. *In the general case when the winning condition on the prover's guess Y is $d_H(X,Y) \leq \gamma n$, where X is the verifiers' bit string and $\gamma \in [0,1[$ is the maximal QBER, the probability of cheating in PV is defined as*

$$\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma) := \max_{\rho_{V_1M_1M_2}} \max_{\{\mathcal{T}^\theta\}} \max_{\{\mathcal{F}^\theta\}} \mathrm{tr}\left(2^{-n} \sum_{\theta,x\in\{0,1\}^n} \sum_{\substack{y\in\{0,1\}^n \\ d_H(x,y)\leq\gamma n}} P_x^\theta \otimes T_y^\theta \otimes F_y^\theta \rho_{V_1M_1M_2} \right)$$

where the first maximization is over all states compatible with the marginal on V_1, P_x^θ, T_x^θ and F_x^θ are the measurement operators for V_1, M_1 and M_2 respectively, and where the second and the third maximisations are short hand for 2^n separate maximisations: for each θ, M_1 and M_2 choose the POVMs which maximize $\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma)$

Definition 3.3.10. *PV is said to be α-secure if there exists $\alpha > 0$ and an integer $N \geq 1$ such that $\forall\, n \geq N$ the probability $\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma)$ that dishonest provers pass the protocol is such that:*

$$\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma) \leq 2^{-\alpha n}. \tag{3.35}$$

Note that the value of α may depend on d, ζ and γ.

In our case we limit the attack scheme by assuming that the adversaries can only share a limited amount of entanglement (assumptions 3.2.5) and that they do not use quantum communication, but they have access to perfect and unlimited classical communication. Moreover we will assume that the device-independent assumption 3.2.1 is satisfied in our model of attack.

Lemma 3.3.11. *In PV in the Noisy Entanglement model, where Bob1 and Bob2 share a state $\rho_{B_1B_2}$ such that $E^{(1)}_{\mathrm{C,LOCC}}(\rho_{B_1B_2}) \leq \log(d)$, if V_1's device is such that $\zeta < 1$ then the*

probability $\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma)$ that Bob2 guesses a string $Y \in \{0,1\}^n$ and $d_H(X,Y) \leq \gamma n$, where X is V_1's outcome measurement, is upper bounded by

$$\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma) \leq B'(n,d,\zeta,\gamma) \tag{3.36}$$

where $B'(n,d,\zeta,\gamma)$ is defined in Theorem 3.2.8.

Proof. We use the proof in [2, Theorem 14], which reduces the security of PV under the assumption that there is no quantum communication between cheaters, to the security of Weak String Erasure in the noisy entanglement model, in other words it proves that $\lambda_{\mathrm{PV}}(n,d,\Gamma,\gamma) \leq \lambda_{NE}(n,d,\Gamma,\gamma)$ and then using Lemma 3.3.7 we conclude the proof. □

If γ is such that it satisfies the condition of Lemma 3.2.9 this bound proves the security of PV since $B'(n,d,\zeta,\gamma)$ decays exponentially (see figure 3.3). The security proof is independent of the implementation of the protocol. Moreover, to allow an honest prover to pass the protocol even when there is some noise in the quantum channel between V_1 and P or if honest prover's measurements are not perfect means that we allow the prover P to guess the string x with some error quantified by the Hamming distance. This choice obviously makes the protocol easier to cheat on when P is dishonest, but according to Lemmas 3.3.11 and 3.2.9 the protocol is still secure if the fraction of errors γ allowed in the guessed string is small enough.

Note that PV is still secure if we allow V_1's device to send the string x to the prover after V_1 makes the measurements on his state. V_1 just has to wait long enough before measuring his state. Then dishonest provers cannot use this information since there is a time constraint on their answers.

3.4. CONCLUSION

By dealing directly with quantum memory in the guessing game, we show that security in WSE can be achieved device independently against an adversary holding a quantum memory of size $r := \log(d) \lesssim 0.45n$ qubits. This improves the previous known result [1] which proved security for $r \lesssim 0.22n$ qubits (see Table 3.1). This result remains valid in the noisy storage device model. To deal with the quantum memory, we had to develop new techniques. This result is a first step toward optimality of the bounds and opens the door to further analyzes of optimal bound in the IID device independent scenario. We don't know however if our bound is optimal. The results in the trusted devices scenario suggest that the optimal bound implies that security can be achieved against an adversary holding a memory of size $r \lesssim n$. It is still an open question if this can be achieved in the device independent scenario.

We also prove security condition stronger than in [1] for a dishonest Alice which can become useful when using WSE in other two-party cryptographic protocol. The previous result only proves security of two-party cryptographic protocol against classical adversary, by proving that at the end of WSE Alice is ignorant about the set $\mathscr{I}$.

Finally we link the security of WSE with the security of PV, and therefore we show for the first time that device independent security can be achieved for PV.

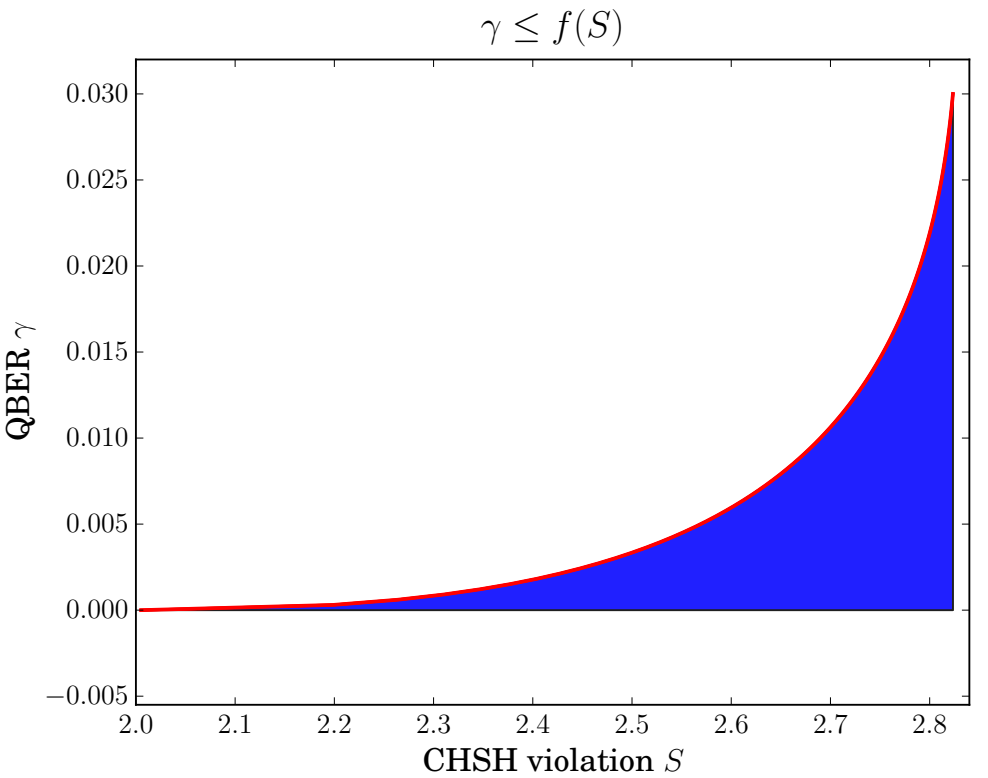


Figure 3.3: QBER γ allowed in function of the CHSH violation S obtained in the testing procedure when $n \to \infty$ and d finite. The blue region is the secure region *i.e.* the region where the bound $B'(n,d,\zeta,\gamma)$ decays exponentially in n for a fixed d.

3.5. TECHNICAL DETAILS

3.5.1. TECHNICAL LEMMA

In the proof of the Key Lemma to be presented below, we will need the following result. Similar results about norm of sums of operators have been obtained by Kittaneh [29], see also [14, Lemma 2].

Lemma 3.5.1. *If $A_1, A_2, \ldots, A_N$ are positive semi-definite operators, then*

$$\left\| \sum_{i\in[N]} A_i \right\| \leq \max_{j\in[N]} \sum_{i\in[N]} \left\| \sqrt{A_i}\sqrt{A_j} \right\|, \tag{3.37}$$

where $[N] := \{1, \ldots, N\}$.

Proof. Let K be an $N \times N$ block matrix with entries $K_{ij} = \sqrt{A_i}\sqrt{A_j}$ and L is an $N \times N$ matrix of entries $L_{ij} = \|\sqrt{A_i}\sqrt{A_j}\|$, we first show that

$$\left\| \sum_{i\in[N]} A_i \right\| = \|K\| \leq \|L\|. \tag{3.38}$$

Defining $\tilde{K} := \sum_j |j\rangle \otimes \sqrt{A_j}$, a direct calculation reveals

$$\tilde{K}^\dagger \tilde{K} = \sum_j A_j \quad \text{and} \quad \tilde{K}\tilde{K}^\dagger = \sum_{jk} |j\rangle\langle k| \otimes \sqrt{A_j}\sqrt{A_k} = K, \tag{3.39}$$

from which follows the first equality since the operator norm satisfies $\|\tilde{K}^\dagger\tilde{K}\| = \|\tilde{K}\tilde{K}^\dagger\|$. We are thus left with proving $\|\tilde{K}\tilde{K}^\dagger\| \leq \|L\|$ where now we rewrite L in the following form

$$L = \sum_{jk} |j\rangle\langle k| \otimes \|\sqrt{A_j}\sqrt{A_k}\|. \tag{3.40}$$

Since the operator norm of a positive semidefinite matrix corresponds to its largest eigenvalue, it suffices to prove that the largest eigenvalue of $\tilde{K}\tilde{K}^\dagger$ is not greater than the largest eigenvalue of L. Let $|\alpha\rangle$ be an eigenvector corresponding to the largest eigenvalue of $\tilde{K}\tilde{K}^\dagger$ and write it as

$$|\alpha\rangle = \sum_j \alpha_j |j\rangle|e_j\rangle, \tag{3.41}$$

where α_j are real and positive and $|e_j\rangle$ are arbitrary but normalised. Then

$$\|\tilde{K}\tilde{K}^\dagger\| = \langle\alpha|\tilde{K}\tilde{K}^\dagger|\alpha\rangle = \sum_{jk} \alpha_j\alpha_k\langle e_j|\sqrt{A_j}\sqrt{A_k}|e_k\rangle. \tag{3.42}$$

Now it suffices to prove that this can be upper bounded by $\langle\alpha'|L|\alpha'\rangle$ for

$$|\alpha'\rangle = \sum_j \alpha_j |j\rangle, \tag{3.43}$$

which implies

$$\|K\| = \|\tilde{K}\tilde{K}^\dagger\| = \langle\alpha|\tilde{K}\tilde{K}^\dagger|\alpha\rangle \leq \langle\alpha'|L|\alpha'\rangle \leq \|L\|. \tag{3.44}$$

To show $\langle\alpha|K|\alpha\rangle \leq \langle\alpha'|L|\alpha'\rangle$, we begin by rewriting K as

$$K = \sum_{jk} |j\rangle\langle k| \otimes \sqrt{A_j}\sqrt{A_k} \tag{3.45}$$

$$= \sum_{j<k} \underbrace{|j\rangle\langle k| \otimes \sqrt{A_j}\sqrt{A_k} + |k\rangle\langle j| \otimes \sqrt{A_k}\sqrt{A_j}}_{=:B_{jk}} + \sum_j |j\rangle\langle j| \otimes A_j \tag{3.46}$$

This form makes hermitian matrices B_{jk} and $|j\rangle\langle j| \otimes A_j$ appear in the sums. K is positive semidefinite so $\langle\alpha|K|\alpha\rangle = |\langle\alpha|K|\alpha\rangle|$ and,

$$|\langle\alpha|K|\alpha\rangle| = |\sum_{j\neq k} \alpha_j\alpha_k\langle j|\langle e_j|B_{jk}|k\rangle|e_k\rangle + \sum_j \alpha_j^2 \underbrace{\langle e_j|A_j|e_j\rangle}_{\leq \|A_j\|}| \tag{3.47}$$

$$\leq \sum_{j\neq k} \alpha_j\alpha_k|\langle j|\langle e_j|B_{jk}|k\rangle|e_k\rangle| + \sum_j \alpha_j^2\|A_j\|. \tag{3.48}$$

Now by decomposing the vectors $|j\rangle|e_j\rangle = \sum_l \beta_l^j |\beta_l\rangle$ and $|k\rangle|e_k\rangle = \sum_m \beta_m^k |\beta_m\rangle$ in an eigenbasis of B_{jk} noted $\{|\beta_i\rangle\}_i$ we get,

$$|\langle j|\langle e_j|B_{jk}|k\rangle|e_k\rangle| = |\sum_{lm} \beta_l^{j*}\beta_m^k \langle\beta_l|B_{jk}|\beta_m\rangle| \tag{3.49}$$

$$= |\sum_l \beta_l^{j*}\beta_l^k \lambda_l| \tag{3.50}$$

where $\{\lambda_l\}_l$ are the eigenvalues of B_{jk}. Using the triangle inequality we have,

$$|\sum_l \beta_l^{j*}\beta_l^k \lambda_l| \leq \sum_l |\beta_l^{j*}||\beta_l^k||\lambda_l| \tag{3.51}$$

$$\leq \max_i |\lambda_i| \underbrace{\sum_l |\beta_l^{j*}||\beta_l^k|}_{\leq 1} \tag{3.52}$$

$$\leq \max_i |\lambda_i| = \|B_{jk}\|. \tag{3.53}$$

It is easy to check that $\|B_{jk}\| = \|\sqrt{A_j}\sqrt{A_k}\|$. Using that and (3.53) in the inequality (3.48) we have,

$$\|K\| = \langle\alpha|K|\alpha\rangle \leq \sum_{jk} \alpha_j\alpha_k \|\sqrt{A_j}\sqrt{A_k}\| = \langle\alpha'|L|\alpha'\rangle \leq \|L\| \tag{3.54}$$

which gives the desired inequality $\|K\| \leq \|L\|$.

Using Hölder's inequality (Lyapunov's inequalities) for induced p-norms, we have

$$\|L\| = \|L\|_2^{\mathrm{I}} \leq \left(\|L\|_1^{\mathrm{I}} \cdot \|L\|_\infty^{\mathrm{I}}\right)^{1/2}, \tag{3.55}$$

where the norms on the right hand side are equal to the maximum absolute row or column sums

$$\|L\|_1^{\mathrm{I}} = \max_j \sum_i \|\sqrt{A_i}\sqrt{A_j}\|, \tag{3.56}$$

$$\|L\|_\infty^{\mathrm{I}} = \max_i \sum_j \|\sqrt{A_i}\sqrt{A_j}\|. \tag{3.57}$$

The Lemma follows since these two norms are equal for hermitian matrices. □

3.5.2. PROOF OF THE KEY LEMMA

The main content of this section is a detailed proof of the Key Lemma presented in the main text. Specifically, we prove a bound on the probability that Bob wins the game, only depending on a quantity ζ that Alice can estimate experimentally, Bob's memory size d, and n which is the number of rounds played in the game.

We split this proof into four steps. In Step 1 we analyse how Jordan's Lemma permits us to conveniently express the effective absolute anti-commutator of Alice's measurements. In Step 2 we derive a bound on the winning probability expressed in terms of

what we call "operator overlap", then in Step 3 we bound this overlap by a simpler expression depending on the effective anti-commutator. We finish the proof in Step 4 by replacing, in the previous simple bound on the overlap, the effective anti-commutator by a quantity that Alice can estimate experimentally.

For the reader's convenience, we have included Table 3.2 which explains the symbols used in the proof.

STEP 1: ALICE'S IID STATE-PREPARATION AND MEASUREMENT DEVICE

In this section we use Jordan's Lemma to rewrite Alice's measurement operators and the absolute effective anti-commutator.

We assume that the devices used by Alice to prepare and measure satisfy the IID assumption, i.e. the state produced in n rounds is of the form $\rho_{AB} = \sigma_{AB}^{\otimes n}$ and the measurement corresponding to input $\theta \in \{0,1\}^n$ can be written as $\{P_x^\theta = \bigotimes_k P_{x_k}^{\theta_k} : x \in \{0,1\}^n\}$, where $\{P_0^0, P_1^0\}$ and $\{P_0^1, P_1^1\}$ are some unknown (but fixed) binary measurements. It is worth stressing that this implies that the reduced state on Alice is of product form, $\rho_A = \sigma_A^{\otimes n}$, regardless of how Bob manipulates his subsystem. We make no assumptions on the dimensions of the system (except that they are finite dimensional).

By Naimark's dilation Theorem we can without loss of generality assume that the measurements $\{P_0^0, P_1^0\}$ and $\{P_0^1, P_1^1\}$ are projective, which allows us to apply Jordan's Lemma [25, 26]. The projectors representing the first outcome P_0^0 and P_0^1 can be simultaneously decomposed into orthogonal projections of rank at most one, projecting on either one or two dimensional subspaces invariant under the action of both projectors (a subspace W is invariant under the linear opearator T if and only if $TW \subseteq W$). Moreover we only get two-dimensional blocks when the projectors have non-trivial overlap, i.e. they are neither orthogonal nor identical:

$$P_0^0 = \sum_{j \in \mathscr{J}} P_{0|j}^0, \;\; P_0^1 = \sum_{j \in \mathscr{J}} P_{0|j}^1, \tag{3.58}$$

where $P_{0|j}^a$ ($a \in \{0,1\}$) are such that $\forall\, j, j' \; P_{0|j}^a P_{0|j'}^a = \delta_{jj'} P_{0|j}^a$ and are acting on a subspace of dimension one or two. Then we have,

$$P_1^0 = \sum_{j \in \mathscr{J}} (S_j - P_{0|j}^0), \;\; P_1^1 = \sum_{j \in \mathscr{J}} (S_j - P_{0|j}^1). \tag{3.59}$$

where S_j is a projection which projects on the subspace where $P_{0|j}^a$ and $P_{1|j}^a$ act. Note that the number of non-zero summands in (3.58) is equal to the rank of P_0^0 or P_0^1 respectively.

A convenient basis of the Hilbert space can be chosen as follows. Each index $j \in \mathscr{J}$ corresponds to either a one or two dimensional subspace. For the two dimensional subspaces indexed by j in $\mathscr{J}$ where both $P_{0|j}^0$ and $P_{0|j}^1$ are nonzero, we pick the orthonormal eigenbasis of $P_{0|j}^0$, namely $|0_{|j}^0\rangle$ and $|1_{|j}^0\rangle$, as the basis for these subspaces

$$P_{0|j}^0 |0_{|j}^0\rangle = |0_{|j}^0\rangle, \;\; P_{0|j}^0 |1_{|j}^0\rangle = 0. \tag{3.60}$$

Moreover, one can pick these basis vectors (by including a phase factor if necessary) such that the eigenstates $|0^1_{|j}\rangle$ and $|1^1_{|j}\rangle$ of $P^1_{0|j}$, which satisfy

$$P^1_{0|j}|0^1_{|j}\rangle = |0^1_{|j}\rangle, \;\; P^1_{0|j}|1^1_{|j}\rangle = 0, \tag{3.61}$$

are related to those of $P^0_{0|j}$ by

$$|0^1_{|j}\rangle = \cos\beta_j|0^0_{|j}\rangle + \sin\beta_j|1^0_{|j}\rangle, \;\; |1^1_{|j}\rangle = \sin\beta_j|0^0_{|j}\rangle - \cos\beta_j|1^0_{|j}\rangle, \tag{3.62}$$

for some angle $\beta_j \in [0,\pi/2]$. For the one dimensional subspaces (also indexed by $j \in \mathscr{J}$) we define $|0^0_{|j}\rangle$ being a unit vector, and $|1^0_{|j}\rangle$ is the null vector. Then we define $|0^1_{|j}\rangle$ and $|1^1_{|j}\rangle$ as previously but with $\beta_j = 0$ or $\beta_j = \pi/2$. In summary, since we have defined a basis for each $j \in \mathscr{J}$, taking the direct sum gives a basis for the whole Hilbert space. Any binary (projective) measurement device admits a characterization through the angles $\beta_j \in [0,\pi/2]$ for $j \in \mathscr{J}$ and this characterization turns out to be sufficient for our purposes.

The previous block decomposition allows us to conveniently compute the effective absolute anticommutator defined as $\epsilon_+ := \frac{1}{2}\operatorname{tr}(|\{A_0,A_1\}|\sigma_A)$ where $A_\theta := P^\theta_0 - P^\theta_1$ for $\theta \in \{0,1\}$. The word "effective" means that ϵ_+ depends not only on Alice's measurements, but also on the state on which the measurements act. Under Jordan's Lemma, the absolute anticommutator becomes

$$|\{A_0,A_1\}| = |\sum_j \{A_{0|_j}, A_{1|_j}\}| = \sum_j 2|\cos(2\beta_j)|S_j \tag{3.63}$$

with $A_{\theta|_j} := P^\theta_{0|j} - P^\theta_{1|j}$ and S_j being the orthogonal projections defined above, where the absolute anticommutator of a two dimensional block j is computed using (3.62) and that of a one dimensional block follows from our definition of $\beta_j = 0$ in Step 1. Let $p_j := \operatorname{tr}(S_j\sigma_A)$ be the probability of σ_A being projected in the j-th block, then, the absolute effective commutator can be written as

$$\epsilon_+ = \sum_j p_j|\cos(2\beta_j)| = \sum_j p_j\epsilon_j, \tag{3.64}$$

where $\epsilon_j := |\cos(2\beta_j)|$ is the absolute effective anticommutator of the block j. It is worth pointing out that for qubit observables there is no notion of "effectiveness", i.e. the incompatibility is fixed by the observables and does not depend on the state.

Also, the previous decomposition of Alice measurements enables the n run projectors to be block diagonalized as

$$P^\theta_x = \bigotimes_{k=1}^n P^{\theta_k}_{x_k} = \bigotimes_{k=1}^n \sum_{b_k\in\mathscr{J}} P^{\theta_k}_{x_k|b_k} = \sum_{b\in\mathscr{J}^n} P^\theta_{x|b}, \tag{3.65}$$

where $P^\theta_{x|b} := \bigotimes_{k=1}^n P^{\theta_k}_{x_k|b_k}$, and $\mathscr{J}$ is the set of indices which label blocks and $\mathscr{J}^n := \mathscr{J}^{\times n}$. We denote the set of projectors associated with this direct sum decomposition by $\{S_b\}_{b\in\mathscr{J}^n}$, where $S_b := \bigotimes_{k=1}^n S_{b_k}$. For each k, we have $P^{\theta_k}_{x_k|b_k}P^{\theta_k}_{x'_k|b'_k} = \delta_{x_k,x'_k}\delta_{b_k,b'_k}P^{\theta_k}_{x_k|b_k}$, and $P^{\theta_k}_{x_k|b_k}$ orthogonal to $P^{\theta'_k}_{x'_k|b'_k}$ whenever $b_k \neq b'_k$. The analysis of the guessing game will rest on these orthogonality relations and the set of angles β_j defined above.

Variable	Range	Meaning
n	$\mathbb{N}$	total number of (measurement) runs
k	$[n]$	index of the run (subscript) or the classical information of Bob (superscript)
θ	$\{0,1\}^n$	measurement string
θ_k	$\{0,1\}$	k^{th} measurement
x	$\{0,1\}^n$	output string
x_k	$\{0,1\}$	k^{th} output
j	$\mathscr{J}$	index of Jordan's Lemma decomposition
b	$\mathscr{J}^n$	vector indexing block combination
b_k	$\mathscr{J}$	k^{th} element of b
$p_{(\cdot)}$	$[0,1]$	probability of $(\cdot)$ (depending on context)
β_{b_k}	$[0,\pi/2]$	angle of Alice's binary measurement in block b_k
ϵ_{b_k}	$[0,1]$	absolute effective anticommutator in block b_k

Table 3.2: Table of symbols for this Technical Details section.

STEP 2: FROM GUESSING PROBABILITY TO "OPERATOR OVERLAPS"

The goal of this section is to bound Bob's wining probability in term of the overlap $\left\|\sqrt{\Pi_b^{\theta',k}}\sqrt{\Pi_b^{\theta,k}}\right\|$. To be precise we show that,

Lemma 3.5.2. *Let $\Pi_b^{\theta,k} := \sum_x P_{x|b}^{\theta} \otimes F_x^{\theta,k}$, where Alice's POVM elements P_x^{θ} are defined in* (3.65)*, and where F_x^{θ} are arbitrary POVM element acting on Bob's systems (registers $B'K$: see eq.* (3.9)*), and $F_x^{\theta,k}$ are defined in eq.* (3.70)*. Bob's wining probability $\lambda(n,d,\Gamma)$ defined in equation* (3.9) *is bounded as follow:*

$$\lambda(n,d,\Gamma) \leq \max_{\left\{p_k,\rho_{AB'}^k\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_{k,b} p_k p_{b|k} \max_{\theta'} 2^{-n} \sum_{\theta} \left\|\sqrt{\Pi_b^{\theta',k}}\sqrt{\Pi_b^{\theta,k}}\right\| \tag{3.66}$$

Proof. Since we assume that the quantum memory of Bob is bounded he cannot store the entire register B received from Alice. More specifically, according to the Bounded Quantum Storage Model he must immediately input the register B into an encoding map which outputs a quantum register B' (whose dimension is bounded by d) and a classical register K (of arbitrary size). The joint state between Alice and Bob is then a qqc-state $\rho_{AB'K} = \sum_k p_k \rho_{AB'}^k \otimes |k\rangle\langle k|$ whose marginal remains IID $\rho_A = \text{tr}_{B'K}(\rho_{AB'K}) = \sigma_A^{\otimes n}$. Once Alice has measured her part of the system, Bob is told the choice of her measurements represented by $\theta \in \{0,1\}^n$ and is asked to guess the string of outcomes. We take the suc-

cess probability given by (3.9) and expand the classical register K to obtain

$$\lambda(n,d,\Gamma) = \max_{\substack{\rho_{AB'K} \\ \text{qqc} \\ \dim(\mathscr{H}_{B'}\leq d)}} \max_{\{\mathscr{F}^\theta\}} \operatorname{tr}\left(2^{-n}\sum_{\theta,x\in\{0,1\}^n} P_x^\theta \otimes F_x^\theta \quad \rho_{AB'K}\right) \tag{3.67}$$

$$= \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^\theta\}} \sum_k p_k \operatorname{tr}\left(\sum_{\theta,x} 2^{-n} P_x^\theta \otimes F_x^\theta \rho^k_{AB'} \otimes |k\rangle\langle k|_K\right) \tag{3.68}$$

$$= \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_k p_k \operatorname{tr}\left(\sum_{\theta,x} 2^{-n} P_x^\theta \otimes F_x^{\theta,k} \rho^k_{AB'}\right), \tag{3.69}$$

where P_x^θ are the measurement operators on Alice's side, and

$$F_x^{\theta,k} := \operatorname{tr}_K(F_x^\theta \mathbb{1}_{B'} \otimes |k\rangle\langle k|_K) \tag{3.70}$$

are d-dimensional measurement operators on Bob's side acting on B', which depend both on his classical memory k and the basis string θ received from Alice. The outer optimization is constrained to ensembles which yield the correct marginal on Alice's side, i.e. $\operatorname{tr}_{B'}(\sum_k p_k \rho^k_{AB'}) = \sigma_A^{\otimes n}$. The inner maximization represents $|\Theta||K|$ independent maximizations each of which is over a POVM $\{F_x^{\theta,k}\}$. The rest of the proof will be concerned with upper bounding $\lambda(n,d,\Gamma)$.

Inserting (3.65) into (3.69) we get

$$\lambda(n,d,\Gamma) = \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_k p_k \operatorname{tr}\left(\sum_{\theta,x} 2^{-n} \sum_b P^\theta_{x|b} \otimes F_x^\theta \rho^k_{AB'}\right), \tag{3.71}$$

Recall that S_b represents the projection operator into the blocks indexed by $b \in \mathscr{J}^n$. Define $\rho^k_{A_bB'} := (S_b \otimes \mathbb{1}_{B'})\rho^k_{AB'}(S_b \otimes \mathbb{1}_{B'})/p_{b|k}$ to be the normalized projections of $\rho^k_{A_bB'}$ into these various blocks with $p_{b|k} := \operatorname{tr}\left((S_b \otimes \mathbb{1}_{B'})\rho^k_{AB'}\right)$. Then

$$\lambda(n,d,\Gamma) = \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_k p_k \sum_b p_{b|k} \operatorname{tr}\left(\sum_{\theta,x} 2^{-n} P^\theta_{x|b} \otimes F_x^{\theta,k} \rho^k_{A_bB'}\right), \tag{3.72}$$

and for convenience let us denote $\Pi_b^{\theta,k} := \sum_x P^\theta_{x|b} \otimes F_x^{\theta,k}$ so that

$$\lambda(n,d,\Gamma) = \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_{k,b} p_k p_{b|k} \operatorname{tr}\left(\sum_\theta 2^{-n} \Pi_b^{\theta,k} \rho^k_{A_bB'}\right). \tag{3.73}$$

Bounding each of the trace terms by its operator norm yields

$$\lambda(n,d,\Gamma) \leq \max_{\left\{p_k,\rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \sum_{k,b} p_k p_{b|k} \left\| \sum_\theta 2^{-n} \Pi_b^{\theta,k} \right\|. \tag{3.74}$$

For each b,k the corresponding operator norm can be bounded using Lemma 3.5.1 as follows

$$\left\| \sum_{\theta} 2^{-n} \Pi_b^{\theta,k} \right\| \leq 2^{-n} \max_{\theta'} \sum_{\theta} \left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\| \tag{3.75}$$

from which (3.74) becomes

$$\lambda(n,d,\Gamma) \leq 2^{-n} \max_{\left\{p_k, \rho^k_{AB'}\right\}} \max_{\{\mathscr{F}^{\theta,k}\}} \underbrace{\sum_{k,b} p_k p_{b|k} \max_{\theta'} \sum_{\theta} \left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\|}_{=:\Lambda}. \tag{3.76}$$

□

STEP 3: BOUND ON OPERATOR OVERLAPS

The goal of this section is to find a bound on $\left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\|$ which holds *independenly of* k. The superscript k of the operator $\Pi_b^{\theta',k}$ reminds us that Bob's measurement might depend on his classical information. Here, we derive a bound which only depends on the dimension of his quantum system i.e. independent of k. Therefore, we will from now omit the superscript k which represented the classical information of Bob. The following Lemma is the key towards the main result.

Lemma 3.5.3. *For all* $\theta', \theta \in \{0,1\}^n$ *and* $b \in \mathscr{J}^n$*, we have*

$$\left\| \sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}} \right\| \leq \min \left\{ 1, \sqrt{d} \prod_{k=1}^{n} \left(\max\{\cos\beta_{b_k}, \sin\beta_{b_k}\} \right)^{w_k} \right\}, \tag{3.77}$$

where d *is the dimension of Bob's quantum memory, and* $w := \theta' \oplus \theta \in \{0,1\}^n$

Proof. Let us begin by simplifying $\sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}}$ using the definition of Π_b^{θ} in Step 2 and orthogonality relations of $P^{\theta}_{x|b}$ in Step 1. Let $S = \{k \in [n] : \theta'_k = \theta_k\}$ and $T = \{k \in [n] : \theta'_k \neq \theta_k\}$ be the indices where the measurement choices agree and differ respectively. Then,

$$\sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}} = \sum_{x,y} P^{\theta'}_{x|b} P^{\theta}_{y|b} \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}} \tag{3.78}$$

$$= \sum_{x,y} \bigotimes_{k\in S} P^{\theta'_k}_{x_k|b_k} P^{\theta_k}_{y_k|b_k} \bigotimes_{k\in T} P^{\theta'_k}_{x_k|b_k} P^{\theta_k}_{y_k|b_k} \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}} \tag{3.79}$$

$$= \sum_{x,y} \underbrace{\bigotimes_{k\in S} \delta_{x_k,y_k} P^{\theta_k}_{y_k|b_k}}_{(\star)} \bigotimes_{k\in T} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle x^{\theta'_k}_{k|b_k} \right| y^{\theta_k}_{k|b_k} \left\rangle \left\langle y^{\theta_k}_{k|b_k} \right| \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}} \tag{3.80}$$

where $\left| y^{\theta_k}_{k|b_k} \right\rangle$ are the eigenvectors defined in Step 1. The notation $\left| y^{\theta_k}_{k|b_k} \right\rangle$ should be read as the eigenvector representing the outcome $y_k \in \{0,1\}$ of the measurement $\theta_k \in \{0,1\}$ restricted to the block $b_k \in \mathscr{J}$.

The sum over $x = (x_1, ..., x_n), y = (y_1, ..., y_n) \in \{0,1\}^n$ can be split into a sum of variables with indices in S which we will denote by $\tilde{x}, \tilde{y}$ and indices in T denoted x', y'. The definition of S implies that $\tilde{x} = \tilde{y}$. Let

$$M_{\tilde{x}} := \sum_{x',y' \in \{0,1\}^{|T|}} \bigotimes_{k \in T} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle x^{\theta'_k}_{k|b_k} \right| y^{\theta_k}_{k|b_k} \rangle \langle y^{\theta_k}_{k|b_k} \Big| \otimes \sqrt{F^{\theta'}_{\tilde{x}x'}} \sqrt{F^{\theta}_{\tilde{x}y'}}, \tag{3.81}$$

where the two strings x' and x together form a bit string of length n and give meaning to the notation $F^{\theta'}_{\tilde{x}x'}$ (same for $F^{\theta}_{\tilde{x}y'}$). Since the register labelled as $(\star)$ consists of orthogonal projectors, the desired operator norm is achieved by a maximization over $\tilde{x} \in \{0,1\}^{|S|}$. That is

$$\left\| \sqrt{\Pi^{\theta'}_b} \sqrt{\Pi^{\theta}_b} \right\| = \max_{\tilde{x} \in \{0,1\}^{|S|}} \|M_{\tilde{x}}\| \tag{3.82}$$

In the following we derive an upper bound which does not depend on $\tilde{x}$. Since for $k \in T$ we have $\theta_k \neq \theta'_k$, we use Eq. (3.62) to evaluate the inner product

$$\langle x^{\theta'_k}_{k|b_k} \Big| y^{\theta_k}_{k|b_k} \rangle = (-1)^{x_k y_k} \cos(\beta_{b_k})^{\overline{x_k \oplus y_k}} \sin(\beta_{b_k})^{x_k \oplus y_k}, \tag{3.83}$$

where $\overline{x_k \oplus y_k} = 1 - x_k \oplus y_k$. Therefore,

$$M_{\tilde{x}} = \sum_{x',y'} (-1)^{x' \cdot \tilde{y}} \bigotimes_{k \in T} \cos(\beta_{b_k})^{\overline{x_k \oplus y_k}} \sin(\beta_{b_k})^{x_k \oplus y_k} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle y^{\theta_k}_{k|b_k} \right| \otimes \sqrt{F^{\theta'}_{\tilde{x}x'}} \sqrt{F^{\theta}_{\tilde{x}y'}}. \tag{3.84}$$

where $\forall x, y \in \{0,1\}^m,\ x.y := \sum_k x_k y_k$

From $\|M_{\tilde{x}}\| = \sqrt{\|M_{\tilde{x}} M^{\dagger}_{\tilde{x}}\|}$ and the definition

$$f(\beta_b, x', y', z') := (-1)^{(x' \oplus z') \cdot \tilde{y}} \prod_{k \in T} \cos(\beta_{b_k})^{\overline{x_k \oplus y_k} + \overline{z_k \oplus y_k}} \sin(\beta_{b_k})^{x_k \oplus y_k + z_k \oplus y_k}, \tag{3.85}$$

where β_b is a vector of angles, we simplify $M_{\tilde{x}} M^{\dagger}_{\tilde{x}}$ and get

$$\|M_{\tilde{x}}\| = \left\| \sum_{x',z'} \bigotimes_{k \in T} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle z^{\theta'_k}_{k|b_k} \right| \otimes \underbrace{\sqrt{F^{\theta'}_{\tilde{x}x'}} \left(\sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right) \sqrt{F^{\theta'}_{\tilde{x}z'}}}_{(**)} \right\|^{1/2}. \tag{3.86}$$

Bounding the register labelled as $(**)$ by its operator norm does not decrease the norm as mentioned in Lemma 3.5.1. Hence we have

$$\|M_{\tilde{x}}\| \leq \left\| \sum_{x',z'} \bigotimes_{k \in T} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle z^{\theta'_k}_{k|b_k} \right| \cdot \left\| \sqrt{F^{\theta'}_{\tilde{x}x'}} \left(\sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right) \sqrt{F^{\theta'}_{\tilde{x}z'}} \right\| \right\|^{1/2}. \tag{3.87}$$

Bounding the outer operator norm with Schatten two norm ($\|\cdot\| \leq \|\cdot\|_2$) gives

$$\|M_{\tilde{x}}\| \leq \left\| \sum_{x',z'} \bigotimes_{k \in T} \left| x^{\theta'_k}_{k|b_k} \right\rangle \left\langle z^{\theta'_k}_{k|b_k} \right| \cdot \left\| \sqrt{F^{\theta'}_{\tilde{x}x'}} \left(\sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right) \sqrt{F^{\theta'}_{\tilde{x}z'}} \right\| \right\|^{1/2}_2 \tag{3.88}$$

$$= \left(\sum_{x',z'} \left\| \sqrt{F^{\theta'}_{\tilde{x}x'}} \left(\sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right) \sqrt{F^{\theta'}_{\tilde{x}z'}} \right\|^2 \right)^{1/4}. \tag{3.89}$$

Using submultiplicativity of the operator norm we have

$$\|M_{\tilde{x}}\| \leq \left(\sum_{x',z'} \left\| \sqrt{F^{\theta'}_{\tilde{x}x'}} \right\|^2 \left\| \sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right\|^2 \left\| \sqrt{F^{\theta'}_{\tilde{x}z'}} \right\|^2 \right)^{1/4} \tag{3.90}$$

$$= \left(\sum_{x',z'} \left\| F^{\theta'}_{\tilde{x}x'} \right\| \underbrace{\left\| \sum_{y'} f(\beta_b, x', y', z') F^{\theta}_{\tilde{x}y'} \right\|^2}_{(*)} \left\| F^{\theta'}_{\tilde{x}z'} \right\| \right)^{1/4} . \tag{3.91}$$

From the definition of $f(\beta_b, x', y', z')$ in (3.85) it is easy to see that

$$|f(\beta_b, x, y, z)| \leq \prod_{k \in T} \max\{\cos^2 \beta_{b_k}, \sin^2 \beta_{b_k}\}. \tag{3.92}$$

Since this bound does not depend on y' we can take it out of the sum

$$(*) \leq \prod_{k \in T} \max\{\cos^4 \beta_{b_k}, \sin^4 \beta_{b_k}\} \left\| \sum_{y} F^{\theta}_{\tilde{x}y'} \right\|^2 \tag{3.93}$$

$$\leq \prod_{k \in T} \max\{\cos^4 \beta_{b_k}, \sin^4 \beta_{b_k}\}. \tag{3.94}$$

The latter inequality holds because $\sum_y F^{\theta}_{\tilde{x}y} \leq \mathbb{1}$. Using this bound in (3.91) gives us,

$$\left\| \sqrt{\Pi^{\theta'}_b} \sqrt{\Pi^{\theta}_b} \right\| \leq \prod_{k \in T} \max\{\cos \beta_{b_k}, \sin \beta_{b_k}\} \left[\sum_{x'z'} \|F^{\theta'}_{\tilde{x}x'}\| \|F^{\theta'}_{\tilde{x}z'}\| \right]^{1/4} \tag{3.95}$$

$$= \prod_{k \in T} \max\{\cos \beta_{b_k}, \sin \beta_{b_k}\} \left[\sum_{x} \|F^{\theta'}_{\tilde{x}x'}\| \right]^{1/2} \tag{3.96}$$

$$\leq \sqrt{d} \prod_{k \in T} \max\{\cos \beta_{b_k}, \sin \beta_{b_k}\} \tag{3.97}$$

where in the last inequality we use the observation that for all $\tilde{x} \in \{0,1\}^{n-t}$

$$\sum_{x'} \|F^{\theta'}_{\tilde{x}x'}\| \leq \sum_{x} \mathrm{tr}(F^{\theta'}_{\tilde{x}x'}) = \mathrm{tr}\left(\sum_{x} F^{\theta'}_{\tilde{x}x'} \right) \leq \mathrm{tr}(\mathbb{1}_d) = d \tag{3.98}$$

since Bob's quantum memory is of dimension at most d. Combining this bound with the trivial bound $\left\| \sqrt{\Pi^{\theta'}_b} \sqrt{\Pi^{\theta}_b} \right\| \leq 1$ completes the proof. □

Lemma 3.5.4. *For all $\theta', \theta \in \{0,1\}^n$ and $b \in \mathscr{J}^n$, we have*

$$\left\| \sqrt{\Pi^{\theta'}_b} \sqrt{\Pi^{\theta}_b} \right\| \leq \min\left\{ 1, \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\epsilon_{b_k}}{2} \right)^{w_k/2} \right\}, \tag{3.99}$$

where d is the dimension of Bob's memory and $w := \theta \oplus \theta' \in \{0,1\}^n$

Proof. Recall that for all $k \in [n]$ and $b \in \mathscr{J}^n$

$$\epsilon_{b_k} := |\cos 2\beta_{b_k}| = \begin{cases} \cos 2\beta_{b_k} & \text{if } \beta_{b_k} \in [0, \pi/4] \\ -\cos 2\beta_{b_k} & \text{if } \beta_{b_k} \in]\pi/4, \pi/2] \end{cases} \tag{3.100}$$

- If $\beta_{b_k} \in [0, \pi/4]$ then $\cos\beta_{b_k} \geq \sin\beta_{b_k}$ and

$$\max\{\cos\beta_{b_k}, \sin\beta_{b_k}\} = \cos\beta_{b_k} = \sqrt{\frac{1+\cos 2\beta_{b_k}}{2}} = \sqrt{\frac{1+\epsilon_{b_k}}{2}}. \tag{3.101}$$

- Similarly, if $\beta_{b_k} \in]\pi/4, \pi/2]$ then $\sin\beta_{b_k} \geq \cos\beta_{b_k}$ and

$$\max\{\cos\beta_{b_k}, \sin\beta_{b_k}\} = \sin\beta_{b_k} = \sqrt{\frac{1-\cos 2\beta_{b_k}}{2}} = \sqrt{\frac{1+\epsilon_{b_k}}{2}}. \tag{3.102}$$

Plugging

$$\max\{\cos\beta_{b_k}, \sin\beta_{b_k}\} = \sqrt{\frac{1+\epsilon_{b_k}}{2}}, \tag{3.103}$$

into Lemma 3.5.3 completes the proof. □

STEP 4: COMPLETING THE PROOF

In this section we first we bound Bob's winning probability in terms of the absolute anti commutator ϵ_+, and then bound it by a quantity that Alice can evaluate experimentally since it is a function of the Bell violation she estimates during the testing phase.

We are now in a position to relate the guessing probability with the average incompatibility ϵ_+. That's to say we show that,

Lemma 3.5.5. *In* (3.76) *we bounded the winning probability in terms of* Λ*, which can be further bounded as follows*

$$\Lambda = 2^{-n} \sum_{k,b} p_k p_{b|k} \max_{\theta'} \sum_{\theta} \left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\| \leq 2^{-n} \sum_{w} \min\left(1, g\left(\vec{\epsilon}_+, w\right)\right), \tag{3.104}$$

where $w := \theta' \oplus \theta \in \{0,1\}^n$, $\epsilon_+ = \sum_{j \in \mathscr{J}} p_j \epsilon_j$, $\vec{\epsilon}_+$ *is the vector* $(\epsilon_+, \epsilon_+, \ldots, \epsilon_+)$*, and*

$$g(\vec{a}, w) := \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+a_k}{2}\right)^{w_k/2},$$

where $\vec{a}$ *is a vector* $(a_1, \ldots, a_k, \ldots, a_n)$*.*

Proof. Define

$$g(\epsilon_b, w) = \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\epsilon_{b_k}}{2}\right)^{w_k/2}, \; w := \theta' \oplus \theta \in \{0,1\}^n. \tag{3.105}$$

When we apply Lemma 3.5.4 we get the bound

$$\max_{\theta'} 2^{-n} \sum_{\theta} \left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\| \leq 2^{-n} \max_{\theta'} \sum_{\theta} \min\left(1, g(\epsilon_b, w)\right). \tag{3.106}$$

From (3.105), we observe that

$$\max_{\theta'} \sum_{\theta} \min\left(1, g(\epsilon_b, w)\right) = \sum_{w} \min\left(1, g(\epsilon_b, w)\right) \tag{3.107}$$

because the objective function to be maximized is independent of θ'. The objective function in the optimization of (3.76) can be bounded as

$$\sum_{k,b} p_k p_{b|k} \max_{\theta'} \sum_{\theta} 2^{-n} \left\| \sqrt{\Pi_b^{\theta',k}} \sqrt{\Pi_b^{\theta,k}} \right\| \tag{3.108}$$

$$\leq \sum_{k,b} p_k p_{b|k} 2^{-n} \sum_{w} \min\left(1, g(\epsilon_b, w)\right), \tag{3.109}$$

where the inner expression is independent of k. This is the uniform bound we mentioned. Performing the sum over k first gives

$$\sum_{k} p_k p_{b|k} \underset{(3.72)}{=} \sum_{k} p_k \operatorname{tr}(S_b \otimes \mathbb{1}_{B'} \rho_{AB'}^{k} S_b \otimes \mathbb{1}_{B'}) \tag{3.110}$$

$$= \operatorname{tr}(S_b \otimes \mathbb{1}_{B'K}\, \rho_{AB'K}\, S_b \otimes \mathbb{1}_{B'K}) \tag{3.111}$$

$$= \operatorname{tr}(S_b \sigma_A^{\otimes n} S_b) = \prod_{k=1}^{n} \operatorname{tr}(S_{b_k} \sigma_A S_{b_k}) = \prod_{k=1}^{n} p_{b_k} =: p_b. \tag{3.112}$$

where p_{b_k} for $b_k \in \mathscr{J}$ has been defined before (3.64).

Hence we see explicitly that while the attack of Bob may induce $p_{b|k}$ non-IID for some k, on average he cannot influence Alice's local IID state and therefore p_b remains IID

Swapping the order of summation over b and w and pulling the summation over b inside the minimum (which can only increase the value) gives the upper bound

$$2^{-n} \sum_{b,w} p_b \min\left(1, g(\epsilon_b, w)\right) \tag{3.113}$$

$$\leq 2^{-n} \sum_{w} \min\Big(1, \sum_{b} p_b g(\epsilon_b, w)\Big) \tag{3.114}$$

The sum inside the minimum,

$$\sum_{b} p_b g(\epsilon_b, w) = \sum_{b} p_b \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\epsilon_{b_k}}{2}\right)^{w_k/2}, \tag{3.115}$$

is a product of sums because p_b is a product (see eq. 3.112):

$$\sum_{b} p_b g(\epsilon_b, w) = \sqrt{d} \prod_{k=1}^{n} \sum_{j \in \mathscr{J}} p_j \left(\frac{1+\epsilon_j}{2}\right)^{w_k/2}. \tag{3.116}$$

Now each sum in the product can be bounded because of the concavity of the square root we get

$$\sum_b p_b g(\epsilon_b, w) \leq \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\epsilon_+}{2}\right)^{w_k/2} = g(\vec{\epsilon}_+, w) \tag{3.117}$$

hence we have

$$2^{-n} \sum_{b,w} p_b \min\left(1, g(\epsilon_b, w)\right) \tag{3.118}$$

$$\leq 2^{-n} \sum_{w} \min\left(1, g(\vec{\epsilon}_+, w)\right) \tag{3.119}$$

where $\epsilon_+ = \sum_{j \in \mathscr{J}} p_j \epsilon_j$ and $\vec{\epsilon}_+$ is the vector $(\epsilon_+, \epsilon_+, \ldots, \epsilon_+)$ □

The following Lemma forms the main result of this appendix. It bounds the winning probability $\lambda(n, d, \Gamma)$ by a function of d and ζ

Lemma 3.5.6. *In the perfect guessing game where Alice's devices behave IID and Bob has a quantum memory of dimension d, his winning probability is bounded by*

$$\lambda(n, d, \Gamma) \leq 2^{-n} \left[\sum_{k=0}^{t} \binom{n}{k} + \sqrt{d} \sum_{k=t+1}^{n} \binom{n}{k} \left(\frac{1+\zeta}{2}\right)^{k/2} \right], \tag{3.120}$$

where t is the threshold defined as

$$t := \left\lfloor -\log d \cdot \left[\log\left(\frac{1+\zeta}{2}\right) \right]^{-1} \right\rfloor \tag{3.121}$$

and $\zeta := \frac{S}{4}\sqrt{8 - S^2}$ with S being the CHSH *violation as defined in Lemma 3.2.4.*

Proof. Combine (3.119) with (3.105) and (3.76) and note that the maximizations over all strategies of Bob drop out because we have bounded the winning probability of an arbitrary strategy. Therefore, we obtain

$$\lambda(n, d, \Gamma) \leq 2^{-n} \sum_{w} \min\left\{1, \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\epsilon_+}{2}\right)^{w_k/2}\right\}. \tag{3.122}$$

Using Lemma 3.2.4 we have $\epsilon_+ \leq \zeta$ and then

$$\lambda(n, d, \Gamma) \leq 2^{-n} \sum_{w} \min\left\{1, \sqrt{d} \prod_{k=1}^{n} \left(\frac{1+\zeta}{2}\right)^{w_k/2}\right\}. \tag{3.123}$$

Since the right-hand side depends only on the Hamming weight of $w \in \{0,1\}^n$ it is easy to perform the minimization explicitly, which yields

$$\lambda(n, d, \Gamma) \leq 2^{-n} \left[\sum_{k=0}^{t} \binom{n}{k} + \sqrt{d} \sum_{k=t+1}^{n} \binom{n}{k} \left(\frac{1+\zeta}{2}\right)^{k/2} \right], \tag{3.124}$$

where t is the threshold defined in the Lemma. □

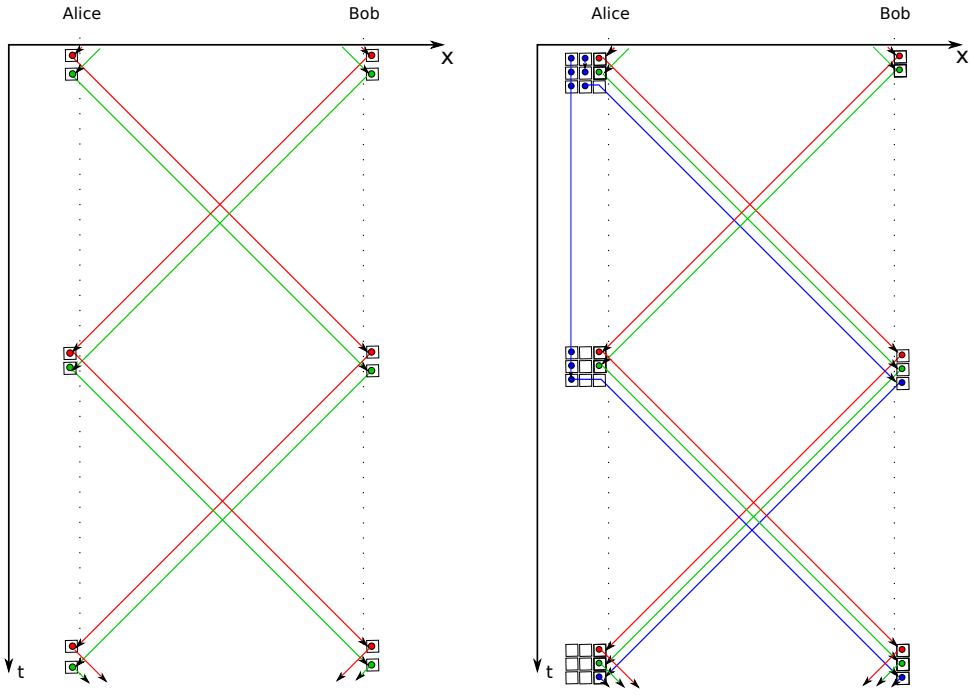


Figure 3.4: On the left hand side an illustration on how to store a certain number of qubits (here two EPR pairs, the red and the green pairs) in an arbitrary large quantum channel thanks to one qubit memory on each side. Alice and Bob keep forwarding each other their half of an entangled state in such a way that the state is preserved in the quantum channel. The right hand side figure illustrates how to create another EPR pair (here the blue EPR pair) using three qubits memory on Alice's side and one on Bob's side. These constructions works for an arbitrarily high amount of EPR pairs by iterating the procedure.

3.5.3. CHEATING STRATEGY USING UNLIMITED QUANTUM CHANNELS

The Figure 3.4 shows how using unbounded quantum channels one can store (left) and create (right) an arbitrary amount of entanglement without having access to more that four qubits memory. This shows that having access to arbitrary quantum channels would allow dishonest parties to prepare and share an arbitrary large amount of entanglement, and therefore it would allow them to successfully attack PV.

REFERENCES

[1] J. Kaniewski and S. Wehner, *Device-independent two-party cryptography secure against sequential attacks,* New Journal of Physics **18**, 055004 (2016).

[2] J. Ribeiro and F. Grosshans, *A tight lower bound for the BB84-states quantum-position-verification protocol,* arXiv:1504.07171 (2015).

[3] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, Advances in Cryptology - CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2007. Proceedings (Springer Berlin Heidelberg, Berlin, Hei-

delberg, 2007) Chap. Secure Identification and QKD in the Bounded-Quantum-Storage Model, pp. 342–359.

[4] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *Cryptography in the bounded quantum storage model,* BRICS Report Series **12** (2005), 10.7146/brics.v12i20.21886.

[5] S. Wehner, C. Schaffner, and B. M. Terhal, *Cryptography from noisy storage,* Phys. Rev. Lett. **100**, 220502 (2008).

[6] F. Dupuis, O. Fawzi, and S. Wehner, *Entanglement sampling and applications,* IEEE Transactions on Information Theory **61**, 1093 (2015).

[7] R. Konig, S. Wehner, and J. Wullschleger, *Unconditional security from noisy quantum storage,* IEEE Transactions on Information Theory **58**, 1962 (2012).

[8] D. Mayers, *Unconditionally secure quantum bit commitment is impossible,* Phys. Rev. Lett. **78**, 3414 (1997).

[9] H.-K. Lo and H. F. Chau, *Why quantum bit commitment and ideal quantum coin tossing are impossible,* Physica D Nonlinear Phenomena **120**, 177 (1998), quant-ph/9711065 .

[10] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, *An experimental implementation of oblivious transfer in the noisy storage model,* Nature Communications **5**, 3418 (2014), arXiv:1308.5098 [quant-ph] .

[11] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner, *Experimental implementation of bit commitment in the noisy-storage model,* Nature Communications **3**, 1326 (2012), arXiv:1205.3331 [quant-ph] .

[12] A. Kent, W. J. Munro, and T. P. Spiller, *Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints,* Phys. Rev. A **84**, 012326 (2011).

[13] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *Position-based quantum cryptography: Impossibility and constructions,* SIAM Journal on Computing **43**, 150 (2014), http://dx.doi.org/10.1137/130913687 .

[14] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, *A monogamy-of-entanglement game with applications to device-independent quantum cryptography,* New Journal of Physics **15**, 103002 (2013).

[15] R. A. Malaney, *Location-dependent communications using quantum entanglement,* Phys. Rev. A **81**, 042319 (2010).

[16] U. Vazirani and T. Vidick, *Fully device-independent quantum key distribution,* Phys. Rev. Lett. **113**, 140501 (2014).

[17] J. Barrett, R. Colbeck, and A. Kent, *Unconditionally secure device-independent quantum key distribution with only two devices,* Phys. Rev. A **86**, 062326 (2012).

[18] B. W. Reichardt, F. Unger, and U. Vazirani, Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS '13 (ACM, New York, NY, USA, 2013) pp. 321–322.

[19] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, *Fully distrustful quantum bit commitment and coin flipping,* Phys. Rev. Lett. **106**, 220501 (2011).

[20] A. Kent, *Quantum tagging for tags containing secret classical data,* Phys. Rev. A **84**, 022335 (2011).

[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Phys. Rev. Lett. **23**, 880 (1969).

[22] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* Theoretical Computer Science **560, Part 1**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}.

[23] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography,* Phys. Rev. Lett. **110**, 010503 (2013).

[24] J. Kaniewski, M. Tomamichel, and S. Wehner, *Entropic uncertainty from effective anticommutators,* Phys. Rev. A **90**, 012332 (2014).

[25] D. Nagaj, P. Wocjan, and Y. Zhang, *Fast Amplification of QMA,* QIC Vol.9 No.11&12, 1053-1068 (2009), arXiv:0904.1549 [quant-ph] .

[26] O. Regev, *Witness-preserving QMA amplification,* Quantum Computation Lecture notes, Spring 2006, Tel Aviv University (2006).

[27] M. Berta, F. G. S. L. Brandão, M. Christandl, and S. Wehner, *Entanglement cost of quantum channels,* IEEE Transactions on Information Theory **59**, 6779 (2013).

[28] F. G. S. L. Brandao and N. Datta, *One-shot rates for entanglement manipulation under non-entangling maps,* arXiv:0905.2673 (2009), arXiv:0905.2673 [quant-ph] .

[29] F. Kittaneh, *Norm inequalities for certain operator sums,* Journal of Functional Analysis **143**, 337 (1997).

4

FULLY DEVICE-INDEPENDENT CONFERENCE KEY AGREEMENT

Jérémy RIBEIRO, Gláucia MURTA, Stephanie WEHNER

We present the first security analysis of conference key agreement (CKA) in the most adversarial model of device independence (DI). Our protocol can be implemented by any experimental setup that is capable of performing Bell tests (specifically, we introduce the "Parity-CHSH" inequality), and security can in principle be obtained for any violation of the Parity-CHSH inequality. We use a direct connection between the N-partite Parity-CHSH inequality and the CHSH inequality. Namely the Parity-CHSH inequality can be considered as a CHSH inequality or an another CHSH inequality (equivalent up to relabelling) depending on the parity of the output of $N-2$ of the parties. We compare the asymptotic key rate for DICKA to the case where the parties use $N-1$ DIQKD protocols in order to generate a common key. We show that for some regime of noise the DICKA protocol leads to better rates.

Parts of this chapter have been published in Phys. Rev. A, **97:022307**, 2018.

4.1. INTRODUCTION

Significant efforts have been undertaken to establish the security of device-independent (DI) QKD [1–7], leading to ever more sophisticated security proofs. Initial proofs assumed a simple model in which the devices act independently and identically (IID) in each round of the protocol. This significantly simplifies the security analysis since the underlying properties of the devices may first be estimated by gaining statistical confidence from the observation of the measurement outcomes in the tested rounds. The main challenge overcome by the more recent security proofs [4–7] was to establish security even if the devices behave arbitrarily from one round to the next, including having an arbitrary memory of the past that they might use to thwart the efforts of Alice and Bob. Assuming that the devices carry at least some memory of past interactions is an extremely realistic assumption due to technical limitations, even if Alice and Bob prepare their own trusted, but imperfect, devices, highlighting the extreme importance of such analyses for the implementation of device-independent QKD. In contrast, relatively little is known about device independence outside the realm of QKD [8–12].

Conference key agreement [13–15] (CKA or N-CKA) is the task of distributing a secret key among N parties. In order to achieve this goal, one could make use of $N-1$ individual QKD protocols to distribute $N-1$ different keys between one of the parties (Alice) and the others ($\text{Bob}_1, \ldots, \text{Bob}_{N-1}$), followed by Alice using these keys to encrypt a common key to all the participants. However the existence of genuine multipartite quantum correlations can bring some advantage to multipartite tasks, and, as shown in Ref. [15], exploring properties of genuine multipartite entanglement can lead to protocols with better performance for conference key agreement.

Here we present the first security analysis of conference key agreement in the most adversarial model of device independence. Our protocol can be implemented using any experimental setup that is capable of violating the Parity-CHSH inequality that we introduce in Def. 4.2.1. Our proof is based on a the connection between the Parity-CHSH inequality and the CHSH inequality [16]. We also compare the asymptotic rates obtained for DICKA with the implementation of $N-1$ independent DIQKD, and show that for some regime of noise it is advantageous to perform DICKA.

This chapter is organized as follows: In Section 4.1.1 we informally present the main results of the chapter. In Section 4.1.2 we quickly remind the reader with some the notation and some definitions and theorems (in particular the Entropy Accumulation Theorem) which are going to be used in the main proofs. We finish discussing the set of hypothesis contained in the device-independent (DI) model. In Section 4.2, we state the DICKA protocol and present the detailed security proof. In Section 4.3 we present the noise model to compare the asymptotic key rate of the DICKA protocol to the case where the parties perform $N-1$ independent DIQKD protocols in order to generate a common key.

4.1.1. RESULTS

In this section we present the results of this chapter: we propose a new protocol for CKA, and analyse its security in the device-independent setting. We then compare the asymptotic key rate of our N-partite CKA protocol to the key rate of a protocol based on $(N-1)$ executions of DIQKD [7].

THE PROTOCOL

Here we present our protocol for DICKA using a N-partite GHZ state and using a Bell test based on a variation of the CHSH inequality that we call the Parity-CHSH inequality which we introduce in section 4.2.1.

For a device-independent implementation of CKA, we consider a protocol with N parties: Alice who possesses one device with two inputs $\{0,1\}$, and Bob_1 who possesses a device with three inputs $\{0,1,2\}$, and ,Bob_2,...,Bob_{N-1} who possess each one device with two inputs $\{0,1\}$. Every device has two outputs. During the protocol, Alice and the Bobs randomly choose some rounds to test for the violation of the Parity-CHSH inequality. They abort the protocol if the frequency of rounds where they win the Parity-CHSH game do not reach a specified threshold δ. We also consider that Alice has a source for generation of the states, which is independent of her measurement device.

Protocol 4.1.1 (DICKA)**.**

1. *For every round $i \in [n]$ do:*
   (a) *Alice uses her source to produce and distribute an N-partite state, $\rho_{A_i B_{(1\ldots N-1),i}}$, shared among herself and the $N-1$ Bobs.*
   (b) *Alice randomly picks T_i, s.t. $P(T_i = 1) = \mu$, and publicly communicates it to all the Bobs.*
   (c) *If $T_i = 0$ Alice and the Bobs choose $(X_i, Y_{(1\ldots N-1),i}) = (0,2,0,...,0)$, and if $T_i = 1$ Alice chooses $X_i \in_R \{0,1\}$ uniformly at random, Bob_1 chooses $Y_{(1),i} \in_R \{0,1\}$ uniformly at random, and Bob_2,...,Bob_{N-1} choose $(Y_{(2\ldots N-1),i}) = (1,\ldots,1)$.*
   (d) *Alice and the Bobs input the previously chosen values in their respective device and record the outputs as $A'_i, B'_{(1\ldots N-1),i}$.*
2. *They all communicate publicly the list of bases $X_1^n Y_{(1\ldots N-1)1}^n$ they used.*
3. ***Error correction:** Alice and the Bobs apply an error correction protocol. We call O_A the classical information that Alice sends to the Bobs. For the purpose of parameter estimation, the Bobs also send some error correction information for the bits produced during the test rounds ($T_i = 1$), we denote $O_{(k)}$ the error correction information sent by Bob_k. If the error correction protocol aborts for at least one Bob then they abort the protocol. If it does not abort they obtain the raw keys $\tilde{K}_A = A', \tilde{K}_{B_{(1\ldots N-1)}}$.*
4. ***Parameter estimation:** For all the rounds i such that $T_i = 1$, Alice uses A'_i and her guess on $B'_{(1\ldots N-1),i}$ to set $C_i = 1$ if they have won the N-partite Parity-CHSH game in the round i, and she sets $C_i = 0$ if they have lost it. Finally she sets $C_i = \perp$ for the rounds i where $T_i = 0$. She aborts if $\sum_i C_i < \delta \cdot \sum_i T_i$, where $\delta \in]3/4, 1/2 + 1/2\sqrt{2}[$.*

5. ***Privacy amplification:*** *Alice and the Bobs apply a privacy amplification protocol to create final keys $K_A, K_{B_{(1\ldots N-1)}}$. We denote S the classical information publicly sent by Alice during this step.*

In this protocol, the ideal state one would like to produce in each round is a N-partite GHZ state. The parties' measurements, ideally, correspond to single qubit Pauli measurements. More details on the measurements are given in Section 4.2.2.

Security Definitions. For completeness, before stating our main result, which establishes the secret key length of Protocol 4.1.1, we first formalise what it means for a DICKA protocol to be secure. As for QKD [17, 18] the security of conference key agreement [15] can be split into two terms: correctness and secrecy. Correctness is a statement about how sure we are that the N parties share identical keys, and secrecy is a statement about how much information the adversary can have about Alice's key.

Definition 4.1.2. *(Correctness and secrecy (informal)) A DICKA protocol is ϵ_{corr}-correct if Alice's and Bobs' keys, K_A, $K_{B_{(1)}}, \ldots, K_{B_{(N-1)}}$, are all identical with probability at least $1-\epsilon_{\text{corr}}$. And it is ϵ_{sec}-secret, if Alice's key K_A is ϵ_{sec}-close to a key that Eve is ignorant about. This condition can be formalized as*

$$p_{\hat{\Omega}} \cdot \left\| \rho_{K_A E|\hat{\Omega}} - \frac{\mathbb{1}_A}{2^l} \otimes \rho_{E|\hat{\Omega}} \right\|_{\text{tr}} \leq \epsilon_{\text{sec}},$$

where $\|\cdot\|_{tr}$ denotes the trace norm, l is the key length, $\hat{\Omega}$ is the event of the protocol not aborting, and $p_{\hat{\Omega}}$ is the probability for $\hat{\Omega}$.

If a protocol is ϵ_{corr}-correct and ϵ_{sec}-secret then it is ϵ^s-correct-and-secret for any $\epsilon^s \geq \epsilon_{\text{corr}} + \epsilon_{\text{sec}}$.

A more complete definition can be found in Chapter 2 section 2.4.2.

So in general when we say that a CKA (or a QKD) protocol is ϵ^s secure, we mean that for any possible physical implementation of the protocol, either it aborts with probability higher than $1-\epsilon^s$ or it is ϵ^s-correct-and-secret, according to Definition 2.4.6 (see section 4.2.2).

A combination of Definition 2.4.6 and the Leftover Hash Lemma (see Theorem 2.3.6 or [17]) relates the length of a secret key, that can be obtained from a particular protocol, with the smooth min-entropy of Alice's raw key A' conditioned on Eve's information (see [17] for a detailed derivation of this statement): An ϵ_{sec}-secret key of size

$$l = H_{\min}^{\epsilon}(A'|E) - 2\log\frac{1}{\epsilon_{PA}} \tag{4.1}$$

can be obtained, for $\epsilon_{sec} > 2\epsilon + \epsilon_{PA}$. The conditional smooth min-entropy is defined as $H_{\min}^{\epsilon}(A|E)_\rho := \sup_{\sigma\in\mathcal{B}(\rho)} H_{\min}(A|E)_\sigma$ (see Chapter 2).

Our main result establishes the length of a secure key that can be obtained from Protocol 4.1.1.

Theorem 4.1.3. *Protocol 4.1.1 generates an ϵ^s-correct-and-secret key, with $\epsilon^s \leq \epsilon_{\text{PA}} + 2(N-1)\epsilon'_{\text{EC}} + 2\epsilon + \epsilon_{\text{EA}}$, of length:*

$$\begin{aligned} l = \max_{p_{\min} \leq \delta_{\text{opt}} \leq p_{\max}} & \left((f(\delta, \delta_{\text{opt}}) - \mu) \cdot n - \tilde{v}\sqrt{n} \right) \\ & + 3\log(1 - \sqrt{1 - (\epsilon/4)^2}) - 2\log(\epsilon_{\text{PA}}^{-1}) \\ & - \text{leak}_{\text{EC}}(O_A) - \sum_{k=1}^{N-1} \text{leak}_{\text{EC}}(O_{(k)}), \end{aligned} \tag{4.2}$$

where ϵ'_{EC} is an error parameter of the error correction protocol, ϵ_{PA} is the privacy amplification error probability, ϵ_{EA} is a chosen security parameter for the protocol, and ϵ is a smoothing parameter. δ is the specified threshold bellow which the protocol aborts. The function $f(\cdot, \delta_{\text{opt}})$ is the tangent of $\hat{f}(\cdot)$ (defined in Lemma 4.2.9) in the point δ_{opt}, where $\delta_{\text{opt}} \in]3/4, 1/2 + 1/2\sqrt{2}[$ is a parameter to be optimized. $\tilde{v} = 2\big(\log(13) + (\hat{f}'(p_{\text{opt}})/\mu + 1)\big)\sqrt{1 - 2\log(\epsilon \cdot \epsilon_{\text{EA}})} + 2\log(7)\sqrt{-\log(\epsilon_{\text{EA}}^2(1 - \sqrt{1 - (\epsilon/4)^2}))}$. And the leakages due to error correction, leak_{EC}*, can be estimated according to a particular implementation of the protocol.*

The security proof of Protocol 4.1.1 consists of two main steps: We first use the recently developed Entropy Accumulation Theorem [19] to split the overall entropy of Alice's string, produced during the protocol, into a sum of the entropy produced on each round of the protocol. Then we develop a new method to bound the entropy produced in one round by a function of the violation of the N-partite Parity-CHSH inequality, which generalises the bound for the bipartite case derived in [1, 2]. An expanded and detailed derivation of Theorem 4.1.3 is presented in Section 4.2.

ASYMPTOTIC KEY RATE AND COMPARISON WITH DIQKD BASED PROTOCOL

In this section we compare (Fig. 4.1) the asymptotic key rate achieved by our N-partite DICKA protocol to the asymptotic key rate of protocol based on $N-1$ execution of the DIQKD protocol presented in [7]. We do this assuming that the noise affecting the qubits is a depolarizing noise.

We remark that bipartite QKD has of course been studied in the device-independent setting [7], but as we are going to see in Figure 4.1, a conference key agreement protocol can be beneficial for certain regimes of noise.

Using Theorem 4.1.3 we get a lower bound on the length of secret key we can obtain with Protocol 4.1.1, which, when divided by the number of rounds n, gives us a lower bound on the secret key rate.

In order to calculate the secret key rate, we also need to estimate the leakages due to error correction, and for that we need to specify the model for an honest implementation. Modeling the noise on the distributed state as a depolarising noise we get:

$$\text{leak}_{\text{EC}}(O_A) \leq ((1-\mu)h(Q) + \mu)n + \mathcal{O}(\sqrt{n}), \tag{4.3}$$

and

$$\text{leak}_{\text{EC}}(O_{(k)}) \leq \mu n + \mathcal{O}(\sqrt{n}), \tag{4.4}$$

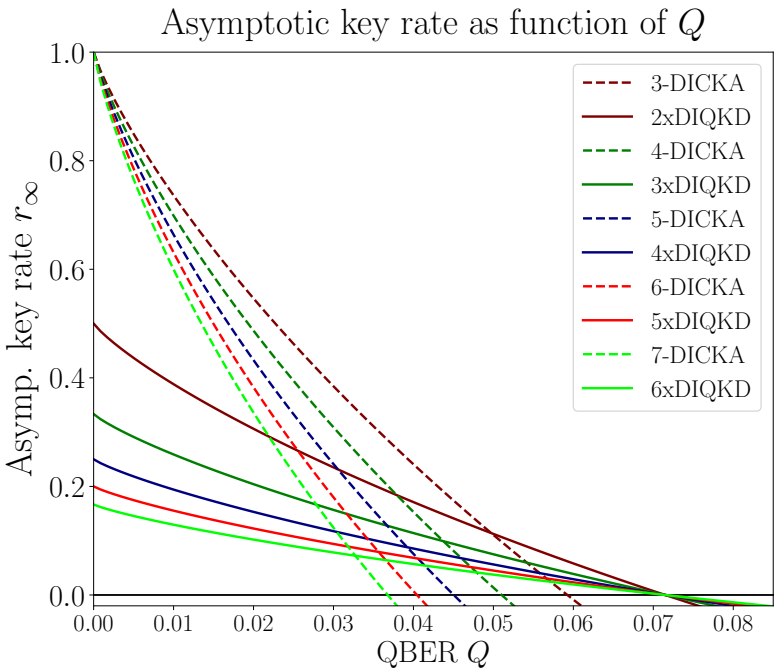


Figure 4.1: Asymptotic key rate for N-DICKA (dashed lines), and for the distribution of a secret key between N parties through $N-1$ DIQKD protocols (solid lines), when each qubit experiences independent bit errors measured at a bit error rate (QBER) Q. From top to bottom, the lines correspond to $N = \{3,4,5,6,7\}$. We observe that for low noise regime it is advantageous to use DICKA instead of $(N-1)\times$DIQKD [7]. In general, the comparison between the two methods depends on the cost and noisiness of producing GHZ states over pairwise EPR pairs.

where Q is the quantum bit error rate (QBER) between Alice and one of the Bobs. A detailed calculation of the leakage for this particular noise model is presented in Section 4.3.

Using this estimation of the leakage in the bounds for the key length (4.15), and by taking $\mu \to 0$, s.t. $\mu\sqrt{n} \to \infty$, we get the asymptotic key rate for Protocol 4.1.1:

$$r^{\infty}_{N\text{-DICKA}} = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\left(\frac{\sqrt{1-2Q}^{N}}{2\sqrt{2}} + \frac{(1-2Q)\left(1-\sqrt{1-2Q}^{N-2}\right)}{8\sqrt{2}}\right)^{2} - 1}\right) - h(Q). \tag{4.5}$$

We compare the above rate with the one we would have if Alice was performing $N-1$

DIQKD protocols in order to establish a common key with all the Bobs [7]:

$$r^{\infty}_{(N-1)\times\text{DIQKD}} = \frac{1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{2(1-2Q)^2 - 1}\right) - h(Q)}{N-1}. \tag{4.6}$$

Because when Alice runs $N-1$ DIQKD protocols she needs n rounds for each of the $N-1$ Bobs, the key rate $r^{\infty}_{(N-1)\times\text{DIQKD}}$ gets a factor of $\frac{1}{N-1}$. Note that here we consider that the cost for locally producing an N-partite GHZ state is comparable to the cost of producing EPR pairs. An analysis taking into account these costs for particular implementations will lead to a more fair comparison.

A comparison of these key rate is given in Figure 4.1, where we see that in some regime of noise, it can be advantageous to use the N-partite DICKA Protocol 4.1.1 instead of $N-1$ independent DIQKD protocols.

Remark 4.1.4. *We remark that proving advantage for a small number of parties already leads to better protocols for networks. Indeed, instead of using DIQKD as building block for a N-DICKA protocol (for large N), one can use k-DICKA protocols, upon availability of k-GHZ states for $k = 3, 4$ or 5.*

4.1.2. PRELIMINARIES

Before going into the proof of our main Theorem 4.1.3, we state the model and assumptions we use in this Chapter. This preliminary section is mostly a reminder for the reader since most of the model and assumptions have been explained in Chapter 2

NOTATION

If we deal with a system composed with N subsystems within a round i of a protocol we denote $A_{(k\ldots l),i}$ for $A_{(k),i}, \ldots A_{(l),i}$ $(k,l \in [N] : k \leq l)$, where $A_{(k),i}$ is the k^{th} subsystem of the round i. If we deal with a system composed of n subsystems across the n rounds of a protocol we denote A_k^l for $A_k, \ldots, A_l$ $(k,l \in [n] : k \leq l)$. Therefore $A_{(k\ldots l)}{}_m^o$ is a short for $A_{(k\ldots l),m}, \ldots A_{(k\ldots l),o}$ $(k,l \in [N], m,o \in [n] : k \leq l, m \leq o)$.

We define a cq-state $\rho_{XA|\Omega}$ conditioned on an event $\Omega \subset \mathscr{X}$ as,

$$\rho_{XA|\Omega} := \frac{1}{p_\Omega} \sum_{x\in\Omega} p_x \cdot |x\rangle\langle x|_X \otimes \rho_{A|x}, \text{ where } p_\Omega := \sum_{x\in\Omega} p_x. \tag{4.7}$$

We will denote by CPTP maps the linear maps that are Completely Positive and Trace Preserving.

Let $\mathscr{C}$ be an alphabet, and $C_1, \ldots, C_n$ be n random variables on this alphabet. We call $\text{freq}(C_1^n)$ the vector whose components labeled by $c \in \mathscr{C}$ are the frequencies of the symbol c:

$$\text{freq}(C_1^n)_c := \frac{|\{i : C_i = c\}|}{n}.$$

ENTROPIES

Throughout this work we will make use the smooth min- (max-) entropy as defined in Chapter 2. Moreover in this chapter we use the Entropy Accumulation Theorem (EAT). The statement of the EAT is quite technical so give in this section a very short reminder.

For more details about the EAT we advise the reader who is not very familiar with this theorem to refer to Chapter 2 Section 2.3.3 on page 30.

Theorem 4.1.5 (The Entropy Accumulation Theorem (EAT) [7, 19])**.** *For $1 \leq i \leq n$ let $\mathcal{M}_i$ be a EAT channel from register R_{i-1} to $A_iB_iC_iR_i$, and let $\rho_{A_1^nB_1^nE}$ of the form,*

$$\rho_{A_1^nB_1^nE} = \mathrm{tr}_{R_n}(\mathcal{M}_n \circ \ldots \circ \mathcal{M}_1(\rho_{R_0E})). \tag{4.8}$$

Let $f_{\min}$ be an affine min-tradeoff function, and $f_{\max}$ be an affine max-tradeoff function. For an event Ω that happens with probability $p(\Omega)$, and for t such that $f_{\min}(\mathsf{freq}(c_1^n)) \geq t$ $\forall\ c_1^n \in \Omega$, it holds that

$$H_{\min}^{\epsilon}(A_1^n|B_1^nE)_{\rho_{|\Omega}} > nt - \nu\sqrt{n} \tag{4.9}$$

and similarly, for t' such that $f_{\max}(\mathsf{freq}(c_1^n)) \leq t'$ $\forall\ c_1^n \in \Omega$,

$$H_{\max}^{\epsilon}(A_1^n|B_1^nE)_{\rho_{|\Omega}} < nt' + \nu\sqrt{n} \tag{4.10}$$

with

$$\nu = 2\left(\log(1+2d_A) + \lceil\|\nabla f\|_{\infty}\rceil\right)\sqrt{1-2\log\left(\epsilon_s \cdot p(\Omega)\right)} \tag{4.11}$$

for f equals to $f_{\min}$ and $f_{\max}$ respectively .

In simple terms the EAT allows to decompose the conditioned smooth (max) min-entropy of a string into the sum of the Von Neumann entropy of each element of the string which is itself bounded by the (max) min-tradeoff function..

DEVICE-INDEPENDENT ASSUMPTIONS

In this section we remind the reader the assumptions we make in the Device-Independent scenario and comment upon them.

Assumptions 4.1.6. *Our DICKA protocol considers N parties, namely Alice, $Bob_1, \ldots, Bob_{N-1}$, and the eavesdropper, Eve. They satisfy the following assumptions:*

1. *Each party is in a lab which is isolated from the outside (in particular from Eve). As a consequence no non-intended information can go in or out of the labs.*
2. *Each party holds a trusted random number generator (RNG).*
3. *All classical communications between the parties are assumed to be authenticated, and all classical operations are assumed to be trusted.*
4. *Each party has a measurement device in their lab in which they can input classical information and which outputs 0 or 1. The measurement devices are otherwise arbitrary, and therefore could be prepared by Eve.*
5. *Alice has a source that produces some N partite quantum state $\rho_{A_iB_{(1\ldots N-1),i}}$ in the round i. We allow Eve to hold the purification of $\rho_{A_1^nB_{(1\ldots N-1)}{}_1^n}$ (the state between Alice and the Bobs for the n rounds of the protocol) and we denote the pure global state $\rho_{A_1^nB_{(1\ldots N-1)}{}_1^nE}$. This source is also assumed to be arbitrary, and therefore we can assume that it is prepared by Eve.*

6. *We will assume that Alice's source and her measurement device are independent (e.g. Alice can isolate the source from the measurement device). Therefore there is no non-intended communication between the source and her measurement device.*

Point 6 of Assumptions 4.1.6 is usually not explicitly stated in previous works on device-independent QKD, however we remark that this assumption is also present in all previous protocols. Indeed assumption 6 is important to guarantee that no extra information about the outcomes of Alice's device is leaked to Eve (since Alice and Bob are in isolated labs), apart from what she can learn from the purifying system in her possession and the classical communication intentionally leaked during the protocol. Previous protocols usually assume that an external source is responsible for producing the states. However note that in order to distribute the states to Alice and Bob's devices one need a quantum channel connecting the external source with their labs, and similarly it is assumed that no information from the devices is leaked through this quantum channel. An alternative approach is to assume that the full state for the n rounds of the protocol is already shared between the two parties at the very beginning of the protocol (and any quantum channel connecting the source and the devices is disconnected once the protocol starts). However this is an unrealistic assumption, since an implementation of such protocol would require quantum memory to last for the entire duration of the protocol. For that reason, here we chose NOT to assume that the state is already shared among all the parties, and assumption 6 prevents the simple attack described in [20, Appendix C], where the outcome of round i is leaked throughout the state transmitted to Bob in the next rounds.

4.2. FROM SELF-TESTING TO DEVICE-INDEPENDENT CONFERENCE KEY AGREEMENT

The Clauser-Horne-Shimony-Holt (CHSH) inequality [16] has been successfully used to prove security of DIQKD [7] in the most adversarial scenario, where only a minimal set of assumptions (similar to Assumptions 4.1.6) is required. The main point of using the CHSH inequality for cryptographic protocols is due to its self-testing properties, which allows one to derive properties about the devices used during the protocol. Therefore, in order to prove the security of Device-Independent Conference Key Agreement (DICKA) it is very natural to think of an N-partite extension of the CHSH inequality.

In this section we will start by introducing our new N-partite Parity-CHSH inequality, which we devise in such a way that it closely relates to the CHSH inequality. Then, we presents our DICKA protocol in details and prove its security using the connection between our Parity-CHSH inequality and the CHSH inequality.

4.2.1. FROM CHSH INEQUALITY TO "PARITY-CHSH" INEQUALITY.

In this section we present our new Parity-CHSH inequality, that is derived from the CHSH inequality in such a way that a N-partite GHZ state can maximally violate it.

The CHSH inequality [16] a two-partite inequality that has already proven its usefulness for device-independent protocols [1, 2, 4–7, 9, 21, 22]. In this section we introduce a slightly different inequality for N parties. Indeed we use the fact that a $N-$partite GHZ state can be turned into either $\Phi^+ := \frac{(|00\rangle+|11\rangle)(\langle 00|+\langle 11|)}{2}$ or $\Phi^- := \frac{(|00\rangle-|11\rangle)(\langle 00|-\langle 11|)}{2}$. by

measuring $N-2$ parties in the X basis. More precisely if the parity of the outcomes of the $N-2$ measurements in the X basis is 0 then the state on the remaining 2 parties is Φ^+, and if the parity of these outcomes is 1 then the state on the remaining systems is Φ^-.

The state Φ^+ can be used to maximally violate the CHSH inequality, and Φ^- can be used to maximally violate an equivalent inequality. Therefore one would expect that the GHZ state can violate a mixing these two CHSH inequality depending on whether we create a state Φ^+ or Φ^-.

We remind the reader with the definition of the CHSH inequality in order to later define our new Parity-CHSH inequality.

Definition (CHSH inequality)**.** *Let Alice and Bob be the two players in this game called the CHSH game. At the beginning of the game, they are both asked a uniformly random binary question $x \in \{0,1\}$ and $y \in \{0,1\}$ respectively. They then have to answer bit a and b respectively. They win the game if and only if*

$$a + b = xy \ mod\, 2.$$

No communication is allowed between Alice and Bob during the game. They can, however, agree on any strategy before the start of the game. The CHSH inequality states that by using a classical strategy – i.e. modeled with local hidden variables – Alice and Bob's winning probability must satisfy the following,

$$P_w^{\text{CHSH}} \leq \frac{3}{4}. \tag{4.12}$$

The state Φ^+ allows to reach the maximum winning probability achievable by quantum mechanics, *i.e.* it allows for $P_w^{\text{CHSH}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85$. Similarirly Φ^- allows to reach the maximum winning probability achievable quantum mechanics($P_w \approx 0.85$) for a game equivalent (up to relabelling) to the CHSH game, in which the winning condition is $a + b = x(y+1) \bmod 2$.

Our new "Parity-CHSH" inequality extends the CHSH inequality to N parties as follows.

Definition 4.2.1 (Parity-CHSH inequality)**.** *Let Alice, $Bob_1, \ldots, Bob_{N-1}$ be the N players of the following game (the Parity-CHSH game). Alice and Bob_1 are asked uniformly random binary questions $x \in \{0,1\}$ and $y \in \{0,1\}$ respectively. The other Bobs are each asked a fixed question, e.g. always equal to 1. The parties all answer bits $a, b_1, \ldots, b_{N-1}$ respectively. We denote by,*

$$\bar{b} := \bigoplus_{2 \leq i \leq N-1} b_i,$$

the parity of the all answers of $Bob_2, \ldots, Bob_{N-1}$. The players win if and only if

$$a + b_1 = x(y + \bar{b}) \ mod\, 2. \tag{4.13}$$

No communication is allowed between Alice and Bob during the game. They can, however, agree on any strategy before the start of the game. As for the CHSH inequality, classical strategies for the Partity-CHSH game must satisfy,

$$P_w^{\text{Parity-CHSH}} \leq \frac{3}{4}. \tag{4.14}$$

Remark 4.2.2. *Note that if we condition on $\bar{b} = 0$, the game is essentially the CHSH game. When conditioned on $\bar{b} = 1$ the Parity-CHSH game reduces to a game equivalent to the CHSH up to relabelling the question y.*

4.2.2. DEVICE-INDEPENDENT CONFERENCE KEY AGREEMENT

We now present a device-independent conference key agreement (DICKA) protocol and prove its security in two steps. We first use the recently developed Entropy Accumulation Theorem [19] to split the overall entropy of Alice's string produced during the protocol, into a sum of entropy produced on each round of the protocol. Then we use the relation between the Parity-CHSH inequality and the CHSH inequality, to bound the entropy produced in one round by a function of the violation of the N-partite Parity-CHSH inequeality, which generalize the bounds found for the bipartite case in [2].

THE PROTOCOL

In this chapter we work with the security Definition 2.4.6 of Chapter 2, which we have already informally spelled out in the Results section of this chapter.

We remark again that this definition was proven to be a criteria for composable security for Quantum Key Distribution in the device dependent scenario [18]. However, for the device-independent case it is not known whether such a criteria is enough for composable security. Indeed, Ref. [23] suggests that this is not the case if the same devices are used for generation of a subsequent key since this new key can leak information about the first key. Following Ref. [7] we choose to adopt Definition 2.4.6 as the security criteria for DICKA.

We now prove that the DICKA Protocol 4.2.3, under the Assumptions 4.1.6, satisfies the above definitions of security. For completeness we re-state the protocol here.

Protocol 4.2.3 (More detail version of Protocol 4.1.1)**.** *The protocol runs as follows for N parties:*

1. *For every round $i \in [n]$ do:*
   - (a) *Alice uses her source to produce and distribute a N-partite state, $\rho_{A_i B_{(1\ldots N-1),i}}$, shared among herself and the $N-1$ Bobs.*
   - (b) *Alice randomly picks T_i , s.t. $P(T_i = 1) = \mu$, and publicly communicates it to all the Bobs.*
   - (c) *If $T_i = 0$ Alice and the Bobs choose $(X_i, Y_{(1\ldots N-1),i}) = (0,2,0,\ldots,0)$, and if $T_i = 1$ Alice chooses $X_i \in_R \{0,1\}$ uniformly at random, Bob_1 chooses $Y_{(1),i} \in_R \{0,1\}$ uniformly at random, and $Bob_2,\ldots,Bob_{N-1}$ choose $(Y_{(2\ldots N-1),i}) = (1,\ldots,1)$.*
   - (d) *Alice and the Bobs input the value they chose previously in their respective device and record the output as $A'_i, B'_{(1\ldots N-1),i}$*
2. *They all communicate publicly the list of bases $X_1^n Y_{(1\ldots N-1)}{}_1^n$ they used.*

3. ***Error correction:*** *Alice and the Bobs apply an error correction protocol. Here we chose a protocol based on universal hashing [24, 25]. If the error correction protocol aborts for at least one Bob then they abort the protocol. If it does not abort they obtain the raw keys* $\tilde{K}_A, \tilde{K}_{B_{(1\ldots N-1)}}$. *We call* O_A *the classical information that Alice has sent to the Bobs during the error correction protocol. Also the Bobs will send some error correction information but only for the bits produced during the testing rounds (*$T_i = 1$*), for the purpose of parameter estimation. We call Alice's guess on Bobs' strings* $G_{(1\ldots N-1)}$, *and we denote* $O_{(k)}$ *the error correction information sent by* Bob_k.

4. ***Parameter estimation:*** *For all the rounds* i *such that* $T_i = 1$, *Alice uses* A'_i *and her guess on* $B'_{(1\ldots N-1),i}$ *to set* $C_i = 1$ *if they have won the N-partite Parity-CHSH game in the round* i, *and she sets* $C_i = 0$ *if they have lost it. Finally she sets* $C_i = \perp$ *for the rounds* i *where* $T_i = 0$. *She aborts if* $\sum_i C_i < \delta \cdot \sum_i T_i$, *where* $\delta \in]3/4, 1/2 + 1/2\sqrt{2}[$.

5. ***Privacy amplification:*** *Alice and the Bobs apply a privacy amplification protocol (namely the universal hashing described in [26]) to create final keys* $K_A, K_{B_{(1\ldots N-1)}}$. *We call* S *the classical information that Alice sent to the Bobs during the privacy amplification protocol.*

Note that the above Protocol 4.2.3 is very similar to the DIQKD protocol given in [7], the difference being that since N parties are present here we use a shared N-partite GHZ state, instead of EPR pairs, and we have to add error corrections. Indeed we have an error correction protocol that permits all the parties to get the same raw key. But since we have N parties involved in the protocol, at least one of the parties needs to know all the other parties' outputs for the testing rounds (when $T_i = 1$) in order to estimate, in the parameter estimation phase, how many times do they succeed in the Parity-CHSH game. For simplicity of the analysis we choose, in Protocol 4.2.3, to communicate this information through error correction protocols.

In the ideal scenario (when there is no noise and no interference of Eve) the state $\rho_{A_1^n B_{(1\ldots N-1)}{}_1^n}$ produced corresponds to n copies of the N-partite GHZ state, distributed across the N parties, and Alice and the Bobs measure the following observables:

1. Alice's observable for $X_i = 0$ is σ_Z and for $X_i = 1$ it is σ_X.

2. Bob_1 uses observable σ_Z when $Y_{(1),i} = 2$, $\frac{\sigma_Z + \sigma_X}{\sqrt{2}}$ when $Y_{(1),i} = 0$, and $\frac{\sigma_Z - \sigma_X}{\sqrt{2}}$ when $Y_{(1),i} = 1$.

3. For the other Bobs, they have the observable σ_Z for $Y_{(k),i} = 0$, and for $Y_{(k),i} = 1$ they have observable σ_X.

In the next sections we are going to present the detailed proof of the following main result:

Theorem 4.2.4. *Let $\epsilon_{\text{EC}}, \epsilon'_{\text{EC}} \in]0,1[$ be the two error parameters of the error correction protocol as described in the Section 4.2.2, $\epsilon_{\text{PA}} \in]0,1[$ be the privacy amplification error probability, $\epsilon_{\text{EA}} \in]0,1[$ be a chosen security parameter for Protocol 4.2.3, and $\epsilon \in]0,1[$ be a smoothing parameter. Protocol 4.2.3 is $(\epsilon^s, \epsilon^c, l)$-secure according to Definition 2.4.6, with $\epsilon^s \leq \epsilon_{\text{PA}} + 2(N-1)\epsilon'_{\text{EC}} + 2\epsilon + \epsilon_{\text{EA}}$, $\epsilon^c \leq (N-1)(2\epsilon_{\text{EC}} + \epsilon'_{\text{EC}}) + \left(1 - \mu\left(1 - \exp\left[-2(p_{\text{exp}} - \delta)^2\right]\right)\right)^n$, and*

$$l = \max_{3/4 \leq \frac{p_{\text{opt}}}{\mu} \leq 1/2 + 1/2\sqrt{2}} \left((f(\hat{q}, p_{\text{opt}}) - \mu) \cdot n - \tilde{v}\sqrt{n}\right) + 3\log(1 - \sqrt{1 - (\epsilon/4)^2}) - 2\log(\epsilon_{\text{PA}}^{-1}) - \text{leak}_{\text{EC}}(O_A) - \sum_{k=1}^{N-1} \text{leak}_{\text{EC}}(O_{(k)}), \tag{4.15}$$

where $\tilde{v} = 2\left(\log(13) + (\hat{f}'(p_{\text{opt}}) + 1)\right)\sqrt{1 - 2\log(\epsilon \cdot \epsilon_{\text{EA}})} + 2\log(7)\sqrt{-\log(\epsilon_{\text{EA}}^2(1 - \sqrt{1 - (\epsilon/4)^2}))}$, $p_{\text{opt}} \in]\mu 3/4, \mu(1/2 + 1/2\sqrt{2})[$ is a parameter to be optimized: more precisely p_{opt} is the unique point were the tangent function $f(\cdot, p_{\text{opt}})$ to the function $\hat{f}(\cdot)$ (see Lemma 4.2.9) is such that $f(p_{\text{opt}}, p_{\text{opt}}) = \hat{f}(p_{\text{opt}})$ (by convexity of $\hat{f}$ we have $\forall x \in [0,1]$ $f(x, p_{\text{opt}}) \leq \hat{f}(x)$). Finally p_{exp} is the expected winning probability to win a single round of the Parity-CHSH game for a honest implementation, $\delta \in]3/4, 1/2 + 1/2\sqrt{2}[$ is the threshold defined in Protocol 4.2.3, and $\hat{q}$ is the vector $(\mu\delta, \mu - \mu\delta, 1 - \mu)^t$.

CORRECTNESS

The correctness of Protocol 4.2.3 comes from the first part of the error correction protocol used by the parties, where Alice sends information to the Bobs so that they generate the raw keys $\tilde{K}_A, \tilde{K}_{B_{(1\ldots N-1)}}$. We want here an error correction protocol that uses only communication from Alice to the Bobs and that minimizes the amount of communication needed. Therefore we are going to use an error correction protocol as the one described in [24, 25]. The idea of this error correction code is that Alice chooses a hash function and sends to the Bobs the chosen function and the hashed value of her bits. We denote this communication O_A. Then each Bob_k will individually use O_A and his own prior knowledge $B_{(k)}{}_1^n X_A{}_1^n Y_{(1\ldots N-1)}{}_1^n T_1^n$ to guess Alice's string. Each of the Bobs can fail to produce a guess, so if one of them fails the protocol aborts. In an honest implementation of the protocol, the probability that one particular Bob, say Bob_k ($k \in [N-1]$), aborts is upper bounded by ϵ_{EC}. Therefore the probability that at least one of them aborts in an honest implementation is at most $(N-1)\epsilon_{\text{EC}}$. If for $k \in [N-1]$ Bob_k does not abort we then have that $P(\tilde{K}_A \neq \tilde{K}_{B_{(k)}}) \leq \epsilon'_{\text{EC}}$. Therefore if none of the Bobs aborts we have that,

$$\begin{aligned} P\left(\tilde{K}_A = \tilde{K}_{B_{(1)}} = \ldots = \tilde{K}_{B_{(N-1)}}\right) &= 1 - P\left(\tilde{K}_A \neq \tilde{K}_{B_{(1)}} \text{ OR} \ldots \text{OR } \tilde{K}_A \neq \tilde{K}_{B_{(N-1)}}\right) \\ &\geq 1 - (N-1)\epsilon'_{\text{EC}} \geq 1 - \epsilon_{\text{corr}}, \end{aligned}$$

where we take $\epsilon_{\text{corr}} \geq (N-1)\epsilon'_{\text{EC}}$, which proves the following lemma:

Lemma 4.2.5. *The Protocol 4.2.3 is ϵ_{corr}-correct, for any $\epsilon_{\text{corr}} \geq (N-1)\epsilon'_{\text{EC}}$, where ϵ'_{EC} is such that if $\forall k \in [N-1]$ Bob_k does not abort the error correction protocol then $P(\tilde{K}_A \neq \tilde{K}_{B_{(k)}}) \leq \epsilon'_{\text{EC}}$.*

COMPLETENESS

We call an honest implementation of the protocol, an implementation where the measurement devices used act in the same way in all the rounds of the protocol, the state used for the n rounds is of the form $\rho^{\otimes n}_{AB_{(1\dots N-1)}}$ (the measurements and the state are then said to be identically and independently distributed (IID)), and such that for one single round, the probability of winning the N partite Parity-CHSH game is $p_{\text{exp}} \in \left]3/4, 1/2 + 1/2\sqrt{2}\right]$.

Lemma 4.2.6. *For any parameter $\delta \in \left]3/4, 1/2 + 1/2\sqrt{2}\right[$, Protocol 4.2.3 is ϵ^c-complete, for*

$$\epsilon^c \leq (N-1)(2\epsilon_{\text{EC}} + \epsilon'_{\text{EC}}) + \left(1 - \mu\left(1 - \exp\left[-2(p_{\text{exp}} - \delta)^2\right]\right)\right)^n, \tag{4.16}$$

where $p_{\text{exp}} > \delta$, δ is a threshold.

Proof. Protocol 4.2.3 can abort at two moments: it can abort during the error correction or during the parameter estimation. For the error correction step, the protocol aborts if one of the Bobs aborts while trying to guess Alice's string, or if Alice aborts while guessing Bobs' testing bits. We are assuming that the Bobs use the same error correction protocol in order to send information about their outputs in the test rounds so that Alice can make her guess. Therefore the overall probability of aborting during the error correction protocol is then bounded by $2(N-1)\epsilon_{\text{EC}}$ for an honest implementation. The probability of aborting during the parameter estimation part (conditioned on not aborting the error correction step) is given by:

$$\begin{aligned} P_{\text{PE}}(\text{abort}) = {} & P(G_{(1\dots N-1)} \text{ is correct}) P\Big(\sum_i C_i < \delta \cdot \sum_i T_i \Big| G_{(1\dots N-1)} \text{ is correct}\Big) \\ & + P(\exists k : G_{(k)} \text{is wrong}) P\Big(\sum_i C_i < \delta \cdot \sum_i T_i \Big| \exists k : G_{(k)} \text{is wrong}\Big) \end{aligned} \tag{4.17}$$

where $G_{(k)}$ is Alice's guess for Bob$_k$'s testing rounds bits. It is said to be correct when the string $G_{(k)} = B'_{(k),I}$ for $I := \{i \in [n] : T_i = 1\}$. By bounding $P(G_{(1\dots N-1)}$ is correct) by 1, $P(\exists k : G_{(k)}$is wrong) by $(N-1)\epsilon'_{\text{EC}}$, and $P\Big(\sum_i C_i < \delta \cdot \sum_i T_i \Big| \exists k : G_{(k)} \text{is wrong}\Big)$ by 1, we get

$$P_{\text{PE}}(\text{abort}) \leq \sum_{j=0}^{n} P\Big(\sum_i T_i = j\Big) \cdot P\Big(\sum_i C_i < \delta \cdot j \Big| \sum_i T_i = j \;\&\; \forall k \tilde{K}_A = \tilde{K}_{B_{(k)}}\Big) + (N-1)\epsilon'_{\text{EC}}. \tag{4.18}$$

Let us consider an honest implementation such that $p_{\text{exp}} > \delta$, we can then rewrite (4.18) as,

$$\begin{aligned} & P_{\text{PE}}(\text{abort}) \\ & \leq \sum_{j=0}^{n} P\Big(\sum_i T_i = j\Big) \cdot P\Big(\sum_i C_i < \big(p_{\text{exp}} - (p_{\text{exp}} - \delta)\big) \cdot j \Big| \sum_i T_i = j \;\&\; G_{(1\dots N-1)} \text{ is correct}\Big) \\ & \qquad + (N-1)\epsilon'_{\text{EC}}. \end{aligned} \tag{4.19}$$

Note that the expectation value $\mathbb{E}(C_i) = p_{\text{exp}}$ and because an honest implementation is IID we can use Hoeffding inequalities to bound $P\Big(\sum_i C_i < \big(p_{\text{exp}} - (p_{\text{exp}} - \delta)\big)\cdot j \Big| \sum_i T_i = j \;\&\; G_{(1\ldots N-1)} \text{ is correct}\Big) < \exp(-2(p_{\text{exp}} - \delta)^2 j)$. Moreover the the IID random variables T_i follow a Bernoulli distribution with $P(T_i = 1) = \mu$. Pluging all of this into eq. (4.19) gives us,

$$P_{\text{PE}}(\text{abort}) \leq \sum_{j=0}^{n} \binom{n}{j} (1-\mu)^{n-j}\mu^j \times \exp(-2(p_{\text{exp}} - \delta)^2 j) + (N-1)\epsilon'_{\text{EC}} \tag{4.20}$$

$$= \sum_{j=0}^{n} \binom{n}{j} (1-\mu)^{n-j}\big(\mu \times \exp(-2(p_{\text{exp}} - \delta)^2)\big)^j + (N-1)\epsilon'_{\text{EC}} \tag{4.21}$$

$$= \Big(1 - \mu\Big(1 - \exp\big[-2(p_{\text{exp}} - \delta)^2\big]\Big)\Big)^n + (N-1)\epsilon'_{\text{EC}}, \tag{4.22}$$

where the last equality comes from the binomial theorem. □

SOUNDNESS

In order to complete the security proof of Protocol 4.2.3, it remains to prove secrecy. Let $\hat{\Omega}'$ be the event that Protocol 4.2.3 does not abort and that the error correction step is successful. The Leftover Hash Lemma [17, Corollary 5.6.1] states that the secrecy of the final key, after a privacy amplification protocol using a family of two-universal hashing functions, depends on the amount of smooth min-entropy of the state before privacy amplification conditioned on the event $\hat{\Omega}'$.

Theorem 4.2.7 (Leftover Hash Lemma [17])**.** *Let $\mathscr{F}$ be a family of two-universal hashing functions from $\{0,1\}^n \to \{0,1\}^l$, such that $F(A_1^n) = K_A$ for $F \in \mathscr{F}$, then it holds that*

$$\left\| \rho_{K_A E|\hat{\Omega}'} - \frac{\mathbb{1}_A}{2^l} \otimes \rho_{E|\hat{\Omega}'} \right\|_{\text{tr}} \leq 2\epsilon + 2^{-\frac{1}{2}(H^{\epsilon}_{\min}(A_1^n|E)_{\rho_{|\hat{\Omega}'}} - l)}. \tag{4.23}$$

According to Theorem 4.2.7, in order to prove the secrecy of Protocol 4.2.3 we need to lower bound the smooth min-entropy $H^{\epsilon}_{\min}(A'^n_1|X_1^n Y_{(1\ldots N-1)}{}_1^n T_1^n OO_{(1\ldots N-1)}E)_{\rho_{|\hat{\Omega}'}}$. The proof goes in the following steps: In Lemma 4.2.10, we introduce an error correction map and bound the entropy $H^{\epsilon}_{\min}(A'^n_1|X_1^n Y_{(1\ldots N-1)}{}_1^n T_1^n E)$ for the state after the action of the error correction map, conditioned on the event that a particular violation is observed and the error correction protocol is successful. In Lemma 4.2.11, we relate the state generated by Protocol 4.2.3 conditioned on the event that the error correction protocols were successful to the state artificially introduced in Lemma 4.2.10, and we estimate $H^{\epsilon}_{\min}(A'^n_1|X_1^n Y_{(1\ldots N-1)}{}_1^n T_1^n OO_{(1\ldots N-1)}E)$, taking into account the information leaked during the error correction protocol. Finally, in Lemma 4.2.12, we combine the previous results proving the soundness of Protocol 4.2.3.

To bound the smooth min-entropy we will use the Entropy Accumulation Theorem (EAT).

Remark 4.2.8. *The reader who is not very familiar with this theorem may read the Entropy Accumulation Theorem section of Chapter 2 on page 30.*

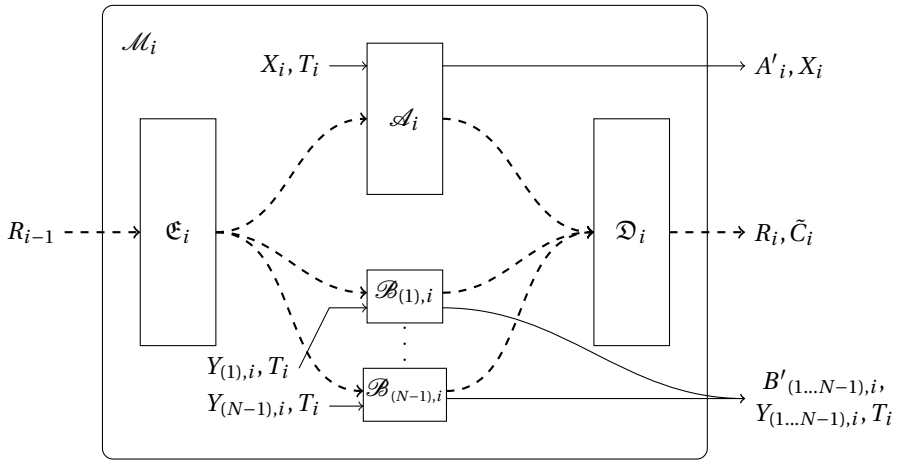


Figure 4.2: Description of the map $\mathscr{M}_i$. This map describes the round i of the first step of the Protocol 4.2.3. T_i is chosen at random such that $P(T_i = 1) = \mu$. $X_i \in \{0,1\}$ represents the "basis" in which Alice's device, represented by the CPTP map $\mathscr{A}_i$, measures its input to get the output $A'_i \in \{0,1\}$. $X_i = 0$ when $T_i = 0$ and $X_i \in_R \{0,1\}$ otherwise. $Y_{(k),i} \in \{0,1,2\}$ represents the "basis" in which Bob$_k$'s device, represented by the CPTP map $\mathscr{B}_{(k),i}$, measures its input to get the output $B'_{(k),i} \in \{0,1\}$. If $T_i = 0$ we have $Y_{(k),i} = 2$, else we have $Y_{(k),i} \in_R \{0,1\}$. If $T_i = 0$ then $\tilde{C}_i = \perp$, else $\tilde{C}_i = w_{\text{Parity-CHSH}}(A'_i, B'_{(1\ldots N-1),i}, X_i, Y_{(1\ldots N-1),i})$.

Indeed, before the error correction part, Protocol 4.2.3 can be described by a composition of EAT channels that we will call $\mathscr{M}_1, \ldots, \mathscr{M}_n$ (see Fig. 4.2).

In order to apply Entropy Accumulation Theorem (EAT) (see Theorem 2.3.13 of Chapter 2) we need to find a min-tradeoff function (see Definition 2.3.12 of Chapter 2) for the maps $\mathscr{M}_i$ defined by the Figure 4.2. *I.e.*, we need to find a function f such that

$$f(q) \leq \inf_{\sigma \in \Sigma_i(q)} H(A'_i \tilde{C}_i | X_i Y_{(1\ldots N-1),i} T_i R)_\sigma, \tag{4.24}$$

for

$$\Sigma_i(q) := \{\sigma_{\tilde{C}_i A'_i B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i R_i R} = (\mathscr{M}_i \otimes \mathbb{1}_R)(\sigma_{R_{i-1}R}) : \sigma_{R_{i-1}R} \in \mathscr{S}(\mathscr{H}_{R_{i-1}R}) \,\&\, \sigma_{\tilde{C}_i} = q\},$$

where $\Sigma_i(q)$ is the set of states that can be generated by the action of the channel $\mathscr{M}_i \otimes \mathbb{1}_R$ on an arbitrary state and such that the classical register $\tilde{C}_i$ has distribution q.

Lemma 4.2.9. *The real function defined as,*

$$\hat{f}(x) := \left(1 - \frac{\mu}{2}\right)\left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4x/\mu - 2)^2 - 1}\right)\right) \tag{4.25}$$

is a min-tradeoff function for the EAT channels $\mathscr{M}_i$ defined by the Figure 4.2. Here μ is the testing probability of the Protocol 4.2.3, and $h(x)$ is the binary entropy: $h(x) = -x\log(x) - (1-x)\log(1-x)$.
We define the affine function $f(\,\cdot\,, p_{\text{opt}})$ over the probability distribution $\mathbb{P}(\{1,0,\perp\})$ as, $\forall\ q = \big(q(1), q(0), q(\perp)\big)^t \in \mathbb{P}(\{1,0,\perp\})$,

$$f(q, p_{\text{opt}}) := \hat{f}'(p_{\text{opt}})q(1) + \hat{f}(p_{\text{opt}}) - \hat{f}'(p_{\text{opt}})p_{\text{opt}}, \tag{4.26}$$

where $p_{\text{opt}} \in]\mu 3/4, \mu(1/2+1/2\sqrt{2})[$.

In order to make the argument more rigorous and general, here $f(\cdot, p_{\text{opt}})$ is a function that takes as input the vector of frequencies $q = \big(q(1), q(0), q(\perp)\big)^t$.

Proof. Let us take a state $\sigma_{\tilde{C}_i A'_i B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i R_i R} \in \Sigma_i(q)$. Then we define the state

$$\sigma'_{\tilde{C}_i A''_i B''_{(1),i} B'_{(2\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i F_i R_i R} \tag{4.27}$$

to be the state we obtain from $\sigma_{\tilde{C}_i A'_i B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i R_i R}$ by replacing A'_i by $A''_i := A'_i \oplus F_i$ and $B'_{(1),i}$ by $B''_{(1),i} := B'_{(1),i} \oplus F_i$ where F_i is a bit that is chosen uniformly at random. None of the other registers are changed, in particular, note that we still have that $\sigma'_{\tilde{C}_i} = q$, where the value of $\tilde{C}_i$ can be determined by the registers A''_i, $B''_{(1),i}$, and $B'_{(2\ldots N-1),i}$. Moreover, since F_i is completely independent of the other variables and given the definition of A''_i, it is easy to check that,

$$H(A'_i \tilde{C}_i | X_i Y_{(1\ldots N-1),i} T_i R)_\sigma = H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R)_{\sigma'}. \tag{4.28}$$

This entropy can be lower bounded as follows:

$$H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R)_{\sigma'} \geq H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b})_{\sigma'}, \tag{4.29}$$

where $\bar{b}$ denotes the register containing the parity of $B'_{(2\ldots N-1),i}$. The right-hand side of the above inequality can be expended as,

$$\begin{aligned} H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b})_{\sigma'} = p_{\bar{b}=0} H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=0)_{\sigma'} \\ + p_{\bar{b}=1} H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=1)_{\sigma'} \end{aligned} \tag{4.30}$$

We will now detail the derivation of a lower bound for $H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=0)$. The lower bound on $H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=1)$ follows the exacte same steps.

Using the chain rule,

$$H(A''_i \tilde{C}_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=0)_{\sigma'} \geq H(A''_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=0)_{\sigma'}, \tag{4.31}$$

and since $P(X_i = 0) = 1 - \frac{\mu}{2}$,

$$H(A''_i | F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b}=0)_{\sigma'} \geq \left(1 - \frac{\mu}{2}\right) \cdot H(A''_i | F_i Y_{(1\ldots N-1),i} T_i R, X_i = 0, \bar{b}=0)_{\sigma'}. \tag{4.32}$$

Given that for $X_i = 0$ Alice's measurement is independent of $Y_{(1\ldots N-1),i}$ and T_i we have

$$H(A''_i | F_i Y_{(1\ldots N-1),i} T_i R, X_i = 0, \bar{b}=0)_{\sigma'} = H(A''_i | F_i R, X_i = 0, \bar{b}=0)_{\sigma'}. \tag{4.33}$$

Using the definition of the conditional Von Neumann entropy we can write:

$$H(A''_i | F_i R, X_i = 0, \bar{b}=0)_{\sigma'} = H(A''_i F_i R | X_i = 0, \bar{b}=0)_{\sigma'} - H(F_i R | X_i = 0, \bar{b}=0)_{\sigma'} \tag{4.34}$$

$$= H(A''_i | X_i = 0, \bar{b}=0)_{\sigma'} + \underbrace{H(F_i R | X_i = 0, \bar{b}=0)_{\sigma'} - H(F_i R | X_i = 0, \bar{b}=0)_{\sigma'}}_{= -\chi(A''_i : F_i R | X=0, \bar{b}=0)_{\sigma'}} \tag{4.35}$$

$$= 1 - \chi(A''_i : F_i R | X_i = 0, \bar{b}=0)_{\sigma'} \tag{4.36}$$

where $\chi(A_i'' : F_i R|X_i = 0, \bar{b} = 0)$ is the Holevo quantity, and the last equality comes from the definition of A_i'' being a uniform variable (for any value of X_i and $\bar{b}$).

In the following we will use p_w as a short for $P_w^{\text{Parity-CHSH}}$. From the definition of the Parity-CHSH inequality (see Def. 4.2.1), one can noticed that conditioned on $\bar{b} = 0$, the Parity-CHSH game reduces the the usual CHSH game, and conditioned on $\bar{b} = 1$ it reduces to a game that is equivalent to CHSH up to flipping input y. Therefore we can write $p_w = p_{\bar{b}=0} p_{w|\bar{b}=0} + p_{\bar{b}=1} p_{w|\bar{b}=1}$, where $p_{w|\bar{b}=0}$ can be viwed as the winning probability of a CHSH game, and $p_{w|\bar{b}=1}$ as the winning probability of the CHSH game with flipped input y. Moreover, for any state leading to a CHSH violation of $P_w^{\text{CHSH}} = p_{w|\bar{b}=0} \in [3/4, 1/2 + 1/2\sqrt{2}]$, Ref. [2, Section 2.3] gives a tight upper bound on $\chi(A_i : F_i R|X_i = 0, \bar{b} = 0)$:

$$\chi(A_i'' : RF_i|X_i = 0, \bar{b} = 0) \leq h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_{w|\bar{b}=0} - 2)^2 - 1}\right), \tag{4.37}$$

where $h(x) = -x\log(x) - (1-x)\log(1-x)$. This leads to,

$$H(A_i''\tilde{C}_i|F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b} = 0)_{\sigma'} \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_{w|\bar{b}=0} - 2)^2 - 1}\right). \tag{4.38}$$

Similarly we can bound,

$$H(A_i''\tilde{C}_i|F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b} = 1)_{\sigma'} \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_{w|\bar{b}=1} - 2)^2 - 1}\right). \tag{4.39}$$

Using these two above inequalities in eq. (4.30) we get,

$$\begin{aligned} H(A_i''\tilde{C}_i|F_i X_i Y_{(1\ldots N-1),i} T_i R, \bar{b})_{\sigma'} &= p_{\bar{b}=0}\left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_{w|\bar{b}=0} - 2)^2 - 1}\right)\right) && (4.40)\\ &\quad + p_{\bar{b}=1}\left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_{w|\bar{b}=1} - 2)^2 - 1}\right)\right) \\ &\geq \left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4(p_{\bar{b}=0}p_{w|\bar{b}=0} + p_{\bar{b}=1}p_{w|\bar{b}=1}) - 2)^2 - 1}\right)\right) && (4.41)\\ &= \left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{(4p_w - 2)^2 - 1}\right)\right), && (4.42) \end{aligned}$$

where the last inequality holds by convexity.

Note that p_w can be expressed in terms of the probability distribution $q = (q(1), q(0), q(\perp))^t$ (where ^{t} is the transpose) as $p_w = \frac{q(1)}{1-q(\perp)}$. And because in our case the definition of the maps $\mathcal{M}_i$ implies $1 - q(1) = \mu$ we have $p_w = \frac{q(1)}{\mu}$. Therefore the function

$$\bar{f}(q) = \hat{f}(q(1)) = \left(1 - \frac{\mu}{2}\right) \cdot \left(1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(4 \cdot q(1)/\mu - 2\right)^2 - 1}\right)\right), \tag{4.43}$$

is a min-tradeoff function, and $\hat{f}$ is a differentiable convex increasing function of one variable. To find an affine min-tradeoff function f we take a tangent to $\hat{f}$ for some value

$p_{\text{opt}}(n,\delta) \in \left]\mu\cdot 3/4, \mu\cdot(1/2+1/2\sqrt{2})\right[$ to be chosen, where μ and δ are defined in the Protocol 4.2.3, which gives us,

$$f(q, p_{\text{opt}}) := \hat{f}'(p_{\text{opt}})q(1) + \hat{f}(p_{\text{opt}}) - \hat{f}'(p_{\text{opt}})p_{\text{opt}}. \tag{4.44}$$

□

In the following Lemma we show that the state $\tilde{\rho}$ created by applying a sequence of n CPTP maps of the form described by Fig. 4.2 on some initial state, (when conditioned on the event of having (statistically) high enough Bell violation), possesses a linear amount of entropy.

Lemma 4.2.10. *Let $\mathcal{M}_{\text{EC}}$ be the CPTP map $A'^n_1 B'_{(1\ldots N-1)}{}^n_1 \mapsto A'^n_1 B'_{(1\ldots N-1)}{}^n_1 K_{B_{(1\ldots N-1)}} G_{(1\ldots N-1)}$ that models the error correction protocols, applied during Step 3 of Protocol 4.2.3, which produce the raw keys $K_{B_{(1\ldots N-1)}}$ and the guess $G_{(1\ldots N-1)}$. For $i \in [n]$ let $\mathcal{M}_i$ be the CPTP map from R_{i-1} to $A'_i B'_{(1\ldots N-1)i} \tilde{C}_i X_i Y_{(1\ldots N-1),i} T_i R_i$ defined in the Fig. 4.2. Let Ω be the event $\{\sum_j \tilde{C}_j \geq \delta\cdot\sum_j T_j$ for $\delta \in \left]3/4, 1/2+1/2\sqrt{2}\right[$ **and** all the error correction protocols were successful, meaning that $\forall k$, $A'^n_1 = K_{B_{(k)}}$ and Alice guess $G_{(1\ldots N-1)}$ is correct$\}$. We define the state,*

$$\tilde{\rho}_{A'^n_1 \tilde{C}^n_1 B'_{(1\ldots N-1)}{}^n_1 X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E} := (\text{tr}_{R_n}\circ\mathcal{M}_n\circ\ldots\circ\mathcal{M}_1\otimes\mathbb{1}_E)(\rho_{R_0E}), \tag{4.45}$$

where $R_0 = A^n_1 B_{(1\ldots N-1)}{}^n_1$, and ρ_{R_0E} is the state shared between Alice, the Bobs, and Eve (produced by Alice's source) across the n rounds of the Protocol 4.2.3 before they apply any measurement. Then we have for any $\epsilon \in]0,1[$,

$$H^{\epsilon}_{\min}\left(A'^n_1 | X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E\right)_{\mathcal{M}_{\text{EC}}(\tilde{\rho})_{|\Omega}} \geq \left(f(\hat{q}, p_{\text{opt}}) - \mu\right)\cdot n - \tilde{v}\sqrt{n} + 3\log(1-\sqrt{1-(\epsilon/4)^2}), \tag{4.46}$$

where $\tilde{v} = 2\left(\log(13)+(\hat{f}'(p_{\text{opt}})+1)\right)\sqrt{1-2\log(\epsilon\cdot p_\Omega)} + 2\log(7)\sqrt{-\log(p^2_\Omega(1-\sqrt{1-(\epsilon/4)^2}))}$, *and* $\hat{q} = \left(\delta\mu, \mu-\delta\mu, 1-\mu\right)^t \in \mathbb{P}(\{1,0,\perp\})$.

Proof. Note that $\tilde{\rho}_{|\Omega} := \text{tr}_{K_{B_{(1\ldots N-1)}} G_{(1\ldots N-1)}}\left(\mathcal{M}_{\text{EC}}(\tilde{\rho})_{|\Omega}\right)$, therefore $H^{\epsilon}_{\min}\left(A'^n_1 | X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E\right)_{\mathcal{M}_{\text{EC}}(\tilde{\rho})_{|\Omega}} = H^{\epsilon}_{\min}\left(A'^n_1 | X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E\right)_{\tilde{\rho}_{|\Omega}}$.

The maps $\mathcal{M}_1,\ldots,\mathcal{M}_n$ are EAT channels with the following Markov conditions,

$$\forall i \in [n],\ A'^{i-1}_1 \tilde{C}^{i-1}_1 \leftrightarrow X^{i-1}_1 Y_{(1\ldots N-1)}{}^{i-1}_1 T^{i-1}_1 E \leftrightarrow X^i_1 Y_{(1\ldots N-1)}{}^i_1 T^i_1. \tag{4.47}$$

Indeed for any round $i \in [n]$ the variables $X_i Y_{(1\ldots N-1),i} T_i$ are chosen independently of any other round $j \neq i$. We have proven that the function $f(\cdot, p_{\text{opt}})$ is a min-tradeoff function for the maps $\mathcal{M}_1,\ldots,\mathcal{M}_n$. We can therefore use the EAT to bound $H^{\epsilon}_{\min}\left(A'^n_1 \tilde{C}^n_1 | X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E\right)_{\tilde{\rho}_{|\Omega}}$:

$$H^{\epsilon}_{\min}\left(A'^n_1 \tilde{C}^n_1 | X^n_1 Y_{(1\ldots N-1)}{}^n_1 T^n_1 E\right)_{\tilde{\rho}_{|\Omega}} \geq n f(\hat{q}, p_{\text{opt}}) - c\sqrt{n}, \tag{4.48}$$

where $\hat{q} = (\mu\delta, \mu-\mu\delta, 1-\mu)$, $c = 2\left(\log(13) + \lceil \hat{f}'(p_{\text{opt}})\rceil\right)\sqrt{1-2\log(\epsilon\cdot p_\Omega)}$, and p_Ω is the probability of the event Ω. This is true because $f(q,, p_{\text{opt}})$ is an increasing function

of $q(1)$, so for any event that implies $\sum_j \tilde{C}_j \geq \delta \cdot \sum_j T_j$ we have that $f(\text{freq}(\tilde{C}_1^n), p_{\text{opt}}) \geq f(\hat{q}, p_{\text{opt}})$, in particular $\Omega \Rightarrow f(\text{freq}(\tilde{C}_1^n), p_{\text{opt}}) \geq f(\hat{q}, p_{\text{opt}})$. Note that because $\forall x \in \mathbb{R}$, $\lceil x \rceil \leq x+1$ we can upper bound $\lceil \hat{f}'(p_{\text{opt}}) \rceil$ by $\hat{f}'(p_{\text{opt}})+1$ and then take $c = 2\big(\log(13)+(\hat{f}'(p_{\text{opt}})+1)\big)\sqrt{1-2\log(\epsilon \cdot p_\Omega)}$.

Using [27, eq. (6.57)] we can relate $H_{\min}^{\epsilon}\big(A_1'^n \tilde{C}_1^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega}$ to $H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega}$:

$$\begin{aligned} H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega} & \\ \geq H_{\min}^{\frac{\epsilon}{4}}\big(A_1'^n \tilde{C}_1^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega} - H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega} & \quad (4.49) \\ + 3\log(1-\sqrt{1-(\epsilon/4)^2}). & \end{aligned}$$

We now need to upper bound $H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega}$. First we note that,

$$H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega} \leq H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | T_1^n E\big)_{\tilde{\rho}|\Omega}.$$

To upper bound $H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | T_1^n E\big)_{\tilde{\rho}|\Omega}$ we will use [20, Lemma 28]. Indeed $H_{\max}^{\frac{\epsilon}{4}}\big(\tilde{C}_1^n | T_1^n E\big)_{\tilde{\rho}|\Omega}$ can be bounded exactly in the same as in [20, Lemma 28], and leads to:

$$H_{\max}^{\epsilon/4}(\tilde{C}_1^n | T_1^n E)_{\tilde{\rho}|\Omega} \leq \mu n + n(\alpha-1)\log^2(7) + \frac{\alpha}{\alpha-1}\log\left(\frac{1}{p_\Omega}\right) - \frac{\log(1-\sqrt{1-(\epsilon/4)^2})}{\alpha-1} \quad (4.50)$$

$$\leq \mu n + n(\alpha-1)\log^2(7) - \frac{\log(p_\Omega^2(1-\sqrt{1-(\epsilon/4)^2}))}{\alpha-1}, \quad (4.51)$$

for $\alpha \in]1,2]$.

Taking $\alpha = 1 + \sqrt{\frac{-\log(p_\Omega^2(1-\sqrt{1-(\epsilon/4)^2}))}{n\log^2(7)}}$ gives us,

$$H_{\max}^{\epsilon/4}(\tilde{C}_1^n | T_1^n E)_{\tilde{\rho}|\Omega} \leq \mu n + 2\sqrt{n}\log(7)\sqrt{-\log(p_\Omega^2(1-\sqrt{1-(\epsilon/4)^2}))}. \quad (4.52)$$

Putting eq. (4.48),(4.49) and (4.52) together gives us,

$$H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega} \geq \big(f(\hat{q}, p_{\text{opt}}) - \mu\big) \cdot n - \tilde{v}\sqrt{n} + 3\log(1-\sqrt{1-(\epsilon/4)^2}), \quad (4.53)$$

where $\tilde{v} = 2\big(\log(13)+(\hat{f}'(p_{\text{opt}})+1)\big)\sqrt{1-2\log(\epsilon \cdot p_\Omega)} + 2\log(7)\sqrt{-\log(p_\Omega^2(1-\sqrt{1-(\epsilon/4)^2}))}$.

Since $H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\mathcal{M}_{\text{EC}}(\tilde{\rho})|\Omega} = H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\tilde{\rho}|\Omega}$, we have,

$$H_{\min}^{\epsilon}\big(A_1'^n | X_1^n Y_{(1\ldots N-1)} {}_1^n T_1^n E\big)_{\mathcal{M}_{\text{EC}}(\tilde{\rho})|\Omega} \geq \big(f(\hat{q}, p_{\text{opt}}) - \mu\big) \cdot n - \tilde{v}\sqrt{n} + 3\log(1-\sqrt{1-(\epsilon/4)^2}). \quad (4.54)$$

This bound holds for any $p_{\text{opt}} \in]\mu 3/4, \mu(1/2+1/2\sqrt{2})[$. □

In the following Lemma we link the result of the previous Lemma to the real state ρ generated by the protocol 4.2.3. Indeed, in the real state, the "Bell violation" is not estimated directly, but via the error corrections that might fail with some small probability. We show that the real state of the protocol, when conditioned on the event that *Protocol 4.2.3 does not abort* **and** *the error corrections were successful*, possesses a linear amount on entropy.

Lemma 4.2.11. *Let us call $\hat{\Omega}$ the event of not aborting the Protocol 4.2.3 and $\hat{\Omega}'$ the event $\hat{\Omega}$ **and** all the error correction protocols were successful, meaning that $\forall k \in [N-1]$, $K_{B_{(k)}} = A'^n_1$ and Alice's guess $G_{(1\dots N-1)}$ is correct. Then, for any $\epsilon_{\text{EA}}, \epsilon'_{\text{EC}}, \epsilon \in]0,1[$, Protocol 4.2.3 either aborts with a probability $1 - P(\hat{\Omega}) \geq 1 - \big(1 - 2(N-1)\epsilon'_{\text{EC}}\big)\epsilon_{\text{EA}}$ ($\Leftrightarrow P(\hat{\Omega}') \leq \epsilon_{\text{EA}}$) or*

$$
\begin{aligned}
H^{\epsilon}_{\min}\big(A'^n_1 | X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 O_A O_{(1\dots N-1)} E\big)_{\rho_{|\hat{\Omega}'}} \geq \\
\max_{3/4 \leq \frac{p_{\text{opt}}}{\mu} \leq 1/2 + 1/2\sqrt{2}} n \left(\big(f(\hat{q}, p_{\text{opt}}) - \mu\big) - \frac{2\big(\log(13) + (\hat{f}'(p_{\text{opt}}) + 1)\big)\sqrt{1 - 2\log(\epsilon \cdot \epsilon_{\text{EA}})}}{\sqrt{n}} \right) \\
- \sqrt{n}\left(2\log(7)\sqrt{-\log(\epsilon^2_{\text{EA}}(1 - \sqrt{1 - (\epsilon/4)^2}))}\right) + 3\log(1 - \sqrt{1 - (\epsilon/4)^2}) - \text{leak}_{\text{EC}}(O_A) \\
- \sum_{k=1}^{N-1} \text{leak}_{\text{EC}}(O_{(k)}),
\end{aligned}
\tag{4.55}
$$

where $\hat{q} = (\mu\delta, \mu - \mu\delta, 1 - \mu)^t$.

Proof. Using the chain rule [27, Lemma 6.8] we get:

$$
\begin{aligned}
H^{\epsilon}_{\min}\big(A'^n_1 | X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 O_A O_{(1\dots N-1)} E\big)_{\rho_{|\hat{\Omega}'}} \\
\geq H^{\epsilon}_{\min}\big(A'^n_1 | X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 E\big)_{\rho_{|\hat{\Omega}'}} - \text{leak}_{\text{EC}}(O_A) - \sum_{k=1}^{N-1} \text{leak}_{\text{EC}}(O_{(k)}),
\end{aligned}
\tag{4.56}
$$

where $\text{leak}_{\text{EC}}(O_A)$ is the leakage due to the error correction protocol (when the Bobs try to guess Alice's bits) and $\text{leak}_{\text{EC}}(O_{(k)})$ is the leakage due to error correction (when Alice tries to guess Bob$_k$'s test rounds bits). These leakages will be estimated in Section 4.3.

We now need to bound $H^{\epsilon}_{\min}\big(A'^n_1 | X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 E\big)_{\rho_{|\hat{\Omega}'}}$. Note that the reduced state on $A'^n_1 X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 E$ of the global state at the end of the Protocol 4.2.3 conditioned on the event $\hat{\Omega}'$ of not aborting and all the error correction protocol were successful, is equal to the state $\mathcal{M}_{\text{EC}}(\tilde{\rho}_{A'^n_1 X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 E})_{|\Omega}$, therefore using Lemma 4.2.10 we get:

$$
H^{\epsilon}_{\min}\big(A'^n_1 | X^n_1 Y_{(1\dots N-1)} {}^n_1 T^n_1 E\big)_{\rho_{|\hat{\Omega}'}} \geq \big(f(\hat{q}, p_{\text{opt}}) - \mu\big) \cdot n - \tilde{v}\sqrt{n} + 3\log(1 - \sqrt{1 - (\epsilon/4)^2}),
\tag{4.57}
$$

where $\tilde{v} = 2\big(\log(13) + (\hat{f}'(p_{\text{opt}}) + 1)\big)\sqrt{1 - 2\log(\epsilon \cdot p_{\hat{\Omega}'})} + 2\log(7)\sqrt{-\log(p^2_{\hat{\Omega}'}(1 - \sqrt{1 - (\epsilon/4)^2}))}$. □

The following Lemma concludes on the soundness of Protocol 4.2.3. To do so we need to relate the event $\hat{\Omega}$ that the protocol 4.2.3 does not abort, with the event $\hat{\Omega}'$ that protocol 4.2.3 does not abort **and** that the error corrections are successful.

Lemma 4.2.12. *For any implementation of the Protocol 4.2.3, either the protocol aborts with a probability greater than* $1-\epsilon_{\text{EA}}$ *or it is* $((N-1)\epsilon_{\text{EC}}+\epsilon_{\text{PA}}+\epsilon)$*-correct-and-secret while producing keys of length* l *defined in eq.* (4.15).

Proof. Let $\hat{\Omega}$ be the event of not aborting in the protocol 4.2.3, and $\hat{\Omega}'$ the event $\hat{\Omega}$ **and** all the error correction protocols were successful. According to Lemma 4.2.11 we are into one of the two following cases:

- The protocol aborts with a probability $1-P(\hat{\Omega}) \geq 1-\left(1-2(N-1)\epsilon'_{\text{EC}}\right)\epsilon_{\text{EA}}$. This is equivalent to $P(\hat{\Omega}') \leq \epsilon_{\text{EA}}$ and implies that $1-P(\hat{\Omega}) \geq 1-\epsilon_{\text{EA}}$.
- The aborting probability is $1-P(\hat{\Omega}) \leq 1-\epsilon_{\text{EA}}$ (which implies that $P(\hat{\Omega}') \geq \epsilon_{\text{EA}}$) and the smooth min-entropy of the final state conditioned on $\hat{\Omega}'$ is bounded as in eq. (4.57). Conditioned on $\hat{\Omega}$ there is two cases:
  - The error correction step failed. This happens with probability at most $2(N-1)\epsilon'_{\text{EC}}$.
  - The error correction were successful and then all the keys agree. We have then the event $\hat{\Omega}'$. Therefore according to Lemma 4.2.11 the entropy is high enough to produce keys of length l such that:

$$\left\| \rho_{K_A E|\hat{\Omega}} - \frac{\mathbb{1}_A}{2^l} \otimes \rho_{E|\hat{\Omega}} \right\|_{\text{tr}} \leq \epsilon_{\text{PA}} + 2\epsilon, \tag{4.58}$$

    where ϵ_{PA} is the privacy amplification error probability and ϵ is the smoothing parameter.

  By combining the two above cases we have that the Protocol 4.2.3 is $(\epsilon_{\text{PA}} + 2(N-1)\epsilon'_{\text{EC}} + 2\epsilon)$-correct-and-secret.

□

4.3. ASYMPTOTIC KEY RATE ANALYSIS

In this section we evaluate the asymptotic key rate of the DICKA Protocol 4.2.3 and compare it to the case where the parties perform $N-1$ DIQKD protocols in order to establish a common key. In implementations where the efficiency of generation of GHZ states is comparable to the efficiency of the generation of EPR pairs a common key using a DICKA protocol can be, in principle, stablished in a much smaller number of rounds, however one need to analyse how the QBER and the leakages in the error correction protocol affects the key generation.

To analyse the key rate we need to evaluate the length l of the final key produced by Protocol 4.2.3, Eq. (4.15), and compute the rate $r := \frac{l}{\#\text{rounds}}$. To achieve this, we need to estimate the leakage due to the error correction step. We use in our analysis an error correction protocol based on universal hashing [24, 25]. The size of the leakage is taken

to be the amount of correction information needed if the implementation were honest, for some abort probability of the error correction protocol of at most ϵ_{EC}, and such that the guess (when not aborting) is correct with probability at least $1-\epsilon'_{\text{EC}}$. For a given honest implementation, this leakage can be bounded as follows [25]:

$$\text{leak}(\text{O}_\text{A}) \leq \max_{k\in[N-1]} H_0^{\tilde{\epsilon}_{\text{EC}}}(A_1^n|B'_{(k)}{}_1^n X_1^n Y_{(1\ldots N-1)} T_1^n) + \log({\epsilon'_{\text{EC}}}^{-1}), \tag{4.59}$$

$$\text{leak}(\text{O}_{(\text{k})}) \leq H_0^{\tilde{\epsilon}_{\text{EC}}}(B'_{(k),I}|{A'}_1^n X_1^n Y_{(1\ldots N-1)} T_1^n) + \log({\epsilon'_{\text{EC}}}^{-1}), \tag{4.60}$$

for $\epsilon_{\text{EC}} = \tilde{\epsilon}_{\text{EC}} + \epsilon'_{\text{EC}}$, $I := \{i \in [n] : T_i = 1\}$ and where $H_0^{\tilde{\epsilon}_{\text{EC}}}$ is evaluated on the state produced by the honest implementation. If it turns out that the implementation is not the expected one then the protocol will just abort with a higher probability but the security is not affected.

We will consider here one particular honest implementation to evaluate the leakage. Then we will compare it to what we would get using $N-1$ device-independent quantum key distribution ($(N-1)\times$DIQKD) protocols to distribute the key to the N parties. For the key rate of the latter we will use the recent and most general analysis given in [7]. Of course the following calculations can be adapted to other implementations.

Lemma 4.3.1 (Asymptotic key rate)**.** *There exist an implementation of Protocol 4.2.3 in which the achieved asymptotic key rate is given by*

$$r_{N-\text{CKA},\infty} = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\left(\frac{\sqrt{1-2Q}^N}{2\sqrt{2}} + \frac{(1-2Q)\left(1-\sqrt{1-2Q}^{N-2}\right)}{8\sqrt{2}}\right)^2 - 1}\right) - h(Q), \tag{4.61}$$

where Q is the QBER between Alice and each of the Bobs.

Proof. In the following analysis we chose an IID honest implementation scenario where we assume that the channel between Alice and each of the Bobs is a depolarizing channel:

$$\mathscr{D}(\rho) = (1-p_{\text{dep}})\rho + p_{\text{dep}}\frac{\mathbb{1}}{2}, \tag{4.62}$$

for $p_{\text{dep}} \in]0,1[$. We will also apply this channel to model the noise on Alice's side. The state that is produced by Alice's source is supposed to be a N-GHZ state denoted $\text{GHZ}_N := |\text{GHZ}_N\rangle\langle\text{GHZ}_N|$, where $|\text{GHZ}_N\rangle := \frac{|0\rangle^{\otimes N}+|1\rangle^{\otimes N}}{\sqrt{2}}$. Therefore the state shared between Alice and the Bobs in one round is $\rho_{AB_{(1\ldots N-1)}} := \mathscr{D}^{\otimes N}(\text{GHZ}_N)$. The QBER between Alice and each of the Bobs can then be expressed as $Q = \frac{2p_{\text{dep}}-p_{\text{dep}}^2}{2}$ ($\Leftrightarrow p_{\text{dep}} = 1-\sqrt{1-2Q}$) and the expected winning probability of the Parity-CHSH game is given by:

$$p_{\text{exp}} = \left[\frac{1}{2} + \frac{(1-p_{\text{dep}})^N}{2\sqrt{2}} + \frac{(1-p_{\text{dep}})^2(1-(1-p_{\text{dep}})^{N-2})}{8\sqrt{2}}\right].$$

We can bound H_0 by $H_{\max}$ [28, Lemma 18] as,

$$H_0^{\tilde{\epsilon}_{\mathrm{EC}}}(A_1^n|{B'}_{(k)}{}_1^n X_1^n Y_{(1\ldots N-1)} T_1^n) \leq H_{\max}^{\tilde{\epsilon}_{\mathrm{EC}}/2}(A_1^n|{B'}_{(k)}{}_1^n X_1^n Y_{(1\ldots N-1)} T_1^n) + \log(8/\tilde{\epsilon}_{\mathrm{EC}}^2 + 2/(2-\tilde{\epsilon}_{\mathrm{EC}})). \tag{4.63}$$

Using the non-asymptotic version of the Asymptotic Equipartition Theorem (see Theorem 2.3.8 or [29, Theorem 9]) we get:

$$H_{\max}^{\tilde{\epsilon}_{\mathrm{EC}}/2}(A_1^n|{B'}_{(k)}{}_1^n X_1^n Y_{(1\ldots N-1)} T_1^n) \leq nH(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i) + \sqrt{n}\Delta(\tilde{\epsilon}_{\mathrm{EC}}), \tag{4.64}$$

where $\Delta(\tilde{\epsilon}_{\mathrm{EC}}) := 4\log\left(2\sqrt{2^{H_{\max}(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i)}} + 1\right) \cdot \sqrt{2\log(8/\tilde{\epsilon}_{\mathrm{EC}}^2)}$. We can now upper bound the entropy for honest implementation of Protocol 4.2.3 as,

$$\begin{aligned} H(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i) &= (1-\mu)\cdot H(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i}, T_i = 0) \\ &\quad + \mu \cdot \underbrace{H(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i}, T_i = 1)}_{\leq 1} \end{aligned} \tag{4.65}$$

$$\leq (1-\mu)\cdot h(Q) + \mu, \tag{4.66}$$

and $H_{\max}(A_i'|B'_{(1\ldots N-1),i} X_i Y_{(1\ldots N-1),i} T_i) \leq 1$. This gives us an upper bound on $\mathrm{leak}(O_A)$:

$$\begin{aligned} &\mathrm{leak}(O_A) \\ &\leq n\cdot\left((1-\mu)\cdot h(Q) + \mu\right) + \sqrt{n}\cdot 4\log\left(2\sqrt{2}+1\right)\cdot\sqrt{2\log(8/\tilde{\epsilon}_{\mathrm{EC}}^2)} + \log(8/\tilde{\epsilon}_{\mathrm{EC}}^2 + 2/(2-\tilde{\epsilon}_{\mathrm{EC}})). \end{aligned} \tag{4.67}$$

Using the same reasoning, we get:

$$\mathrm{leak}(O_{(k)}) \leq n\cdot\mu + \sqrt{n}\cdot 4\log\left(2\sqrt{2}+1\right)\cdot\sqrt{2\log(8/\tilde{\epsilon}_{\mathrm{EC}}^2)} + \log(8/\tilde{\epsilon}_{\mathrm{EC}}^2 + 2/(2-\tilde{\epsilon}_{\mathrm{EC}})). \tag{4.68}$$

Putting this into equation (4.15) we get,

$$\begin{aligned} l = &\left(f(\hat{q}, p_{\mathrm{opt}}) - (1-\mu)h(Q) - (N+1)\mu\right)\cdot n - \hat{v}\sqrt{n} + 3\log(1-\sqrt{1-(\epsilon/4)^2}) - \log(\epsilon_{\mathrm{PA}}^{-1}) \\ &- N\cdot\log(8/\tilde{\epsilon}_{\mathrm{EC}}^2 + 2/(2-\tilde{\epsilon}_{\mathrm{EC}})), \end{aligned} \tag{4.69}$$

where $\hat{v} = \tilde{v} + N\cdot 4\log\left(2\sqrt{2}+1\right)\cdot\sqrt{2\log(8/\tilde{\epsilon}_{\mathrm{EC}}^2)}$, and $\tilde{v}$ is defined in Theorem 4.2.4.

Note that in the asymptotic regime $n\to\infty$ we can take the threshold δ to be $\delta = p_{\mathrm{exp}}$, and the optimal p_{opt} will be $p_{\mathrm{opt}} = \mu\delta = \mu p_{\mathrm{exp}}$. Also for the asymptotic analysis we chose $\mu = n^{-1/10}$. Therefore the asymptotic rate $r_\infty := \lim_{n\to\infty}\frac{l}{\#\mathrm{rounds}}$ becomes,

$$\begin{aligned} r_{N-\mathrm{CKA},\infty} &= \hat{f}(\mu p_{\mathrm{exp}}) - h(Q) \\ &= 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\left(\frac{\sqrt{1-2Q}^N}{2\sqrt{2}} + \frac{(1-2Q)\left(1-\sqrt{1-2Q}^{N-2}\right)}{8\sqrt{2}}\right)^2 - 1}\right) - h(Q). \end{aligned} \tag{4.70}$$

□

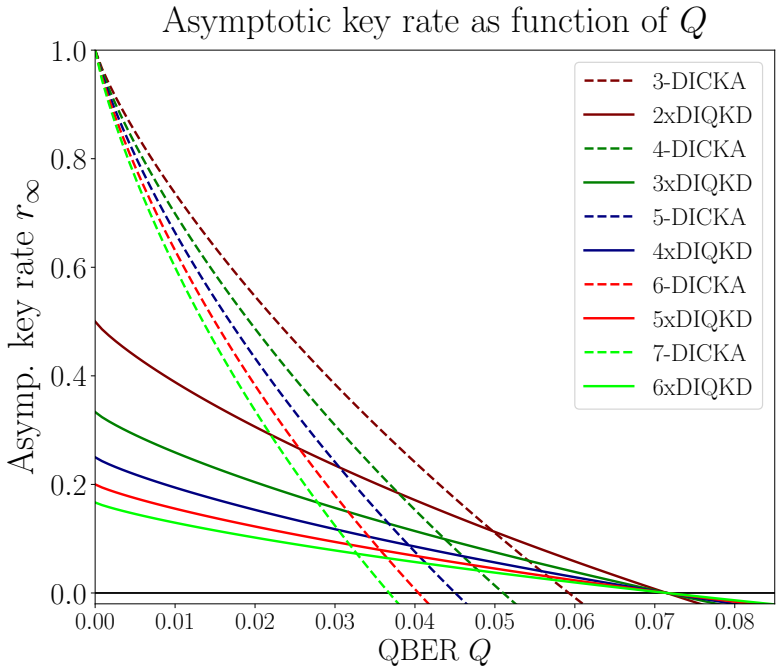


Figure 4.3: Asymptotic key rate for N-device-independent CKA (DICKA, dashed lines), and for the distribution of a secret key between N parties through $N-1$ device-independent quantum key distribution ($(N-1)\times$DIQKD) protocols (solid lines), when each qubit experiences independent bit errors measured at a bit error rate (QBER) Q. From top to bottom, the lines correspond to $N = \{3,4,5,6,7\}$. We observe that for low noise it is advantageous to use our device-independent N-CKA protocol instead of using $N-1$ DIQKD protocols [7]. In general, the comparison between the two methods depends on the cost and noisiness of producing GHZ states over pairwise EPR pairs.

We then compare it to the asymptotic rate we would get if in order to distribute a key to N parties, Alice were to use a DIQKD protocol for each of the Bobs. To get the asymptotic rate for the $(N-1)$ DIQKD protocols, we use the analysis given in [7]. In their DIQKD protocol they consider an honest implementation where the state is a depolarized EPR pair $(1-v)\Phi_{AB} + v\frac{\mathbb{1}}{2}$. If we say that, for each Bob, Alice sends the state via the same depolarizing channel she uses in the previous analysis (and that she has the same noise on her qubits), we can link the parameter v with the depolarizing parameter p_{dep} of the channel and to the QBER Q: $v = 2p - p^2 = 2Q$. Therefore we get:

$$r_{(N-1)\times\text{QKD},\infty} = \frac{1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{2\cdot(1-2Q)^2 - 1}\right) - h(Q)}{N-1}. \tag{4.71}$$

Note that the factor $1/(N-1)$ comes from the fact that the total number of rounds while running $N-1$ DIQKD protocols is $(N-1)n$, where n is the number of rounds for one DIQKD protocol.

The comparison of the key rates of DICKA, Eq. (4.70), and $(N-1)\times$DIQKD, Eq. (4.71), for different values of N, are plotted in Fig. 4.3. The results show that for low noise it is advantageous to use the DICKA protocol. In this comparison we assume that the cost of generation of a GHZ state is the same as the cost to generate one EPR pair. However, in implementations where the GHZ state is created out of EPR pairs that will not be the case. Therefore the cost of creation of these states must be taken into account in the analysis of the particular implementations. Note, also, that in this Section we have modelled the implementation for depolarising channels, however the security analysis is general and can be adapted for any particular implementation.

4.4. CONCLUSION

We presented the first security proof for a fully device-independent implementation of conference key agreement. We have shown that, in principle, security can be achieved for any violation of the Parity-CHSH inequality that detects genuine multipartite entanglement. It remains an open point whether the protocol can be extended in such a way that for violations of the Parity-CHSH inequality that do not certify genuine N-partite entanglement we can still guarantee security.

We have compared the asymptotic key rates achieved with the DICKA protocol versus $N-1$ implementations of DIQKD, modelling the quantum channel connecting the parties as depolarising channels. For implementations where the cost of local generation of GHZ states and EPR pairs is comparable, we show that it is advantageous to use DICKA for low noise regimes. A careful analysis that takes into account the costs of generation of the states is still needed for particular implementations.

We remark that proving advantage for a small number of parties already leads to better protocols for networks. Indeed, instead of using DIQKD as building block for a N-DICKA protocol (for large N), one can use k-DICKA protocols, upon availability of k-GHZ states for $k = 3, 4$ or 5.

Finally, we also remark that our DICKA protocol can be adapted for other multipartite Bell inequalities. However, in general, finding good lower bounds on Eve's information about Alice's output as a function of the Bell violation is a difficult task.

REFERENCES

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks,* Phys. Rev. Lett. **98**, 230501 (2007).

[2] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-independent quantum key distribution secure against collective attacks,* New Journal of Physics **11**, 045021 (2009).

[3] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices,* Nature Communications **2**, 238 (2011), arXiv:1009.1567 [quant-ph] .

[4] C. A. Miller and Y. Shi, *Robust Protocols for Securely Expanding Randomness and*

Distributing Keys Using Untrusted Quantum Devices, Journal of the ACM (JACM) **63** (2016).

[5] C. A. Miller and Y. Shi, *Universal security for randomness expansion from the spot-checking protocol,* SIAM Journal on Computing **46**, 1304 (2017).

[6] U. Vazirani and T. Vidick, *Fully device-independent quantum key distribution,* Phys. Rev. Lett. **113**, 140501 (2014).

[7] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation,* Nature Communications **9**, 459 (2018).

[8] J. Ribeiro, L. Phuc Thinh, J. Kaniewski, J. Helsen, and S. Wehner, *Device-independence for two-party cryptography and position verification,* arXiv:1606.08750 (2016), arXiv:1606.08750 [quant-ph] .

[9] J. Kaniewski and S. Wehner, *Device-independent two-party cryptography secure against sequential attacks,* New Journal of Physics **18**, 055004 (2016).

[10] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, *Fully distrustful quantum bit commitment and coin flipping,* Phys. Rev. Lett. **106**, 220501 (2011).

[11] A. Kent, *Quantum tagging for tags containing secret classical data,* Phys. Rev. A **84**, 022335 (2011).

[12] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, *A monogamy-of-entanglement game with applications to device-independent quantum cryptography,* New Journal of Physics **15**, 103002 (2013).

[13] M. Burmester and Y. Desmedt, Advances in Cryptology — EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings, edited by A. De Santis (Springer Berlin Heidelberg, Berlin, Heidelberg, 1995) pp. 275–286.

[14] K. Chen and H.-K. Lo, Proceedings. International Symposium on Information Theory, 2005. ISIT 2005. (2005) pp. 1607–1611.

[15] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruss, *Multi-partite entanglement can speed up quantum key distribution in networks,* New Journal of Physics (2017).

[16] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Phys. Rev. Lett. **23**, 880 (1969).

[17] R. Renner, Security of Quantum Key Distribution, Ph.D. thesis, PhD Thesis, 2005 (2005).

[18] C. Portmann and R. Renner, *Cryptographic security of quantum key distribution,* arXiv:1409.3525 (2014), arXiv:1409.3525 [quant-ph] .

[19] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation,* arXiv:1607.01796 (2016), arXiv:1607.01796 [quant-ph] .

[20] J. Ribeiro, G. Murta, and S. Wehner, *Fully general device-independence for two-party cryptography and position verification,* arXiv:1609.08487 (2016), arXiv:1609.08487 [quant-ph] .

[21] M. Coudron and H. Yuen, *Infinite Randomness Expansion and Amplification with a Constant Number of Devices,* arXiv:1310.6755 (2013), arXiv:1310.6755 [quant-ph] .

[22] J. Ribeiro, L. P. Thinh, J. m. k. Kaniewski, J. Helsen, and S. Wehner, *Device independence for two-party cryptography and position verification with memoryless devices,* Phys. Rev. A **97**, 062307 (2018).

[23] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography,* Phys. Rev. Lett. **110**, 010503 (2013).

[24] G. Brassard and L. Salvail, Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 410–423.

[25] R. Renner and S. Wolf, Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 199–216.

[26] R. Renner and R. König, Second Theory of Cryptography Conference, TCC 2005. Volume 3378 of Lecture (2005).

[27] M. Tomamichel, Quantum Information Processing with Finite Resources - Mathematical Foundations, SpringerBriefs in Mathematical Physics, Vol. 5 (Springer International Publishing, 2016).

[28] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information,* IEEE Transactions on Information Theory **57**, 5524 (2011).

[29] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition property,* IEEE Transactions on Information Theory **55**, 5840 (2009).

5

TOWARDS A REALIZATION OF DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

Glaúcia MURTA, Suzanne B. VAN DAM, Jérémy RIBEIRO, Ronald HANSON, and Stephanie WEHNER

In the implementation of device-independent quantum key distribution we are interested in maximizing the key rate, i.e. the number of key bits that can be obtained per signal, for a fixed security parameter. In the finite size regime, we furthermore also care about the minimum number of signals required before key can be obtained at all. Here, we perform a fully finite size analysis of device independent protocols using the CHSH inequality both for collective and coherent attacks. For coherent attacks, we sharpen the results recently derived in Arnon-Friedman et al., Nat. Commun. 9, 459 (2018) [1], to reduce the minimum number of signals before key can be obtained. In the regime of collective attacks, where the devices are restricted to have no memory, we employ two different techniques that exploit this restriction to further reduce the number of signals. We then discuss experimental platforms in which DIQKD may be implemented. We analyse Bell violations and expected QBER achieved in previous Bell tests with distant setups and situate these parameters in the security analysis. Moreover, focusing on one of the experimental platforms, namely nitrogen-vacancy based systems, we describe experimental improvements that can lead to a device-independent quantum key distribution implementation in the near future.

Parts of this chapter have been published in Quantum Science and Technology, 4:035011, 2019

5.1. INTRODUCTION

5.1.1. QUANTUM KEY DISTRIBUTION

Quantum key distribution (QKD) [2, 3] is a remarkable example of the advantages that quantum systems bring to accomplishing classical tasks. All the classical crypto-systems used for key exchange are based on computational assumptions and, therefore, are susceptible to retroactive attacks. Indeed, if an adversary keeps track of the public information exchanged during the communication of an encrypted message and, in a later future, a more efficient algorithm or faster machines become available, then the messages exchanged in the past can be decrypted. The novelties brought by quantum systems allow two parties to establish a common key that is information-theoretically secure and, therefore, can be used to achieve perfect secure communication with a one-time pad encryption.

Quantum key distribution schemes explore intrinsic properties of quantum systems, such as no-cloning [4, 5] and monogamy of entanglement [6], in order to achieve security even against an all powerful adversary who has unlimited computational power. The well known quantum key distribution scheme BB84 [2] can tolerate a reasonable amount of noise and decent rates[1] can be achieved with current technology, see for example the analyses of [9–11]. BB84-based QKD has been successfully implemented over long distances, see for example [12, 13], and even satellite-based secure quantum communication was established [14].

A successful implementation of the BB84 protocol is, however, highly dependent on a good characterisation of the underlying quantum system and the measurement devices. For example, the protocol can easily be broken if the devices are performing measurements in four dimensional systems instead of qubits, see discussions in [15, 16]. Furthermore, hacking of existent implementations that exploit experimental imperfections were presented (see e.g. [17–20]).

A good characterization of the experimental setup is a strong assumption. What is more, when quantum technologies become commercially available, we might often buy devices from a provider which is not entirely trustworthy. Fortunately, quantum properties allow us to overcome this problem: By exploring the strong correlations that arise in quantum systems, one can prove security of quantum key distribution even in the very adversarial scenario where Alice and Bob do not have complete knowledge of the internal working of their measurement devices or the underlying quantum system that they are measuring [1, 16, 21–34]. This is the device-independent (DI) model.

5.1.2. THE DEVICE-INDEPENDENT SCENARIO

In this section we remind the reader with the assumptions we make in the device-indepdent scenario and extensively comment its implications and possible issues one might have in practice.

Assumptions 5.1.1 (Device-independent model)**.** *In the device-independent model we assume:*

[1] Due to finite size effects a minimal number of rounds is required in order to guarantee security. For the BB84 protocol this minimal number of rounds required is $\sim 10^4$. Moreover, a quantum bit error rate (QBER) of up to 20% can be tolerated [7, 8] for large enough number of rounds.

1. *Isolated labs: no information is leaked from or enters Alice's and Bob's labs, apart from the state distribution before the measurements and the public classical information dictated by the protocol.*

2. *Isolated source: the preparation of states is independent of the measurements.*

3. *Trusted classical post-processing: all the public classical communication is performed using an authenticated channel and the local classical computations are trusted.*

4. *Trusted Random Number Generators: Alice and Bob possess independent and trusted random number generators.*

A bit of thought can make one conclude that completely removing any of these assumptions leads to a strategy where the key is leaked to the adversary. However, we remark that partial relaxation of these assumptions can still be considered. In Ref. [35], QKD is proved to achieve everlasting security by relaxing Assumption 5.1.1*(3)* to a computationally secure authenticated channel, but assuming the eavesdropper to be computationally bounded during the execution of the protocol. In many device independent protocols, instead of Assumption 5.1.1*(2)*, it is assumed that all the n systems are prepared before the measurement phase starts, so that no information other than the classical public communication is exchanged during the protocol. However, this would require quantum memory from Alice and Bob in order to store the quantum states along the protocol. In an implementation where the quantum states are generated round by round, and therefore in which no long term quantum memory is required, Assumption 5.1.1*(2)* is necessary to avoid that the state prepared by the source leaks the raw bits generated by Alice's device in the previous round. Indeed, if the source is arbitrarily correlated with the measurement devices the state prepared can contain an additional degree of freedom that encodes the string of bits generated in the previous rounds (this strategy is detailed in [36, Appendix C]). We remark that, in experimental platforms, the preparation of states and the measurements are either performed within the same systems or optically connected ones, and therefore one needs to assume that the process of generating a quantum state is not correlated with the previously performed measurements. This assumption is, however, often well justified based on a description of the setup. Ref. [37] addresses the problem of hidden memory in the devices. The authors show that a malicious eavesdropper can program the measurement devices in such a way that information about a previously generated key may be leaked through the public communication of a subsequent run of the key generation protocol, if the devices are re-used. Ref. [38] proposes an alternative to overcome memory attacks and covert channels in general, as well as the need to assume that all the classical post-processing is trusted. By introducing protocols based on secure multi-party computation distributed among more devices, ref. [38] relaxes the black-box model to reliability of only one of the quantum devices. Moreover, the classical post-processing can tolerate up to a third of malicious classical devices.

Another assumption that is often used in security proofs is that the rounds of the experiment are *independent and identically distributed* (IID). This, in particular, implies

that the measurement devices are memoryless and the state shared by Alice and Bob is the same for every round on the protocol. The IID assumption can be justified, for example, in experimental setups where Alice and Bob control to some extent the source and measurement devices, but do not have a full characterization of their working.

Assumptions 5.1.2 (IID assumption)**.** *An IID implementation assumes:*

- *IID devices: the devices behave independently and in the same way in every round of the protocol.*
- *IID states: The state distributed is the same for every round of the protocol. In summary, the state of the n rounds can be written as* $\rho_{A_1^n B_1^n E} = \rho_{ABE}^{\otimes n}$.

The eavesdropper attacks in QKD are classified in three types: Individual attacks, where the eavesdropper has no memory and therefore is restricted to attack individually each round of the protocol; Collective attacks: where in every round the systems of Alice and Bob, as well as the measurement devices, are prepared identically but the eavesdropper is allowed to make arbitrary global operations on her quantum side information; and Coherent attacks: additionally to the global operations the eavesdropper can perform in her quantum side information, the states shared by Alice and Bob in each round can be arbitrarily correlated, as well as the measurement devices in the DI scenario can have memory and operate according to the results of previous rounds, *i.e.*, do not satisfy the IID assumption. The IID assumption, stated in Assumptions 5.1.2, corresponds to the scenario where the eavesdropper is restricted to collective attacks. In what follows we focus on two types of adversarial attacks: collective attacks and coherent attacks.

5.1.3. DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION PROTOCOLS

The first ideas of device-independent QKD arose in the E91 protocol [3], which uses a test of the CHSH inequality [39] in order to certify that Alice and Bob share a maximally entangled state. This idea of self-testing quantum devices was further explored in [15]. Indeed, device-independent quantum key distribution relies on the violation of a Bell inequality in order to certify the security of the generated key. The simplest DIQKD protocol uses the CHSH inequality for the security test:

$$S = \mathbb{E}(A_0B_0) + \mathbb{E}(A_0B_1) + \mathbb{E}(A_1B_0) - \mathbb{E}(A_1B_1) \leq 2, \tag{5.1}$$

where $\mathbb{E}(A_xB_y) = p(a = b|xy) - p(a \neq b|xy)$ represents the correlation of the outputs a, b of Alice and Bob when they perform the measurement labeled by x, y respectively. The CHSH inequality can be phrased as a game [40] in which Alice and Bob receive x and y, respectively, as inputs and the winning condition is that their outputs satisfy $a + b = x \cdot y$, with the operations $+, \cdot$ taken modulo 2. The winning probability $\omega := P_w^{\text{CHSH}}$ of the CHSH game relates to the violation S by

$$\omega = \frac{4 + S}{8}. \tag{5.2}$$

For DIQKD based on the CHSH inequality, we consider protocols where Alice possesses a device with two possible inputs $X \in \{0, 1\}$ and Bob has a device with three possible inputs $Y \in \{0, 1, 2\}$. The inputs $X \in \{0, 1\}$ and $Y \in \{0, 1\}$ are used to test for the CHSH

inequality, and the inputs $X = 0$ and $Y = 2$ are used for the other rounds, often called key generation rounds, where maximal correlation of the outputs is expected. The parameters of interest are the Bell violation S, or winning probability ω, achieved in the test rounds and the quantum bit error rate (QBER) Q of the key generation rounds. We consider that an implementation of the protocol is expected to have n rounds and a portion γn of these rounds is used for testing of the CHSH condition.

A DIQKD protocol can be divided in three phases:

- An initial phase where Alice and Bob use their respective devices to measure the quantum systems and, according to the obtained outputs, generate the n-bit strings A_1^n and B_1^n.

- A second phase where Alice and Bob publicly exchange classical information in order to perform error correction, to correct their respective strings generating the raw keys; and parameter estimation, to estimate the parameters of interest (Bell violation, S, and QBER, Q). At the end of this phase Alice and Bob are supposed to share equal n-bit strings and have an estimate of how much knowledge an eavesdropper might have about their raw key.

- In the final phase, Alice and Bob perform privacy amplification, where the not fully secure n-bit strings are mapped into smaller strings K_A and K_B, which represents the final keys of Alice and Bob respectively.

The specific protocols we consider for our analyses are detailed in Section 5.2, (see Protocol 5.2.1 and Protocol 5.2.3).

In order to define security of a DIQKD protocol, we follow Refs. [1, 41] and adopt the security definition that is universally composable for standard QKD protocols [42]. Universal composability is the statement that a protocol remains secure even if it is used arbitrarily in composition with other protocols. It is important to remark that, for the device-independent case, attacks proposed in Ref. [37] show that composability is not achieved if the same devices are re-used for generation of a subsequent key. Indeed, in [37], the authors have shown that a malicious eavesdropper can program the measurement devices in such a way that information about a previously generated key may be leaked through the public communication of a subsequent run of the key generation protocol, if the devices are re-used. It is still an open problem what is the minimum set of assumptions that can lead to universal composability of DIQKD (e.g. the attacks of Ref. [37] can be avoided if we assume that Alice and Bob have sufficient control over the existing internal memory of their devices, so that they can re-set it after an execution of the protocol).

Let K_A and K_B denote the final key held by Alice and Bob, respectively, after they perform a DIQKD protocol. A DIQKD protocol is secure if it is correct and secret (see Definition 2.4.6). Correctness is the statement that Alice and Bob share the same key at the end of the protocol, *i.e.*, $K_A = K_B$. Secrecy is the statement that the eavesdropper is totally ignorant about the final key.

Definition 5.1.3 (Correctness)**.** *A DIQKD protocol is ϵ_{corr}-correct if the probability that*

the final key of Alice, K_A, differs from the final key of Bob, K_B, is smaller than ϵ_{corr}, i.e.

$$P(K_A \neq K_B) \leq \epsilon_{corr}. \tag{5.3}$$

Definition 5.1.4 (Secrecy)**.** *Let Ω denote the event of not aborting in a DIQKD protocol and $p(\Omega)$ be the probability of the event Ω. The protocol is ϵ_{sec}-secret if, for every initial state ρ_{ABE} it holds that*

$$p(\Omega) \cdot \frac{1}{2} \| \rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_E \|_1 \leq \epsilon_{sec}, \tag{5.4}$$

where $\tau_{K_A} = \frac{1}{|K_A|} \sum_k |k\rangle\langle k|_A$ is the maximally mixed state in the space of strings K_A, and $\| \cdot \|_1$ is the trace norm.

If a protocol is ϵ_{corr}-correct and ϵ_{sec}-secret, then it is ϵ^s_{DIQKD}-correct-and-secret for any $\epsilon^s_{DIQKD} \geq \epsilon_{corr} + \epsilon_{sec}$. See Definition 2.4.6 for a more detailed definition of security of a DIQKD protocol.

Given an DIQKD protocol that has n rounds and generates a final correct-and-secret key of l bits, then the secret key rate is defined as

$$r = \frac{l}{n}. \tag{5.5}$$

Our goal is to derive the secret key rate as a function of the parameters of interest, S and Q, that Alice and Bob can estimate during the execution of the protocol.

5.1.4. SECURITY PROOF OF DIQKD

Even though the BB84 quantum key distribution scheme dates back to 1984 [2], the formal security proof in the asymptotic regime only came out more than a decade later, see e.g. [43–46]. Security in the composable paradigm in the finite regime against general coherent attacks was only formalized in 2005 [47–49]. Moreover, a finite key analysis without the IID assumption over the state preparation and with parameters compatible with current technology only came in 2012 [9, 10].

In the device-independent scenario, security against a quantum eavesdropper[2] restricted to collective attacks was first proved in [16, 27]. A proof against general attacks assuming memoryless devices was presented in [28, 29]. The problem of extending the security proofs to coherent attacks in the device-independent scenario remained open for a long time. One of the main difficulties is that de Finetti techniques [48, 51], used to extend security proofs against collective attacks to general coherent attacks in standard QKD, are not applicable in the DI scenario. A series of recent works [31–34] culminated in the Entropy Accumulation Theorem (EAT) [1] (see [41, 52] for extended versions). The EAT allows one to extend the analysis against collective attacks to the fully device-independent scenario, resulting in asymptotically tight security proofs and high rates in the finite size regime.

[2] A discussion on earlier security proofs that do not restrict the eavesdropper to the quantum formalism can be found in [50].

5.1.5. EXPERIMENTAL DIQKD

Protocols for DIQKD rely on a Bell test between two distant parties [16]. In order to certify security, this Bell test should be free of loopholes that could be exploited by an adversary. While closing the detection loophole is crucial for a DIQKD implementation, the spacelike separation required for loophole-free Bell tests can be relaxed. In a DIQKD experiment, no-communication between the devices does not have to be guaranteed by spacelike separation, since the assumption of isolated labs, Assumption 5.1.1*(1)*, is already needed to ensure that the generated key is not leaked to the eavesdropper at any point in time. We are thus interested in considering Bell violations between distant - albeit not necessarily spacelike separated - setups in which the detection-loophole is closed [53–60]. The recent performance of fully loophole-free Bell tests [53–56] mark technological progress towards Bell tests without detection loophole over increasingly distant setups, as needed for practically useful DIQKD.

Despite the experimental progress, a device-independent quantum key distribution protocol has not yet been performed. The reason for this is that a Bell violation alone is not enough to guarantee security in a DIQKD protocol. One also needs to account for the amount of information leaked during the error correction, when Alice and Bob correct their string of bits in order to achieve a perfectly correlated raw key. The amount of information required for error correction is determined by the QBER. With a finite QBER, as in practical systems, a large Bell violation is needed to achieve a positive key rate. Moreover, a high minimal number of rounds is required for security due to finite-size effects. The large number of necessary rounds requires a significantly high entangling rate. Altogether, DIQKD demands a low QBER, high Bell violation and high entangling rates. Even though some systems satisfy parts of these requirements, e.g. a high Bell violation [53, 56, 59, 60] or high entangling rate [54, 55, 57, 58], so far there are no systems that combine all requirements. In section 5.2.3 we describe the potential platforms for an experimental implementation of DIQKD in detail.

5.2. RESULTS

We now present our results. In Section 5.2.1, we establish the key rates for DIQKD protocols based on the CHSH inequality, both for coherent and collective attacks in the finite size regime. As a benchmark, in Section 5.2.2, we compare the key rates that can be achieved in the finite regime for the two adversarial scenarios (collective and coherent attacks) using an implementation with depolarizing noise. In Section 5.2.3, we discuss the state of the art of experimental implementations. We estimate the parameters of interest for previously performed Bell experiments and situate them in the security proofs. Additionally, focusing on Nitrogen-vacancy based systems we indicate experimental improvements that can lead to an implementation of DIQKD in the near future. Throughout this manuscript we use Log_{10} to denote logarithm to base 10 and log to denote logarithm to base 2.

5.2.1. KEY RATES

In the following, we derive the key rates in the finite size regime for DIQKD protocols where the CHSH inequality is used for certifying security. For coherent attacks we sharpen

the results recently derived in [1]. For collective attacks we perform the analysis by employing two techniques: the finite version of the asymptotic equipartition property [61] and the additivity of the 2-Rényi entropy.

KEY RATES FOR COHERENT ATTACKS.
In order to analyze the key rates against general coherent attacks we use the recently developed Entropy Accumulation Theorem (EAT) [1, 41, 52] and consider the following protocol.

Protocol 5.2.1 (DIQKD Protocol for coherent attacks [41])**.**

for *For every block* $j \in [m]$

Set $i = 0$ *and* $C_j = \perp$.

while $i \leq s_{max}$

Set $i = i + 1$.

Alice and Bob choose a random bit $T_i \in \{0,1\}$ *such that* $P(T_i = 1) = \gamma$.

If $T_i = 0$ *Alice and Bob choose inputs* $(X_i, Y_i) = (0,2)$.

else *they choose* $X_i, Y_i \in \{0,1\}$ *(the observables for the CHSH test).*

end if

Alice and Bob use their devices with the respective inputs and record their outputs, A_i *and* B_i *respectively.*

If $T_i = 1$ *they set* $i = s_{max} + 1$.

end while

end for

Error Correction: *Alice and Bob apply the error correction protocol EC, communicating script* O_{EC} *in the process. If EC aborts they abort the protocol, else they obtain raw keys* $\tilde{A}_1^n$ *and* $\tilde{B}_1^n$.

Parameter estimation: *Using* B_1^n *and* $\tilde{B}_1^n$*, Bob sets*

$$C_i = \begin{cases} 1, & \text{if } T_i = 1 \text{ and } A_i \oplus B_i = X_i \cdot Y_i \\ 0, & \text{if } T_i = 1 \text{ and } A_i \oplus B_i \neq X_i \cdot Y_i \\ \perp, & \text{if } T_i = 0 \end{cases} \tag{5.6}$$

He aborts if

$$\sum_j C_j < m \times \left(\omega_{exp} - \delta_{est}\right)\left(1 - (1-\gamma)^{s_{\max}}\right),$$

i.e., if they do not achieve the expected violation.

Privacy Amplification: *Alice and Bob apply the privacy amplification protocol PA and obtain the final keys* K_A *and* K_B *of length* l.

In Protocol 5.2.1, the total number of rounds is not fixed in advance, however for a number of blocks m large enough the number of rounds will correspond, with high probability, to the expected value n. This is a technicality introduced in Ref. [1, 41] in order to obtain better rates in the finite regime. A more detailed explanation can be found in [41, Appendix B]. Improvements on the second order term of the Entropy Accumulation Theorem, that do not rely on the introduction of blocks, were recently obtained in [62]. Following the techniques of [1, 41], we derive Theorem 5.2.2.

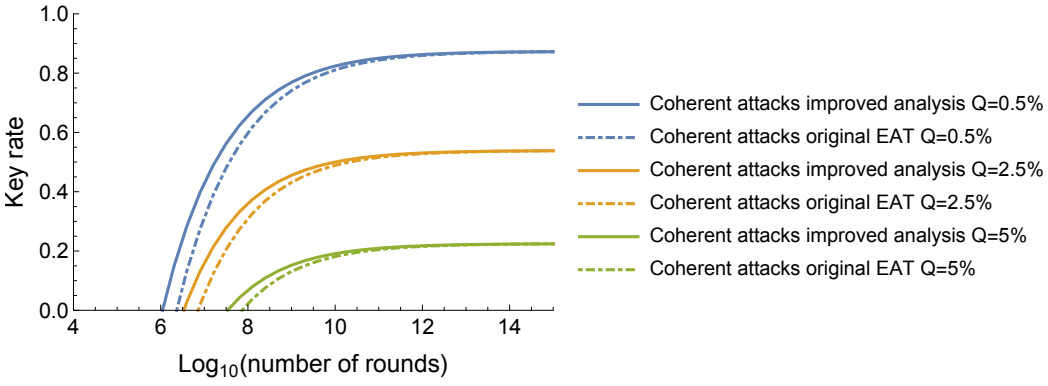
Theorem 5.2.2 (Key rates for coherent attacks)**.** *Either Protocol 5.2.1 aborts with probability higher than* $1-(\epsilon_{EA}+\epsilon_{EC})$*, or it generates a* $(2\epsilon_{EC}+\epsilon_{PA}+\epsilon_s)$*-correct-and-secret key of length*

$$l \geq \frac{n}{\bar{s}}\eta_{opt} - \frac{n}{\bar{s}}h(\omega_{exp}-\delta_{est}) - \sqrt{\frac{n}{\bar{s}}}\nu_1 - leak_{EC} \tag{5.7}$$
$$-3\log\left(1-\sqrt{1-\left(\frac{\epsilon_s}{4(\epsilon_{EA}+\epsilon_{EC})}\right)^2}\right)+2\log\left(\frac{1}{2\epsilon_{PA}}\right),$$

where $leak_{EC}$ *is the leakage due to error correction step and the functions* $\bar{s}$*,* η_{opt}*,* ν_1 *and* ν_2 *are specified in Table 5.1.*

Theorem 5.2.2 sharpens the original analysis [1, 41] and has slightly improved key rates in the finite regime. This results in a reduction of the minimum number of rounds (signals) required for positive rates by about a factor of two, as illustrated in Figure 5.1. A detailed derivation of Theorem 5.2.2 can be found in 5.5.2.

Figure 5.1: Key rate r vs logarithm of the number of rounds n. Comparison of the improvements in the key rate, for an implementation where the maximally entangled state is subjected to depolarizing noise and therefore $S = 2\sqrt{2}(1-2Q)$, for QBER $Q = \{0.5\%, 2.5\%, 5\%\}$. The dashed curves correspond to the key rates derived in the original analysis [1, 41], the solid lines represent the key rates derived in Theorem 5.2.2. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.



$s_{\max} = \left\lceil \frac{1}{\gamma} \right\rceil$
$\bar{s} = \frac{1-(1-\gamma)^{\left\lceil \frac{1}{\gamma} \right\rceil}}{\gamma}$
$\eta_{opt} = \max_{\frac{3}{4} < \frac{p_t(1)}{1-(1-\gamma)^{s_{max}}} < \frac{2+\sqrt{2}}{4}} \left[F_{\min}(\vec{p}, \vec{p}_t) - \frac{1}{\sqrt{m}} \nu_2 \right]$
$F_{\min}(\vec{p}, \vec{p}_t) = \frac{d}{dp(1)} g(\vec{p}) \Big\vert_{\vec{p}_t} \cdot p(1) + \left(g(\vec{p}_t) - \frac{d}{dp(1)} g(\vec{p}) \Big\vert_{\vec{p}_t} \cdot p_t(1) \right)$
$g(\vec{p}) = s \left[1 - h\left(\frac{1}{2} + \frac{1}{2} \sqrt{16 \frac{p(1)}{1-(1-\gamma)^{s_{max}}} \left(\frac{p(1)}{1-(1-\gamma)^{s_{max}}} - 1 \right) + 3} \right) \right]$
$\nu_2 = 2 \left(\log(1 + 2 \cdot 2^{s_{\max}} 3) + \left\lceil \frac{d}{dp(1)} g(\vec{p}) \Big\vert_{\vec{p}_t} \right\rceil \right) \sqrt{1 - 2 \log \epsilon_s}$
$\nu_1 = 2 \left(\log 7 + \left\lceil \frac{\lvert h'(\omega_{exp} + \delta_{est}) \rvert}{1-(1-\gamma)^{s_{\max}}} \right\rceil \right) \sqrt{1 - 2 \log \epsilon_s}$

Table 5.1: Explicit form of the terms that appear in Theorem 5.2.2. For a detailed derivation see 5.5.2.

KEY RATES FOR COLLECTIVE ATTACKS

For collective attacks, we derive the finite key rates by employing two techniques: the finite version of the asymptotic equipartition property and the additivity property of the conditional α-Rényi entropies. To deal with collective attacks we can use a simplified version of Protocol 5.2.1, where the number of rounds is fixed.

Protocol 5.2.3 (DIQKD protocol for collective attacks)**.**

for $i = 1$ *to* n

Alice and Bob choose a random bit $T_i \in \{0,1\}$ *such that* $P(T_i = 1) = \gamma$.

if $T_i = 0$ *Alice and Bob choose inputs* $(X_i, Y_i) = (0,2)$.

else *they choose* $X_i, Y_i \in \{0,1\}$ *(the observables for the CHSH test).*

end if

Alice and Bob use their devices with the respective inputs and record the outputs, A_i *and* B_i *respectively.*

end for

Error correction: *Alice and Bob apply the error correction protocol EC, communicating* O_{EC} *in the process. If EC aborts they abort the protocol, else they obtain raw keys* $\tilde{A}_1^n$ *and* $\tilde{B}_1^n$.

Parameter estimation: *Using* B_1^n *and* $\tilde{B}_1^n$*, Bob sets for the first test rounds*

$$C_i = \begin{cases} 1, & \text{if } A_i \oplus B_i = X_i \cdot Y_i \\ 0, & \text{if } A_i \oplus B_i \neq X_i \cdot Y_i \end{cases} \tag{5.8}$$

For the remaining rounds he sets $C_i = \perp$.

He aborts if

$$\sum_j C_j < \gamma n \times \left(\omega_{exp} - \delta_{est}\right),$$

i.e., if they do not achieve the expected violation.

Privacy Amplification: *Alice and Bob apply the privacy amplification protocol PA and obtain the final keys K_A and K_B of length l.*

In the following theorem we state the length of a secure key that can be derived using the asymptotic equipartition property, which is formally stated in Theorem 5.4.6.

Theorem 5.2.4. *Either Protocol 5.2.3 aborts with probability higher than $1-(\epsilon_{con}+\epsilon_{EC})$, or it generates a $(2\epsilon_{EC}+\epsilon_s+\epsilon_{PA})$-correct-and-secret key of length:*

$$\begin{aligned} l \geq n\Big[1 - h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})((\omega_{exp}-\delta_{est}-\delta_{con})-1)+3}\right) \\ -(1-\gamma)h(Q)-\gamma h(\omega_{exp})\Big] \\ -\sqrt{n}\left(4\log\left(2\sqrt{2}+1\right)\left(\sqrt{\log\frac{2}{\epsilon_s^2}}+\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right)\right) \\ -\log\left(\frac{8}{\epsilon'^2_{EC}}+\frac{2}{2-\epsilon'_{EC}}\right)-\log\left(\frac{1}{\epsilon_{EC}}\right)-2\log\left(\frac{1}{2\epsilon_{PA}}\right) \end{aligned} \tag{5.9}$$

A detailed derivation of Theorem 5.2.4 can be found in 5.5.2.

Using a different technique, namely bounding the key rate by the conditional collision entropy, we derive the following result.

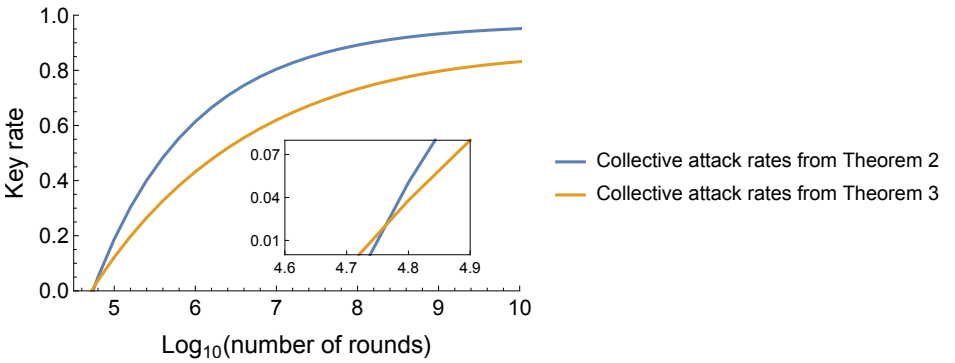
Theorem 5.2.5. *Either Protocol 5.2.3 aborts with probability higher than $1-(\epsilon_{con}+\epsilon_{EC})$, or it generates a $(2\epsilon_{EC}+\epsilon_{PA})$-correct-and-secret key of length:*

$$\begin{aligned} l \geq n\Big[-\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})(1-(\omega_{exp}-\delta_{est}-\delta_{con}))-2}\right) \\ -(1-\gamma)h(Q)-\gamma h(\omega_{exp})\Big] \\ -\sqrt{n}\left(4\log\left(2\sqrt{2}+1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right) \\ -\log\left(\frac{8}{\epsilon'^2_{EC}}+\frac{2}{2-\epsilon'_{EC}}\right) \\ -\log\left(\frac{1}{\epsilon_{EC}}\right)-2\log\left(\frac{1}{2\epsilon_{PA}}\right)-2\log\left(\frac{1}{\epsilon_{con}+\epsilon_{EC}}\right). \end{aligned} \tag{5.10}$$

An important step in the proof of Theorem 5.2.5 is to derive a lower bound on the collision entropy as a function of the CHSH violation S. A tight lower bound is proved in Theorem 5.4.10. The detailed proof of Theorem 5.2.5 is presented in 5.5.2.

The rates presented in Theorem 5.2.4 are asymptotically tight, while Theorem 5.2.5 achieves strictly smaller asymptotic rates. However, one can note that in Theorem 5.2.5 the term proportional to $\sqrt{n}$ has a smaller pre-factor. This can potentially lead to an advantage for the minimum number of rounds required for security. For Protocol 5.2.3, an advantage can only be observed for very low noise regime, as illustrated in Figure 5.2. We remark, however, that for protocols based on other Bell inequalities the techniques used for deriving Theorem 5.2.5 can present significant advantage for the collective attack analysis. This is further discussed in Section 5.4.3.

Figure 5.2: Key rates vs logarithm of the number of rounds n for Protocol 5.2.3 (collective attacks). The blue curve represent the key rate using Theorem 5.2.4 and the yellow curve shows the key rate using Theorem 5.2.5. It is considered an implementation with depolarizing noise and QBER $Q = 0.01\%$. The inset graph shows a zoom in the region of low number of rounds. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.



The following table lists the parameters of the DIQKD protocols in consideration.

n	expected number of rounds
l	final key length
γ	fraction of test rounds
Q	quantum bit error rate
S	CHSH violation
ω_{exp}	expected winning probability on the CHSH game in an honest implementation
δ_{est}	width of the statistical interval for the Bell test
δ_{con}	confidence interval for the Bell test in Protocol 5.2.3
ϵ_s	smoothing parameter
$\epsilon_{EC}, \epsilon'_{EC}$	error probabilities of the error correction protocol
ϵ_{EA}	error probability of Bell violation estimation in Protocol 5.2.1
ϵ_{con}	error probability of Bell violation estimation in Protocol 5.2.3
ϵ_{PA}	error probability of the privacy amplification protocol
leak_{EC}	leakage in the error correction protocol

Table 5.2: Parameters of the considered DIQKD protocols, Protocol 5.2.1 and Protocol 5.2.3.

5.2.2. COMPARISON OF KEY RATES FOR DEPOLARIZING NOISE MODEL

We now compare the key rates achieved in the finite regime under the assumption of collective attacks (IID scenario) and against general coherent attacks (fully DI scenario). As a benchmark, we focus on an honest implementation where the maximally entangled state is prepared and subjected to depolarizing noise[3]:

$$\rho = (1-\nu)|\Phi^+\rangle\langle\Phi^+| + \nu\frac{I}{4}. \tag{5.11}$$

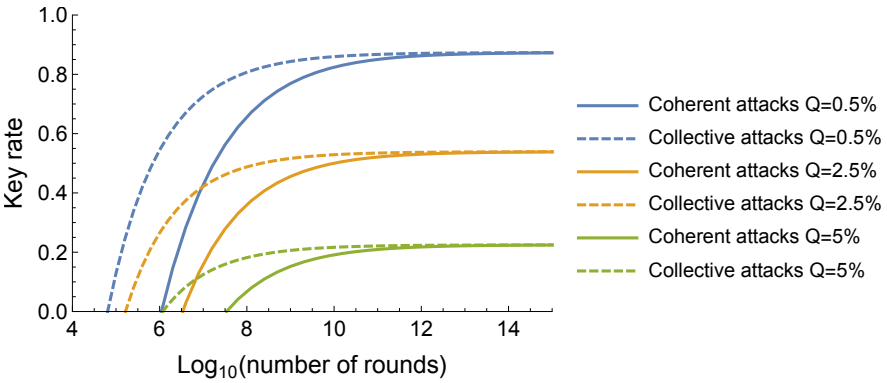
In this case, the parameters of interest – the value of the CHSH inequality S and the QBER Q – relate to the noise parameter ν by

$$Q = \frac{\nu}{2} \text{ and } S = 2\sqrt{2}(1-\nu) \rightarrow S = 2\sqrt{2}(1-2Q). \tag{5.12}$$

In Figure 5.3 we compare the key rates achievable under the IID assumption, given by Theorem 5.2.2, and in the fully DI scenario, Theorem 5.2.4, for an honest implementation with depolarizing noise.

[3]This noise model can also be seen as the case where each individual qubit suffers a depolarization with parameter ν', where $\nu = 2\nu' - \nu'^2$.

Figure 5.3: Key rates vs logarithm of the number of rounds for collective attacks (dashed lines) and coherent attacks (solid lines). The different curves represent different values of QBER $Q = (0.5\%, 2.5\%.5\%)$ considering an implementation where the maximally entangled state is subjected to depolarizing noise (see relation (5.12)). The security parameters are taken as $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.



5

Figure 5.3 shows that the key rates approach the same asymptotic values, however the minimum number of rounds required to guarantee security is significantly higher for general coherent attacks. Indeed, by adding the assumption that the eavesdropper is restricted to collective attacks, the minimum number of signals required to have a positive key rate drops by about two orders of magnitude. However, even for collective attacks, this minimum number of required rounds is considerably large given the current entanglement generation rates. This is one of the big challenges to be overcome for a DIQKD implementation. In the next Section we are going to discuss the state of the art of experiments, and situate the current achievable parameters (Bell violation, QBER and entanglement generation rate) in the security proofs.

5.2.3. THE STATE-OF-THE-ART EXPERIMENTAL DIQKD

In the following, we discuss experimental platforms in which DIQKD may be implemented. We analyse Bell violations and expected QBER achieved in previous Bell tests with distant setups and situate these parameters in the context of the key rates derived in Theorems 5.2.2 and 5.2.4. A summary of the findings is presented in Table 5.4 and Figures 5.5 and 5.6.

In experimental setups, distant entanglement is typically generated using photons to establish the connection. We distinguish two approaches based on the role of the photonic qubits: *(i) All-photonic schemes:* Approaches in which the entangled state is encoded in the photonic state directly. In this case, measurements of the photonic states on two remote setups enable to infer their entanglement. *(ii) Heralded schemes:* In this case, the entangled state is typically created in a long-lived system and the photons are used as a means of establishing the entanglement between two distant systems.

In this section we provide a discussion of the parameters in each of these schemes and the related challenges towards an implementation of DIQKD. We provide a more detailed discussion of one of the systems, namely nitrogen-vacancy (NV) centres in diamonds, and describe improvements in experimental parameters that can lead to a DIQKD

implementation in the near future.

DIQKD WITH ALL-PHOTONIC ENTANGLEMENT.
Since in all-photonic schemes the entangled state is directly encoded on the photonic state, photon losses limit the entangled state detection efficiency. Closing the detection loophole in a Bell test thus requires very efficient entangled-photon sources and photon detectors. Recent technological advances enabled all-photonic Bell tests that close the detection-loophole [57, 58], later combined with spacelike separation in loophole-free Bell tests [54, 55].

In photonic systems the detection efficiency also impacts the entangled state fidelity. We thus may expect that Bell violations are low in photonic systems. To avoid having to deal with undetected events, photonic Bell tests typically employ the CH-Eberhard inequality [63, 64]. The CHSH and CH-Eberhard inequalities are equivalent[4], such that we can estimate the CHSH violation achieved in photonic experiments. Table 5.4 presents the corresponding value for the CHSH inequality achieved in the experiments of Refs. [54, 55, 57, 58]. One can note that the violations achieved are indeed low, ranging from 2.00004 to 2.02. Combined with a finite QBER ($> 2\%$), this poses a significant challenge for the implementation of a DIQKD protocol in photonic systems.

However, if these systems would enter the regime of positive key rates, the entanglement generation rate can be very high ($\sim 10^5$ Hz), such that they could easily reach the asymptotic key rate values.

In order to overcome photon losses, several proposals for implementing heralding schemes in all-photonic systems were presented. In this case, the entangled state is created between photons and, also, this entanglement is heralded by the interference of other photons. In particular, in Ref. [65] the authors propose a scheme based on a qubit amplifier that combines single photon sources and linear optics. This proposal was further explored in Ref. [66]. Schemes based on entanglement swapping by quantum relay were also considered [67–69]. Ref. [67] makes a comparison of the performance of the two types of schemes. Analyses in Refs. [65, 67–69] make assumptions on the possible attacks performed by the eavesdropper. New protocols based on single photon sources were recently proposed in Ref. [70]. The proposed schemes uses a combination of spontaneous parametric down conversion sources and single-photon sources in order to achieve a setup where a heralding process could overcome transmission photon losses. The security analysis presented in Ref. [70] does not restrict the eavesdropper attacks. These setups are a promising proposal to bring the parameters of all-photonic systems to the region of positive asymptotic key rates (see Figure 5.5 and 5.6). However single-photon sources still lack the required performance for an implementation of these schemes.

DIQKD WITH HERALDED ENTANGLEMENT.
Due to the nature of heralded entangling schemes, photon losses do not influence the entangled state detection efficiency or fidelity. Heralded schemes have been used to entangle distant atomic ensembles [71, 72], trapped ions [73], atoms [74], NV centres

[4] One can see that by replacing non-detected events by the deterministic classical strategy “output 1" in a test of the CHSH inequality.

[75], quantum dots [76], and mechanical oscillators [77]. So far, entangled state fidelities sufficiently high to violate Bell's inequalities have only been reached with trapped ions [59, 60], atoms [56, 74], and with NV centres [53, 78]. The Bell violations observed in Refs. [53, 56, 59, 60, 78] are in the range $S = 2.22$ to $S = 2.41$, with a lower bound on the QBER, estimated from detection efficiencies alone, around 0.04 (see Table 5.4 for a full overview). Apart from the results reported in [60], these parameters are not in the region of positive key rate (see Figures 5.5 and 5.6). However, all of them are in the proximity of this region, such that setup improvements may enable to reach it.

The challenge for these implementations is however their low entangling rate, induced by photon losses. Current rates range from $(\text{minutes})^{-1}$ [56, 59, 60, 74] to $(\text{hours})^{-1}$ [53, 78]. A significant speed-up in the entanglement generation rate is thus needed in order to achieve the minimum number of rounds required for DIQKD. Higher entangling rates in heralded schemes were recently achieved with trapped ions [79] and NV centres [80, 81], although with lower state fidelities, and no Bell violations are reported. Even though in Ref. [81] the state fidelity is just high enough to be able to violate Bell inequalities, the expected Bell violation would be low. Enhancement in entangling rates, e.g. with optical cavities to improve light-matter coupling efficiency [82] is therefore crucial to achieving an implementation of DIQKD with heralded schemes.

5

NITROGEN-VACANCY CENTRE-BASED NETWORKS.
In this section, we focus on heralded entanglement generation between nitrogen-vacancy centres in diamond for DIQKD. Nitrogen-vacancy (NV) centres are defect centres in the diamond lattice. They contain an electronic spin with good coherence properties and spin-selective optical transitions that can be used for intialization, readout and entanglement generation [75, 83]. Next to the electronic spin, nearby weakly coupled nuclear spins can serve as long-lived memories [84, 85]. These properties make the NV centre a promising quantum network node.

Entanglement between distant NV centres can be generated using an heralded scheme. Typically, local entanglement is first generated between the NV electronic spin and a photon mode. And subsequently, entanglement between distant NV centres is achieved through entanglement swapping by interfering the two photon modes from distant setups [86]. As discussed above for heralded protocols, photon attenuation does not influence the fidelity of the generated entangled state or the detection efficiency. The detection of the spin states has near-unit efficiency [87].

DIQKD PARAMETERS.
In a loophole-free Bell test with NV centres [53, 78], a CHSH violation $S = 2.38 \pm 0.14$ was observed between systems separated by 1.3 kilometers. Taking into account the entangled state fidelity and detection efficiency, we estimate that the corresponding QBER would be $Q = 0.06 \pm 0.03$. The Bell violation achieved in [53, 78] is considerably high, especially if compared to loophole-free Bell test experiments in photonic systems [54, 55]. However, these parameters are not good enough to generate a secure key. Indeed, using Theorems 5.2.2 and 5.2.4, one concludes that it is not possible to achieve positive key rate with these parameters (see Figures 5.5 and 5.6).

In the following, we suggest two near-term experimental improvements to enhance these parameters.

Firstly, the frequency stability of the laser used to excite NV centres during the entanglement protocols can be increased using an external cavity. The instability of the laser can influence the indistinguishability of photons emitted by the distant NV centres. The indistinguishability is crucial for photon interference, which can be quantified by the visibility of the two-photon quantum interference (TPQI). We expect that compared to previous implementation [53], the improved laser frequency stability can lead to an improvement in TPQI visibility from 0.88 to 0.90.

Secondly, both the CHSH violation S and the QBER Q are impacted by the NV electronic spin state readout. The readout can be performed using resonant excitation of a spin-selective optical transition [87]. Improvements to the detection efficiency can be obtained by storing the spin state in the nearby nitrogen spin state, and performing repeated readout [88]. We estimate that the repeated readout can lead to an average readout fidelity of ≈ 0.985, compared to an initial 0.97 [89] [5].

Other improvements can be envisioned, such as enhancement of the detection efficiency by improving the photon collection efficiency through the use of parabolic reflectors [90] or optical cavities [91]. In the following discussion we limit ourselves to the two advances listed above and summarized in Table 5.3.

DIQKD parameters	Ref. [53, 78]		Expected	
setup	A	B	A	B
average readout fidelity	0.974	0.969	0.985	0.985
TPQI visibility	0.88		0.90	
S	2.38 ± 0.14		2.47	
Q	0.06 ± 0.03		0.051	

Table 5.3: The CHSH violation S and QBER Q in NV centre-based implementations are strongly dependent on the TPQI visibility and the readout fidelity. The resulting values are shown for parameters achieved in a loophole-free Bell test, and for expected values from several readily-implementable improvements.

Taking into account these improvements, the expected DIQKD parameters are $S \approx 2.47$ and $Q \approx 0.051$. In Figure 5.4 we illustrate the rates achievable for these parameters against general coherent attacks and under the assumption that the eavesdropper is restricted to collective attacks. We see that the required minimum number of rounds is of order 10^8 for general attacks, and about 5×10^6 for collective attacks.

[5] We note that this readout method increases the readout duration, which compromises spacelike setup-separation. However, security in a DIQKD implementation does not require spacelike separation since it is superfluous with the assumption of isolated labs in place (see Assumptions 5.1.1). Therefore, an increased readout time does not present a problem for security.

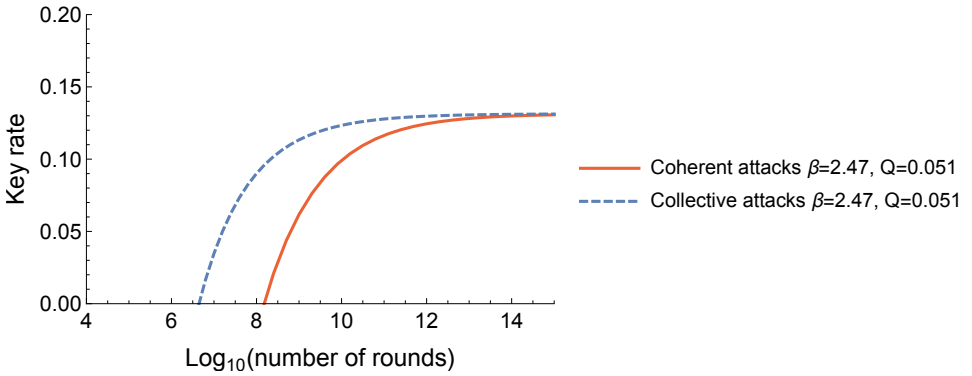


Figure 5.4: Key rates vs logarithm of the number of rounds n for parameters that are readily-implementable in NV centres setups (CHSH violation $S = 2.47$ and QBER $Q = 0.051$). The red line shows the key rates obtained against general coherent attacks, and the blue dashed line shows the key rates under the assumption of collective attacks. The security parameters are chosen to be $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.

ENTANGLING RATE.

Although the improved parameters lead to a positive key rate, this does not mean that DIQKD with NV centres is readily achievable. The system faces another challenge: the probabilistic nature of the heralded entanglement scheme limits the entanglement generation rate.

In the heralded entanglement generation protocol used in [53, 75] the photonic qubit is time-bin encoded and entanglement is heralded with the detection of a photon in each of two time-bins [86]. Since two photons have to be detected, the rate of the protocol is proportional to the square of the photon losses. For the spacelike separated setups in [53] the total emission and detection efficiency per photon is $\approx 10^{-4}$, leading to a total success probability of $\approx 10^{-8}$. Since the repetition rate, limited by the spin-state reset time, is of the order of $\approx \mu$s, generating a raw key of length 10^6 bits would take $\approx 10^3$ days. It is clear that a speed-up of entanglement generation rate is required to use NV centres in a DIQKD protocol. We describe two approaches toward this.

Firstly, this could be achieved by adapting the entanglement generation protocol. A linear dependency of the rate on photon losses can be achieved by employing an extreme-photon-loss (EPL) protocol [92] or single-photon (SP) protocol [93]. Demonstrated implementations of these protocols with NV centres indeed provide a speed-up in entanglement rate of three orders of magnitude [80, 81]. However, these implementations do not yet provide the entangled state fidelities leading to Bell violations that allow for DIQKD (the entangled state fidelities are $F_{EPL} = 0.65 \pm 0.03$ and $F_{SP} = 0.81 \pm 0.02$, leading to no Bell violation for the EPL protocol and a small violation $S_{SP} = 2.1$ for the single photon protocol). Better parameters may be achieved with improvements of the robustness of the nuclear-spin memories [85] and with an improved photon detection versus dark-count rate [93].

Secondly, an increase in the entanglement rate can be achieved by a reduction of the photon losses per round. These losses consist of three parts: a low coherent-photon

emission probability, a non-unit collection efficiency and fiber attenuation. The photon attenuation during transmission over fibers is ≈ 8 dB for the NV emission wavelength (637 nm). To maintain high entangling rates for distant setups, this should be reduced. This can be achieved by frequency downconversion of the photons at a wavelength of 637 nm emitted by the NV centres to telecom frequencies [94, 95]. The emission probability of coherent photons, ≈ 3%, and subsequent collection efficiency (≈ 10%, [75]) together limit the best achievable entangling rates. They can be addressed simultaneously by embedding the NV centre in an optical cavity to enhance coherent-photon emission and the collection efficiency [91]. A promising approach employs NV centres in diamond membranes in Fabry-Perot microcavities [96–98]. In such a design NV centres remain far away from the optical interface, retaining bulk-like optical coherence properties. These cavities are expected to provide three orders of magnitude enhancement in entangling rate for a two-click protocol [97]. Together with the improved DIQKD parameters described above, this makes a demonstration of DIQKD with NV centres experimentally feasible.

	S	Q
(1) Matsukevich et al., PRL 100, 150404 (2008) [59]	2.22 ± 0.07	0.041 ± 0.003
(2) Pironio et al., Nature 464, 1021-1024 (2010) [60]	2.414 ± 0.058	0.041 ± 0.003
(3) Giustina et al., Nature 497, 227-230 (2013) [57]	2.02096 ± 0.00032	0.0297 ± 0.0003
(4) Christensen et al., PRL 111, 130406 (2013) [58]	2.00022 ± 0.00003	0.0244 ± 0.0009
(5) Giustina et al., PRL 115, 250401 (2015) [54]	2.000030 ± 0.000002	0.0379 ± 0.0002
(6) Shalm et al., PRL 115, 250402 (2015) [55]	2.00004 ± 0.00001	0.0292 ± 0.0002
(7) Hensen et al., Nature 526 682-686 (2015) [53]	2.38 ± 0.14	0.06 ± 0.03
(8) Rosenfeld et al., PRL 119, 010402 (2017) [56]	2.221 ± 0.033	0.035 ± 0.003
(9) Expected improvements in NV systems	2.47	0.051

Table 5.4: Summary of the estimated parameters of interest for DIQKD. (1,2) are Bell tests with trapped ions, (3-5) are all-photonic experiments, (7) uses NV centres and (8) trapped atoms. (9) reports on near-term achievable parameters with NV centers as described in Section 5.2.3. In all experiments the detection loophole is closed; (5-8) additionally close the locality loophole. The CHSH violations for neutral atoms (8), trapped ions (1,2) and NV centres (7) are as reported in the corresponding experiments. For (3), (4) and (5), in which the value of the CH-Eberhard inequality J is reported, we make use of the relation $S = 4J + 2$ between the CHSH value and the CH-Eberhard value. This relation is found if one attributes "output 1" to undetected events in a CHSH inequality test. For (6) the CHSH violation was estimated directly from the reported data. For the estimation of the QBER (Q), in (1),(2) and (8) we assume perfect classical correlation in the generated state and find a lower bound for the QBER from reported detection efficiencies (0.979 ± 0.002 [99] for (1) and (2), and 0.982 ± 0.002 [100] for (8)). For NV centres (7), we additionally account for imperfections in the entangled state based on the reported density matrix. For all-photonic systems (3-6), the QBER is estimated by taking into account the detection efficiency and using the reported estimated state and the measurements performed by Alice, optimizing over measurements for Bob.

Figure 5.5: Region of positive key rates for coherent attacks: The red area is the region of values of QBER (Q) and CHSH violation (S) for which a positive key rate cannot be reached with any number of rounds. In the green area, the dashed curves represents the minimum number of rounds required to get positive key rate. For parameters above each curve, a key rate can be extracted if the number of rounds is higher than specified in the curve. The points show the Bell violation and estimated QBER achieved by previous experiments (see Table 5.4). They, however, do not reflect the corresponding entanglement generation rates. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.

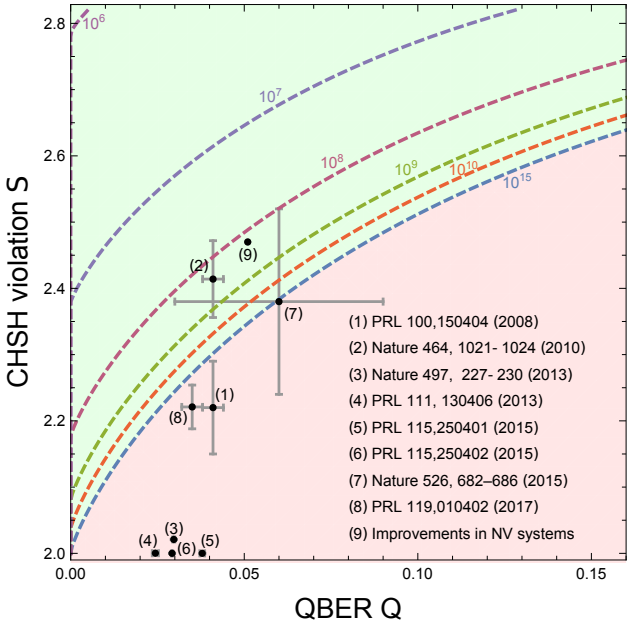
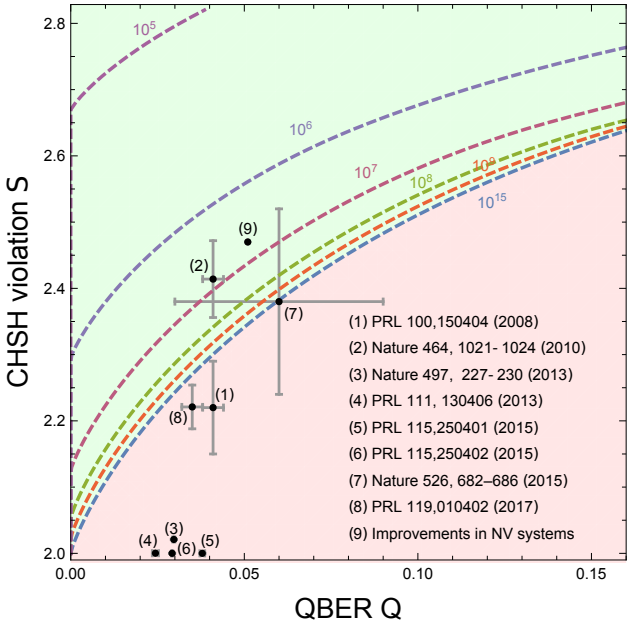


Figure 5.6: Region of positive key rates for collective attacks: The red area is the region of values of QBER (Q) and CHSH violation (S) for which a positive key rate cannot be reached with any number of rounds. In the green area, the dashed curves represents the minimum number of rounds required to get positive key rate. For parameters above each curve, a key rate can be extracted if the number of rounds is higher than specified in the curve. The points show the Bell violation and estimated QBER achieved by previous experiments (see Table 5.4). They, however, do not reflect the corresponding entanglement generation rates. Similarly to [1], we take $\epsilon^c_{DIQKD} = 10^{-2}$ and $\epsilon^s_{DIQKD} = 10^{-5}$.



5.3. DISCUSSION

Detection-loophole-free Bell tests between separated setups mark an important step towards the implementation of DIQKD. Progress towards extending Bell experiments to larger distances were also achieved, in particular by the Bell tests additionally closing the locality loophole. However a DIQKD protocol has not yet been implemented.

In order to shed light on the experimental performance needed for DIQKD, we have derived the key rates in the finite size regime as a function of the experimental parameters: CHSH violation S and QBER Q. For comparison of the key rates obtained in the finite regime for coherent and collective attacks, we have used as a benchmark an implementation where the maximally entangled state is subjected to depolarizing noise. Although the asymptotic key rates against collective attacks and general coherent attacks coincide, it is known that this is not the case in the finite regime. We find that, with the currently available tools, security against coherent attacks requires a minimum number of rounds about two orders of magnitude higher than what is necessary for security against collective attacks for realistic near-term parameters.

Here, we have focused on DIQKD protocols that use the CHSH inequality. So far the

CHSH inequality is the one which leads to the best performance for a DIQKD protocol. The challenge in using other Bell inequalities is that, up to date, only non-tight lower bounds on the secure key rates can be derived. Therefore, it is still an open question whether any other Bell inequality can outperform the CHSH, either in terms of maximum tolerable QBER, higher rates or lower minimum number of rounds required.

Towards exploring the potential of different experimental platforms to implement DIQKD, we have analyzed the Bell violation and expected QBER of previously performed Bell tests and situated these parameters in the context of the derived key rates. Figures 5.5 and 5.6 summarize this analysis.

For photonic systems, a DIQKD implementation is currently barred by the very low CHSH violation. To overcome this, a strong reduction of photon losses is required.

Detection-loophole free Bell tests based on heralded entanglement schemes approach the allowed region, with the Bell test of Ref. [60], performed with trapped ions separated by 1 meter, even exhibiting parameters in the allowed region. These heralded schemes however suffer from low entangling rates resulting from photon losses. An increase in the entangling rates is expected to be achieved by improving collection efficiencies, e.g. by employing optical cavities. Moreover, with frequency downconversion these results can be extended to long ($\gg 1$ km) distances. We illustrate that with near-term experimental improvements for NV centres, in combination with optical cavities for enhancing entangling rate, described in Section 5.2.3, a demonstration of DIQKD is achievable.

5.4. METHODS

We now present the theoretical tools that allows us to derive the key rates for the device-independent quantum key distribution protocols, Protocol 5.2.1 and Protocol 5.2.3. We start by defining some quantities that are going to play an important role in the security proof and state in more details the security definition for device-independent quantum key distribution.

5.4.1. NOTATION AND DEFINITIONS

As for the previous chapters we will use the (smoothed) min- and max-entropy as defined in Chpater 2. In this chapter we will however use other entropic quantities of interest that are the conditional von-Neumann entropy, $H(A|E)_\rho$, and the conditional collision entropy $H_2(A|E)_\rho$. They are particular cases of the one-parameter family of entropies called sandwiched conditional Réyni entropies, first defined in Ref. [101].

Definition 5.4.1. *For any density operator ρ_{AE} and for $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty)$ the sandwiched α-Réyni entropy of A conditioned on E is defined as*

$$H_\alpha(A|E)_\rho := \frac{1}{1-\alpha} \log \left(\mathrm{Tr} \left[\left(\rho_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \rho_E^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right), \tag{5.13}$$

where $\rho_E^{\frac{1-\alpha}{2\alpha}}$ is a short notation for $\mathbb{1}_A \otimes \rho_E^{\frac{1-\alpha}{2\alpha}}$.

A variant can also be defined as

$$H_\alpha^\uparrow(A|E)_\rho := \sup_{\sigma_E \in \mathscr{S}} \frac{1}{1-\alpha} \log \left(\mathrm{Tr} \left[\left(\sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \sigma_E^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right), \tag{5.14}$$

where $\mathscr{S}$ denotes the set of quantum states and the supremum is taken over density operators σ_E.

The min- and max- entropy correspond to the extremal cases of definition (5.14) for $\alpha = \infty$ and $\alpha = \frac{1}{2}$ respectively. For $\alpha \to 1$, definition (5.13) and (5.14) coincide and one recover the standard conditional von-Neumann entropy. Properties of the conditional α-Réyni entropies are presented in 5.5.1.

5.4.2. SECURITY OF DIQKD

In order to determine what it means for a DIQKD protocol to be secure, we adopt the security definition used in [41]. This security definition follows the universally composable security definition for standard QKD protocols [42]. However it is important to note that for the device-independent case composability was never proved and attacks proposed in Ref. [37] show that composability is not achieved if the same devices are re-used for generation of a subsequent key.

In the composably secure paradigm, the security of a protocol is defined in terms of its distance to an ideal protocol [42, 102]. Following this definition, given a protocol described by the completely positive and trace preserving (CPTP) map $\text{diqkd}_{\text{real}}$, we say that the protocol is ϵ^s_{DIQKD}-secure for any $\epsilon^s_{DIQKD} \geq \epsilon$ if:

$$\epsilon := \frac{1}{2}\|\text{diqkd}_{\text{real}} - \text{diqkd}_{\text{ideal}}\|_\diamond \tag{5.15}$$

$$= \sup_{\rho_{ABE}} \frac{1}{2}\|\text{diqkd}_{\text{real}}(\rho_{\text{ABE}}) - \text{diqkd}_{\text{ideal}}(\rho_{\text{ABE}})\|_1. \tag{5.16}$$

Expression (5.16) can be split into two terms that reflect independently the correctness and the secrecy of the protocol (see [42]), given by Definitions 5.1.3 and 5.1.4. Correctness is the statement that Alice and Bob share equal strings of bits at the end of the protocol. And secrecy states how much information the eavesdropper can have about their shared key.

Another requirement for a good DIQKD protocol is that there exist a realistic implementation that do not lead the protocol to abort almost all the time, *i.e.*, the protocol should have some robustness. This is captured by the concept of completeness.

Definition 5.4.2 (Security)**.** *A DIQKD protocol is $(\epsilon^s_{DIQKD}, \epsilon^c_{DIQKD}, l)$-secure if*

1. *(Soundness) For any implementation of the protocol, either it aborts with probability greater than $1 - \epsilon^s_{DIQKD}$ or an ϵ^s_{DIQKD}-correct-and-secret key of length l is obtained.*

2. *(Completeness) There exists an honest implementation of the protocol such that the probability of not aborting, $p(\Omega)$, is greater than $1 - \epsilon^c_{DIQKD}$.*

The correctness of the final key is ensured by the error correction step. During error correction, Alice sends to Bob a sufficient amount of information so that he can correct his raw key. If Alice and Bob do not abort in this step, then the probability that they end up with different raw keys is guaranteed to be very small. For the secrecy of the protocol, according to Definition 5.1.4, one needs to estimate how far the final state describing

Alice's key and the eavesdropper system is from a state where the eavesdropper is totally ignorant about Alice's key, see Eq. (5.4). The formal security proof of quantum key distribution became possible due to the quantum Leftover Hash Lemma [49, 103] that quantifies the secrecy of a protocol as a function of a conditional entropy of the state before privacy amplification and the length of the final key.

Theorem 5.4.3 (Leftover Hash Lemma ([49], Theorem 5.5.1)). *Let $\rho_{A_1^n E}$ be a classical-quantum state and let $\mathscr{H}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^l$, that maps the classical n-bit string A_1^n into K_A. Then*

$$\|\rho_{K_A HE} - \tau_{K_A} \otimes \rho_{HE}\|_1 \leq 2^{-\frac{1}{2}\left(H_2^{\uparrow}(A_1^n|E)_\rho - l\right)}. \tag{5.17}$$

For the proof of the Leftover Hash Lemma we refer to Ref. [49]. In Ref. [49], it was shown that the Leftover Hash lemma can also be formulated in terms of the smooth min-entropy, and the price to pay is only a linear term in the security parameter[6].

Theorem 5.4.4 (Leftover Hash Lemma with smooth min-entropy [11, 49]). *Let $\rho_{A_1^n E}$ be a classical-quantum state and let $\mathscr{H}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^l$, that maps the classical n-bit string A_1^n into K_A. Then*

$$\|\rho_{K_A HE} - \tau_{K_A} \otimes \rho_{HE}\|_1 \leq 2^{-\frac{1}{2}\left(H_{\min}^{\epsilon}(A_1^n|E)_\rho - l\right)} + 2\epsilon. \tag{5.18}$$

Given the Leftover Hash Lemma, stated in Theorems 5.4.3 and 5.4.4, and the definition of secrecy, Definition 5.1.4, we can now express the length of a secure key as a function of the entropy of Alice's raw key conditioned on Eve's information before privacy amplification.

Theorem 5.4.5 (Key length). *Let $p(\Omega)$ be the probability that the DIQKD protocol does not abort for a particular implementation. If the length of the key generated after privacy amplification is given by*

$$l = H_2^{\uparrow}(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right). \tag{5.19}$$

then the DIQKD protocol is ϵ_{PA}-secret.

We can also express the key length in terms of the smooth min-entropy, where if l satisfies

$$l = H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{p(\Omega)}{2\epsilon_{PA}}\right) \tag{5.20}$$

$$\geq H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right), \tag{5.21}$$

then the DIQKD protocol is $(\epsilon_{PA} + \epsilon_s)$-secret.

We see that the leftover hash lemma expressed in terms of smooth min-entropy only leads to an extra ϵ_s term in the security parameter. However, the smooth min-entropy can be much larger than the 2-Rényi entropy $H_2^{\uparrow}$ and, therefore, it is advantageous to lower bound the key by the smooth min-entropy.

[6] In Ref. [49], the leftover hash lemma was formulated with the smooth min-entropy defined as a supremum over states that are ϵ-close to ρ in the trace norm. The proof of Theorem 5.4.4, with the smooth min-entropy defined according to Definition 5.4.1, can be found in Ref. [11].

5.4.3. SECURITY ANALYSIS

In the previous section we have seen that in order to determine the length of a secret key generated by a particular protocol one needs to estimate the (smooth-min or 2-Rényi) entropy of Alice's string conditioned on all the information available to the eavesdropper before privacy amplification. Now, in order to estimate this quantity for a DIQKD protocol one faces two main challenges:

- How to evaluate the entropy of a very long string of bits?
- How to evaluate the one-round entropy in the device-independent scenario?

In Section 5.4.3 we present the theoretical tools that allow to reduce the problem of evaluating the entropy of a string of bits to the evaluation of a single round. Moreover, in the DI scenario we do not want to make any assumptions over the underlying quantum state and measurement devices. In Section 5.4.3 we present a tight bound derived in [16, 27] for the one round conditional von Neumann entropy of protocols where Alice and Bob test the CHSH inequality. Moreover we explore further this bound to prove a tight bound on the single round conditional collision entropy as a function of the CHSH violation.

REDUCING THE PROBLEM TO THE ESTIMATION OF ONE ROUND.

We now present the techniques that allow to reduce the evaluation of the entropy $H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}}$ to the estimation of the conditional von Neumann entropy of a single round for the two adversarial scenarios under consideration, collective attacks and coherent attacks. Moreover, for the IID scenario, *i.e.* when the eavesdropper is assumed to be restricted to collective attacks, we show how to break the analysis of the entropy $H_2^{\uparrow}(A_1^n|E)_{\rho_{|\Omega}}$ into single rounds evaluation.

THE IID SCENARIO (COLLECTIVE ATTACKS).

When we restrict the eavesdropper to collective attacks, we are assuming that, even though she can perform an arbitrary operation in her quantum side information, the state distributed by the source and the behavior of Alice's and Bob's devices are the same in every round of the protocol. This implies that after n rounds, the state shared by Alice, Bob and Eve is $\rho_{A_1^n B_1^n E} = \rho_{ABE}^{\otimes n}$. In this case, the quantum asymptotic equipartition property (AEP) [61] allows to break the conditional smooth min-entropy of state $\rho_{AE}^{\otimes n}$ into n times the conditional von Neumann entropy of the state ρ_{AE}.

Theorem 5.4.6 (Asymptotic equipartition property [61])**.** *Let $\rho = \rho_{AE}^{\otimes n}$ be an IID state. Then for $n \geq \frac{8}{5}\log\frac{2}{\epsilon^2}$*

$$H_{\min}^{\epsilon}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \geq nH(A|E)_{\rho_{AE}} - \sqrt{n}\,\delta(\epsilon,\eta) \tag{5.22}$$

and similarly

$$H_{\max}^{\epsilon}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \leq nH(A|E)_{\rho_{AE}} + \sqrt{n}\,\delta(\epsilon,\eta) \tag{5.23}$$

where $\delta(\epsilon,\eta) = 4\log\eta\sqrt{\log\frac{2}{\epsilon^2}}$ and $\eta = \sqrt{2^{-H_{\min}(A|E)_{\rho_{AE}}}} + \sqrt{2^{H_{\max}(A|E)_{\rho_{AE}}}} + 1$.

The quantum AEP is a generalization to quantum systems of the classical statement that, in the limit of many repetitions of a random experiment, the output sequence is one from the typical set. Therefore, under the assumption of collective attacks, the quantum AEP reduces the problem of estimating the key rate of a string of n bits to the problem of bounding the one-round conditional von Neumann entropy. We remark that the AEP implies an additional term, proportional to $\sqrt{n}$, which is significant for the finite regime analyses.

In Section 5.4.2, we have seen that the left-over hash lemma can also be stated in the terms of the 2-Réyni conditional entropy $H_2^{\uparrow}(A|E)_\rho$. A useful property of the conditional $H_\alpha^{\uparrow}$ entropies is additivity [104] (see 5.5.1 Property 5.5.1(2)), which implies the following lemma.

Lemma 5.4.7. *Let $\rho = \rho_{AE}^{\otimes n}$ be an IID state. Then*

$$H_2^{\uparrow}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} = nH_2^{\uparrow}(A|E)_{\rho_{AE}} \geq nH_2(A|E)_{\rho_{AE}}, \tag{5.24}$$

where $H_2(A|E)_{\rho_{AE}}$ denotes the collision entropy.

Validity of Lemma 5.4.7 can be seen from the following: equality in (5.24) follows from the additivity property of $H_\alpha^{\uparrow}$ entropies, Property 5.5.1(2) in 5.5.1, and the inequality follows from the definition of α-Rényi entropies, Definition 5.4.1.

Therefore, for collective attacks one can break the analysis into the evaluation of a single-round entropy by using both, the formulation of the left-over hash lemma in terms of the smooth-min entropy, Theorem 5.4.4, and in terms of the 2-Rényi entropy, Theorem 5.4.3. The possible advantage of using Lemma 5.4.7 over the AEP, Theorem 5.4.6, is that no extra overhead term $\mathcal{O}(\sqrt{n})$ is gained due to the additive property of the 2-Réyni conditional entropy $H_2^{\uparrow}(A|E)_\rho$. However, in general the von Neumann entropy can be much larger than the collision entropy, and this trade-off has to be taken into account. We remark that, for protocols based on other Bell inequalities, the techniques used for deriving Theorem 5.2.5 can be advantageous for collective attack analysis. This is due to the fact that for other Bell inequalities there is no known technique to directly bound the conditional von-neumann entropy and a good bound on the min-entropy can be found using semidefinite-programming techniques (see Section 5.4.3).

THE FULLY DI SCENARIO (COHERENT ATTACKS).
In the fully device-independent scenario the eavesdropper can perform a general coherent attack, and the state shared by the parties may not be of the form $\rho_{ABE}^{\otimes n}$. Therefore, the tools presented in the previous section are not applicable in this scenario. In standard QKD, de Finetti techniques [48, 49, 51] allow one to extend the proofs against collective attacks to coherent attacks for protocols that present some symmetry. The price to pay is an overhead term $\mathcal{O}(\sqrt{n})$ whose pre-factor depends on the dimension of the underlying system. However, in the device-independent scenario, we do not want to make assumptions on the dimension of the underlying system. Moreover, symmetry of the protocol is not guaranteed, as we do not know the behaviour of the measurement devices. Therefore, de Finetti techniques cannot be used to straightforwardly extend the

security proofs against collective attacks to coherent attacks in the device-independent scenario.

Recently, this problem was overcome by the Entropy Accumulation Theorem (EAT) [1, 52]. In this section, we state the Entropy Accumulation Theorem, which allows to break the entropy $H_{\min}^{\epsilon_s/p(\Omega)}(A_1^n|E)_{\rho_{|\Omega}}$ into the entropy of single rounds and therefore extends proofs against collective attacks to coherent attacks.

We give here a quick reminder of the statement of the Entropy Accumulation Theorem. For more details see Chapter 2 Section 2.3.3.

Theorem 5.4.8 (The Entropy Accumulation Theorem (EAT) [52])**.** *For $1 \leq i \leq n$ let $\mathcal{M}_i$ be a EAT channel from register R_{i-1} to $A_iB_iC_iR_i$, and let $\rho_{A_1^nB_1^nE}$ of the form,*

$$\rho_{A_1^nB_1^nE} = \mathrm{tr}_{R_n}(\mathcal{M}_n \circ \ldots \circ \mathcal{M}_1(\rho_{R_0E})). \tag{5.25}$$

Let $f_{\min}$ be an affine min-tradeoff function, and $f_{\max}$ be an affine max-tradeoff function. For an event Ω that happens with probability $p(\Omega)$, and for t such that $f_{\min}(\mathsf{freq}(c_1^n)) \geq t$ $\forall\ c_1^n \in \Omega$, it holds that

$$H_{\min}^{\epsilon}(A_1^n|B_1^nE)_{\rho_{|\Omega}} > nt - \nu\sqrt{n} \tag{5.26}$$

and similarly, for t' such that $f_{\max}(\mathsf{freq}(c_1^n)) \leq t'\ \forall\ c_1^n \in \Omega$,

$$H_{\max}^{\epsilon}(A_1^n|B_1^nE)_{\rho_{|\Omega}} < nt' + \nu\sqrt{n} \tag{5.27}$$

with

$$\nu = 2\left(\log(1+2d_A) + \lceil\|\nabla f\|_\infty\rceil\right)\sqrt{1-2\log\left(\epsilon_s \cdot p(\Omega)\right)} \tag{5.28}$$

for f equals to $f_{\min}$ and $f_{\max}$ respectively.

Analogous to the AEP, the Entropy Accumulation Theorem allows us to break the entropy of the string of bits into the entropy of a single round. Note, however, that this single-round entropy does not refer to the real entropy of each round of the protocol, but is evaluated over the hypothetical states that would achieve the observed violation. It is important to remark that a crucial assumption in the EAT [1, 52] is that some of the variables of interested satisfy what is called the Markov condition (see Chapter 2 Section 2.3.3). This is the case for QKD protocols performed sequentially. For definition and discussion of the implications of the Markov condition, see [52].

ESTIMATING THE ONE-ROUND ENTROPY.

Now that we have reduced the evaluation of the secret key length to the estimation of the conditional von Neumann entropy of a single round, we are ready to face the next challenge: How to estimate the single round entropy without any assumptions on the quantum states and behavior of the measurement devices.

THE CHSH SCENARIO:
The CHSH scenario [39], where Alice and Bob each perform one among two possible binary measurements, is significantly simpler than other Bell scenarios. Due to the fact that the CHSH inequality has only two binary inputs per party, a strong result [105, 106] states that the description of any realization of a CHSH experiment can be decomposed into subspaces of dimension two, where projective measurements are performed in each subspace. This allows one to restrict the analysis to qubits, which significantly simplifies the problem. Exploring these nice properties, a tight bound on the von Neumann entropy of Alice's outcome conditioned on Eve's information, as a function of the CHSH violation, was derived in [16, 27].

Lemma 5.4.9. *Given that Alice and Bob share a state ρ_{AB} that achieves a violation S for the CHSH inequality, it holds that*

$$H(A|E)_\rho \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{S}{2}\right)^2 - 1}\right). \tag{5.29}$$

5

In Section 5.4.3 we have seen that for collective attacks the key rate can also be estimated by the single round collision entropy. And due to the additivity property of $H_2^\uparrow$, no overhead $\sqrt{n}$ term is present. Therefore, this analysis can potentially lead to an advantage with respect to the minimum number of rounds required for positive key rate. The conditional collision entropy satisfies the following relation [104, Corollary 5.3]

$$H_2(A|E)_\rho \geq H_{\min}(A|E)_\rho. \tag{5.30}$$

And a lower bound for the conditional min-entropy as a function of the Bell violation was derived in [107]:

$$H_{\min}(A|E)_\rho \geq -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{S^2}{4}}\right). \tag{5.31}$$

Therefore expression (5.31) can be used to bound the conditional collision entropy as a function of the violation S. We now prove that this bound is actually tight.

Theorem 5.4.10. *There exist a state ρ^*_{AB} and measurements for Alice and Bob such that, ρ^*_{AB} achieves violation S and the collision entropy of Alice's output A conditioned on Eve's quantum information E is*

$$H_2(A|E)_{\rho^*} = -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{S^2}{4}}\right). \tag{5.32}$$

The proof of Theorem 5.4.10 is presented in 5.5.3. Theorem 5.4.10 together with relations (5.30) and (5.31) imply a tight lower bound for the conditional collision entropy as a function of the CHSH violation S. In Figure 5.7 we plot $H(A|E)$ and $H_2(A|E)$ as a function of the violation S. One can see that the points of maximum and minimum

entropy (corresponding to maximal violation $S = 2\sqrt{2}$ and no violation, respectively) coincide, but for intermediate values of S the conditional collision entropy is smaller than the conditional von Neumann entropy.

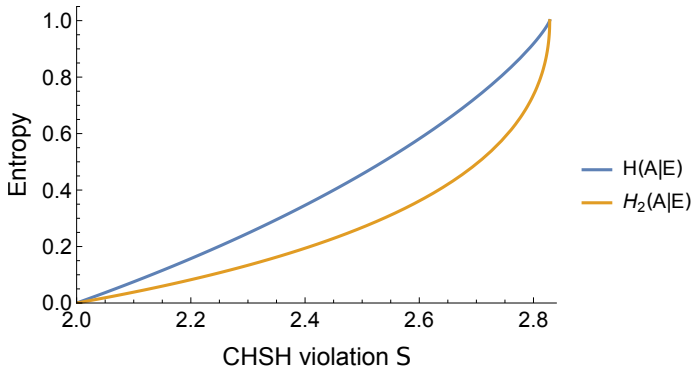


Figure 5.7: Graph illustrating the difference of the conditional von Neumann entropy $H(A|E)$ and the conditional collision entropy $H_2(A|E)$ as a function of the CHSH violation S.

OTHER BELL INEQUALITIES AND THE MIN-ENTROPY ESTIMATION:
The use of different Bell inequalities has proved to be advantageous in different taks. For example, a tilted CHSH inequality was used to certify maximal randomness in states arbitrarily close to separable [108], and inequalities with more inputs and outputs have shown to exhibit higher noise robustness [109]. Therefore it is natural to ask whether other Bell inequalities can also bring advantage to the task of device-independent quantum key distribution.

By considering an arbitrary Bell inequality, one faces the problem that the techniques used to bound the conditional von Neumann entropy as a function of the CHSH violation do not apply. Indeed, the proof of Lemma 5.4.9 is highly based on the fact that one can reduce the analysis to qubits. In fact, very few results are known on tight bounds for the conditional von Neumann entropy as a function of the Bell violation for other inequalities. In [110] a bound was derived for a family of inequalities denoted measurement-device-dependent inequalities [111], which are very suitable for the task of randomness amplification. In [112] a tight bound was derived as a function of the violation of the multipartite MABK inequality [113–115]. However in these two cases the proof is based on a reduction to the CHSH inequality.

In general, the conditional von Neumann entropy can be lower bounded by the conditional min-entropy

$$H(A|E)_\rho \geq H_{\min}(A|E)_\rho. \tag{5.33}$$

The advantage of looking at the conditional min-entropy is that it can be computed as a function of the Bell violation by a semi-definite programming [107]. The idea is that in order to estimate the min-entropy one can upper bound the guessing probability, P_{guess} (see Eq. (2.55) in Chapter 2), of the eavesdropper. This problem can then be expressed as an optimization over probability distributions, which is exactly the information available in the device-independent scenario. As shown in Ref. [107], for any Bell inequality, an

upper bound on the p_{guess} can be obtained by a semidefinite programming making use of the NPA-hierarchy [116, 117].

Lower bounding the conditional von-Neumann entropy by the min-entropy might be far from optimal. For example, for the CHSH inequality we have that the conditional von Neumann entropy as a function of the violation is much larger than the conditional min-entropy, as illustrated in Fig. 5.7 (recall that, in Theorem 5.4.10, $H_{\min}(A|E)_\rho$ was shown to be a tight bound on $H_2(A|E)_\rho$ as a function of the CHSH violation). By making use of the tight bound on the conditional von Neumann entropy, eq. (5.29), one can prove security for DIQKD up to 7.1% of QBER [16], whereas using the min-entropy, eq. (5.31), security can only be guaranteed up to a QBER of 5.2% [107].

It is still an open problem whether any other Bell inequality can lead to better performance for DIQKD than the CHSH inequality. Recently, an extensive analysis of the performance of different Bell inequalities for the task of randomness expansion was presented in [118].

KEY RATES.

5

The techniques presented in Sections 5.4.3 and 5.4.3 allows us to establish the length of a secure key that can be extracted as a function of the CHSH violation S and QBER Q.

For coherent attacks, the Entropy Accumulation Theorem (Theorem 5.4.8) and the tight lower bound on the conditional von Neumann entropy (Lemma 5.4.9) are the key tools to establish Theorem 5.2.2. The complete proof of Theorem 5.2.2 includes several intermediate steps, and is presented in details in 5.5.2.

For collective attacks, the key ingredients to derive Theorem 5.2.4 are the asymptotic equipartition property (Theorem 5.4.6) and Lemma 5.4.9. A detailed proof of Theorem 5.2.4 is presented in 5.5.2. We have also presented a different technique of breaking the entropy of Alice's string into the entropy of single rounds in the IID scenario, namely by making use use of the additivity of 2-Réyni entropy, Lemma 5.4.7. This technique, together with Theorem 5.4.10 leads to Theorem 5.2.5. A detailed proof of Theorem 5.2.5 can be found in 5.5.2.

5.5. TECHNICAL DETAILS

5.5.1. DEFINITIONS

In this Section we present some properties of the conditional sandwiched α-Réyni entropies [101], Definition 5.4.1, and the smoothed entropies that are used for the security proof.

Proposition 5.5.1. *The conditional α-Rényi entropies satisfy:*

1. ***Data processing*** *([104] Corollary 5.1): Let $\tau_{AB'} = I_A \otimes \mathcal{E}_B(\rho_{AB})$, where $\mathcal{E}_B$ is a CPTP(B, B') channel, then*

$$H_\alpha(A|B)_\rho \leq H_\alpha(A|B')_\tau \text{ and } H^\uparrow_\alpha(A|B)_\rho \leq H^\uparrow_\alpha(A|B')_\tau. \tag{5.34}$$

2. ***Additivity*** *([104] Corollary 5.2): For $\rho_{AB} \otimes \tau_{A'B'}$ it holds that*

$$H^\uparrow_\alpha(AA'|BB')_{\rho\otimes\tau} = H^\uparrow_\alpha(A|B)_\rho + H^\uparrow_\alpha(A'|B')_\tau. \tag{5.35}$$

3. ***Entropy of classical information****([104] Lemma 5.3): For ρ_{ABX} classical in X*

$$H_\alpha(XA|B)_\rho \geq H_\alpha(A|B)_\rho \text{ and } H^\uparrow_\alpha(XA|B)_\rho \geq H^\uparrow_\alpha(A|B)_\rho. \tag{5.36}$$

4. ***Conditioning on classical information*** *(see [104] Lemma 5.4): For ρ_{ABX} classical in X,*

$$H^\uparrow_\alpha(A|XB) \geq H^\uparrow_\alpha(A|B) - \log\big(\text{rank}(\rho_X)\big) \tag{5.37}$$

$$\geq H^\uparrow_\alpha(A|B) - \log|X|, \tag{5.38}$$

where $\text{rank}(\rho_X)$ *is the rank of matrix ρ_X and $|X|$ is the dimension of system X.*

5. ***Conditioning on classical information*** *(see [104] Proposition 5.1): Let $\rho_{ABX} = \sum_x p_x \rho^x_{AB} \otimes |x\rangle\langle x|$ then,*

$$H_\alpha(A|BX)_\rho = \frac{1}{1-\alpha}\log\left(\sum_x p(X=x)2^{\left((1-\alpha)H_\alpha(A|BX=x)_\rho\right)}\right), \tag{5.39}$$

$$H^\uparrow_\alpha(A|BX)_\rho = \frac{\alpha}{1-\alpha}\log\left(\sum_x p(X=x)2^{\left(\frac{1-\alpha}{\alpha}H^\uparrow_\alpha(A|BX=x)_\rho\right)}\right). \tag{5.40}$$

And for the conditional von Neumann it holds that

$$H(A|BX)_\rho = \sum_x p(X=x)H(A|BX=x)_\rho. \tag{5.41}$$

6. ***Entropy of the conditioned state*** *(see [52] Lemma B.5): Let $\rho_{ABX} = \sum_x p_x \rho_{AB|x}$ then,*

$$H^\uparrow_\alpha(A|B)_{\rho_{AB|x}} \geq H^\uparrow_\alpha(A|B)_\rho - \frac{\alpha}{\alpha-1}\log\left(\frac{1}{p_x}\right). \tag{5.42}$$

In Property 5.5.1.(4), the relation $H^\uparrow_\alpha(A|XB) \geq H^\uparrow_\alpha(A|B) - \log|X|$ was stated in [104]. We remark that the middle inequality follows from the fact that $H^\uparrow_\alpha(A|XB)$ is invariant under local isometries. Therefore if $X' = \mathcal{V}(X)$ is a full rank operator where $\mathcal{V}(\cdot)$ is an isometry, we have that

$$H^\uparrow_\alpha(A|XB) = H^\uparrow_\alpha(A|X'B) \geq H^\uparrow_\alpha(A|B) - \log|X'| \tag{5.43}$$

and since $\mathcal{V}(\cdot)$ is an isometry $|X'| = \text{rank}(\rho_X)$.

The min- and max- entropy are the particular extreme cases of $H^\uparrow_\alpha$ for $\alpha = \infty$ and $\alpha = \frac{1}{2}$ respectively. For $\alpha \to 1$ one recovers the standard conditional von-Neumann entropy.

The smoothed entropies satisfy several chain rules. Some of them are stated below. A more complete list of chain rule relations can be found in [104, 119].

Proposition 5.5.2 (Chain rules for the smooth min-entropy)**.** *The smooth min-entropy satisfy the following relations*

1. *For a quantum state* ρ_{ABC},

$$H_{\min}^{\epsilon}(A|BC)_{\rho} \geq H_{\min}^{\frac{\epsilon}{4}}(AB|C)_{\rho} - H_{\max}^{\frac{\epsilon}{4}}(B|C)_{\rho} - 2\log\left(1-\sqrt{1-\left(\frac{\epsilon}{4}\right)^2}\right). \tag{5.44}$$

2. *If* X *is a classical register and* ρ_{ABX} *a quantum-quantum-classical state, it holds that*[7]

$$H_{\min}^{\epsilon}(A|XB)_{\rho} \geq H_{\min}^{\epsilon}(A|B)_{\rho} - \log\left(\text{rank}(\rho_X)\right), \tag{5.45}$$

where $\text{rank}(\rho_X)$ *is the rank of state* ρ_X.

A fully contained overview with properties and relations between different entropies can be found in [104] (see also, [120]).

5

5.5.2. SECURITY PROOF

According to Definition 5.4.2, a security proof of a DIQKD protocol consists in completeness and soundness. We start by proving completeness of Protocols 5.2.1 and 5.2.3.

Theorem 5.5.3 (Completeness)**.** *The DIQKD protocols in consideration, Protocols 5.2.1 and 5.2.3 are* ϵ_{DIQKD}^{c} *complete, with*

$$\epsilon_{DIQKD}^{c} \leq \epsilon_{EC}^{c} + \epsilon_{est} + \epsilon_{EC}. \tag{5.46}$$

Proof. The protocols in consideration can abort in two steps. Either because the error correction fail, or because the estimated Bell violation is not high enough. Let us consider an honest implementation consisting of IID rounds where the expected winning CHSH probability is ω_{exp}.

$$\begin{aligned} p(\text{abort}) &= p((\text{EC abort}) \text{ or } (\text{EC does not abort and Bell test fail})) \\ &\leq p(\text{EC abort}) + p(\text{EC does not abort and Bell test fail}) \end{aligned}$$

Now, the probability that the error correction protocol abort for an honest implementation is $p(\text{EC abort}) \leq \epsilon_{EC}^{c}$. And for the other term we have

$$\begin{aligned} &p(\text{EC does not abort and Bell test fail}) \\ &\quad = p(K_A = K_B)\, p\Big(\sum_i C_i < \sum_i T_i \times \left(\omega_{exp} - \delta_{est}\right) | K_A = K_B\Big) \\ &\qquad + p(K_A \neq K_B)\, p\Big(\sum_i C_i < \sum_i T_i \times \left(\omega_{exp} - \delta_{est}\right) | K_A \neq K_B\Big) \\ &\quad \leq \epsilon_{est} + \epsilon_{EC}, \end{aligned}$$

where $\epsilon_{est} = e^{-2\gamma n(\delta_{est})^2}$ follows from Hoeffding's inequality. □

[7] In [104] relation $H_{\min}^{\epsilon}(A|XB)_{\rho} \geq H_{\min}^{\epsilon}(A|B)_{\rho} - \log|X|$ was proved. Relation (5.45) with the rank of ρ_X follows as pointed out in Property 5.5.1.(4).

For the soundness proof we have to evaluate correctness and secrecy, Definitions 5.1.3 and 5.1.4. For an error correction protocol with error parameter ϵ_{EC} we have that given that the error correction protocol does not abort, the probability that the string $\tilde{B}$ after error correction is equal to A_1^n with probability higher than $1-\epsilon_{EC}$ and consequently

$$P(K_A \neq K_B) \leq \epsilon_{EC}. \tag{5.47}$$

For the secrecy let us recall that, for each considered Protocol, Ω is defined as the event that the respective protocols do not abort. That happens when the error correction protocol does not abort and they achieved the required violation of CHSH according to Bob's estimation of Alice's string. Now, let us the define the event $\hat{\Omega}$ as the event Ω of the Protocol not aborting **and** the error correction being successful, *i.e.* $\tilde{B}_1^n = A_1^n$. Now the quantity we need to estimate for the secrecy, relates to the event $\hat{\Omega}$ by

$$\begin{aligned} \|\rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_E\|_1 &\leq \|\rho_{K_A E|\Omega} - \rho_{K_A E|\hat{\Omega}}\|_1 + \|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\|_1 \\ &\leq \epsilon_{EC} + \|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\|_1 \end{aligned} \tag{5.48}$$

which follows from the fact that, since when error correction succeeds, the probability of $\tilde{B}_1^n = A_1^n$ is higher than $(1-\epsilon_{EC})$ then the following operator inequality holds: $\rho_{K_A E|\Omega} \geq (1-\epsilon_{EC})\rho_{K_A E|\hat{\Omega}}$.

In the following, we proceed to evaluate $\|\rho_{K_A E|\hat{\Omega}} - \tau_{K_A} \otimes \rho_E\|_1$ in order to prove Theorems 5.2.2, 5.2.4 and 5.2.5.

PROOF OF THEOREM 5.2.4

In this Section we present the proof of Theorem 5.2.4, that determines the size of a secret key one can extract from Protocol 5.2.3 under the assumption that the eavesdropper is restricted to collective attacks. Importantly, Theorem 5.2.4 is based on the asymptotic equipartition property, Theorem 5.4.6, in order to break the entropy of the n rounds into the one-round entropy.

The collective attacks assumption implies that in each round of the protocol the state distributed to Alice and Bob is the same, as well as their devices function in the same way, *i.e.* the rounds are independent and identically distributed (IID). Therefore the state shared between Alice, Bob and Eve after Alice and Bob measure their raw keys is described by a tensor product form $\rho_{ABE}^{\otimes n}$.

The asymptotic equipartition property (AEP) [61], Theorem 5.4.6, states that the smooth min-entropy of a tensor product of states is almost equivalent (up to terms of order of $\sqrt{n}$) to n times the von-Neumann entropy of an individual system. We now make use of the quantum AEP to derive the length of a secure key that one can achieve for Protocol 5.2.3.

As established by the Leftover Hash Lemma, Theorem 5.4.4, the maximal length of a secure key is determined by the smooth min-entropy of Alice's raw key conditioned on all information available to the eavesdropper, given that the protocol did not abort. In the case of Protocol 5.2.3, it is given by

$$H_{\min}^{\frac{\epsilon_S}{p(\Omega)}}(A_1^n|X_1^n Y_1^n T_1^n EO_{EC})_{\rho_{|\hat{\Omega}}}. \tag{5.49}$$

Here we recall that O_{EC} is the information exchanged by Alice and Bob during the error correction protocol. T_1^n, X_1^n, Y_1^n are, respectively, the variable that determines whether the round is a test or a key generation round, and Alice and Bob's inputs, which are communicated publicly. $\hat{\Omega}$ is the event that error correction protocol succeeds, *i.e.* $K_A = K_B$ and the CHSH probability estimated by Bob is $\omega \geq \omega_{exp} - \delta_{est}$. In the following we describe the steps to estimate (5.49).

In order to avoid the conditioned state we can give one step back and note that in Definition 5.1.4 we want to bound

$$p(\hat{\Omega})\|\rho_{K_A HE|\hat{\Omega}} - \tau_{K_A} \otimes \rho_{HE|\hat{\Omega}}\|_1 = \|\rho_{K_A HE \wedge \hat{\Omega}} - \tau_{K_A} \otimes \rho_{HE \wedge \hat{\Omega}}\|_1 \tag{5.50}$$

where $\rho_{K_A HE \wedge \hat{\Omega}} = p(\hat{\Omega})\rho_{K_A HE|\hat{\Omega}}$. Now using the Leftover Hash Lemma, Theorem 5.4.4, we can express an $(\epsilon_{PA} + \epsilon_s)$-secret key by

$$l = H_{\min}^{\epsilon_s}(A_1^n|E)_{\rho_{\wedge\Omega}} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right). \tag{5.51}$$

Now we make use of the fact that the smooth-min-entropy of the conditioned state is lower bounded by the smooth-min-entropy of the state without conditioning, as proved in Ref. [11, Lemma 10]

$$H_{\min}^{\epsilon_s}(A_1^n|E)_{\rho_{\wedge\Omega}} \geq H_{\min}^{\epsilon_s}(A_1^n|E)_{\rho}. \tag{5.52}$$

In the following we proceed to estimate the quantity

$$H_{\min}^{\epsilon_s}(A_1^n|X_1^n Y_1^n T_1^n E O_{EC})_{\rho}. \tag{5.53}$$

STEP 1: ACCOUNTING FOR THE LEAKAGE IN THE ERROR CORRECTION. Using the chain rule relation for the smooth min-entropy conditioned on classical information, Property 5.5.2*(2)*, we have

$$H_{\min}^{\epsilon_s}(A_1^n|X_1^n Y_1^n T_1^n E O_{EC})_{\rho} \geq H_{\min}^{\epsilon_s}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho} - \text{leak}_{EC}, \tag{5.54}$$

where $\text{leak}_{EC} = \text{rank}(\rho_{O_{EC}})$ represents the minimum amount of classical information that needs to be communicated from Alice to Bob in order to perform error correction[1]. We consider that Alice and Bob use a protocol based on universal hashing which has minimum leakage [121]. In [122] it was proved that the minimum leakage is given by

$$\text{leak}_{EC} \leq H_0^{\epsilon'_{EC}}(A_1^n|B_1^n X_1^n Y_1^n T_1^n) + \log\left(\frac{1}{\epsilon_{EC}}\right), \tag{5.55}$$

where, if Alice and Bob do not abort, then $K_A = K_B$ with probability at least $1 - \epsilon_{EC}$. And for an honest implementation, the error correction protocol aborts with probability at

[1] Note that in a realistic implementation Alice might send the error correction information using an encoding in order to overcome errors in the transmission due to channel losses. Therefore, in general $\rho_{O_{EC}}$ may not be full rank.

most $\epsilon^c_{EC} = \epsilon'_{EC} + \epsilon_{EC}$. Here H_0 is a Rényi entropy first introduced in Ref. [49] (in Ref. [104], it is denoted $\tilde{H}_0^{\uparrow}$). The entropy H_0^{ϵ}, relates to the smooth max-entropy in the following way [103, Lemma 18],

$$H_0^{\epsilon'_{EC}}(A_1^n|B_1^n X_1^n Y_1^n T_1^n) \leq H_{\max}^{\frac{\epsilon'_{EC}}{2}}(A_1^n|B_1^n X_1^n Y_1^n T_1^n) + \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2-\epsilon'_{EC}}\right). \tag{5.56}$$

We now can use of the asymptotic equipartition property, Theorem 5.4.6, to decompose (5.56) into the sum of the entropy of single rounds. Moreover, for an honest implementation with winning CHSH probability ω_{exp} and QBER Q we have that for the test rounds $H(A|BXYT=1) = h(\omega_{exp})$ and for the key generation rounds $H(A|BXYT=0) = h(Q)$. Therefore the one round entropy is given by

$$\begin{aligned} H(A|BXYT) &= p(T=0)H(A|BXYT=0) + p(T=1)H(A|BXYT=1) \\ &= (1-\gamma)h(Q) + \gamma h(\omega_{exp}), \end{aligned} \tag{5.57}$$

where in the first equality we have use Property 5.5.1 *(5)*.

Therefore, the leakage due to error correction is given by

$$\begin{aligned} \text{leak}_{EC} \leq n((1-\gamma)h(Q) + \gamma h(\omega_{exp})) + \sqrt{n}\left(4\log\left(2\sqrt{2}+1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right) \\ + \log\left(\frac{8}{\epsilon'^2_{EC}} + \frac{2}{2-\epsilon'_{EC}}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right). \end{aligned} \tag{5.58}$$

It is not known if an efficient error correction protocol can achieve the minimum leakage estimated in Eq. (5.58), and practical implementations may use protocols with higher leakage. Ref. [123] analyses the leakage in error correction for concrete protocols, based on state-of-the-art error correcting codes, with efficient implementation. A more realistic analysis of the error correction leakage should take into account an specific code.

STEP 2: BREAKING THE ENTROPY INTO SINGLE ROUNDS.

We now can use the asymptotic equipartition property in order to bound $H_{\min}^{\epsilon_s}(A_1^n|X_1^n Y_1^n T_1^n E)_\rho$. The assumption of collective attacks implies that the state under consideration has the tensor product form and therefore

$$H_{\min}^{\epsilon_s}(A_1^n|X_1^n Y_1^n T_1^n E)_\rho \geq n\, H(A|XYTE)_\rho - \sqrt{n}\delta(\epsilon_s,\eta), \tag{5.59}$$

where $\delta(\epsilon_s,\eta)$ and η are specified in Theorem 5.4.6.

For the scenario under consideration we have

$$\eta \leq 2\sqrt{2^{H_{\max}(A|XYTE)_\rho}} + 1 \leq 2\sqrt{2} + 1. \tag{5.60}$$

The first inequality follows from the fact that A is a classical register and therefore has positive conditional min-entropy, which implies $-H_{\min}(A|XYTE)_\rho \leq H_{\min}(A|XYTE)_\rho \leq$

$H_{\max}(A|XYTE)_\rho$. The second inequality follows from the fact that since A is a binary variable $H_{\max}(A|XYTE)_\rho \leq 1$. Therefore,

$$\delta(\epsilon_s,\eta) \leq 4\log\left(2\sqrt{2}+1\right)\sqrt{\log\left(\frac{2}{\epsilon_s^2}\right)}. \tag{5.61}$$

STEP 3: ESTIMATING THE ONE-ROUND ENTROPY.
Now it only remains to lower bound $H(A|XYTE)_\rho$. Lemma 5.4.9 states the tight lower bound for the conditional von-Neumann entropy as a function of the winning probability ω for the CHSH game derived in [16, 41]. Using this bound we have that if ρ is a state that achieves winning probability ω then

$$H(A|XYTE)_\rho \geq 1 - h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16\omega(\omega-1)+3}\right). \tag{5.62}$$

Now, Protocol 5.2.3 aborts if the observed frequency of winning events is smaller than $\omega_{exp}-\delta_{est}$. Therefore, given the event $\hat{\Omega}$ that Protocol 5.2.3 does not abort and $K_A = K_B$, we have that Alice and Bob observe a violation higher than $\omega_{exp}-\delta_{est}$. Now we need to take into account that the CHSH violation is estimated with a finite number of rounds. So in order to infer the real winning probability ω^* of the IID implementation, we can make use of the Hoeffding's inequality in order to define a confidence interval: If $\omega^* < \omega_{exp}-\delta_{est}-\delta_{con}$ then

$$\Pr\left(\omega_{observed} \geq \omega_{exp}-\delta_{est}\right) \leq e^{-2\gamma n(\delta_{con})^2} := \epsilon_{con}. \tag{5.63}$$

Therefore, given that Alice and Bob do not abort the protocol, we infer that the expected winning probability of the system under consideration is higher than $\omega_{exp}-\delta_{est}-\delta_{con}$, and therefore

$$\begin{aligned} &H(A|XYTE)_\rho \geq \\ &1-h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})((\omega_{exp}-\delta_{est}-\delta_{con})-1)+3}\right) \end{aligned} \tag{5.64}$$

Putting the results of these steps together we have that either Protocol 5.2.3 aborts with probability higher than $1-(\epsilon_{con}+\epsilon_{EC})$, or the probability of aborting is smaller than $(\epsilon_{con}+\epsilon_{EC})$ and a $(2\epsilon_{EC}+\epsilon_s+\epsilon_{PA})$-correct-and-secret key can be generated of size

$$\begin{aligned} l \geq n\Big[&1-h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})((\omega_{exp}-\delta_{est}-\delta_{con})-1)+3}\right) \\ &-(1-\gamma)h(Q)-\gamma h(\omega_{exp})\Big] \\ &-\sqrt{n}\left(4\log\left(2\sqrt{2}+1\right)\left(\sqrt{\log\frac{2}{\epsilon_s^2}}+\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right)\right) \\ &-\log\left(\frac{8}{\epsilon'^2_{EC}}+\frac{2}{2-\epsilon'_{EC}}\right)-\log\left(\frac{1}{\epsilon_{EC}}\right)-2\log\left(\frac{1}{2\epsilon_{PA}}\right). \end{aligned} \tag{5.65}$$

This establishes Theorem 5.2.4.

PROOF OF THEOREM 5.2.5

We now present the proof of Theorem 5.2.5, that determines the size of a secret key one can extract from Protocol 5.2.3 for collective attacks, but differently from Theorem 5.2.4, we now use the additivity property of the 2-Rényi entropy, Lemma 5.4.7, in order to break the entropy of the string into the one-round entropy.

We are now interested in estimate the length of a secure key as established in Theorem 5.4.3, which is given by

$$H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E O_{EC})_{\rho_{|\hat{\Omega}}}. \tag{5.66}$$

As in 5.5.2 we now present the steps that lead to the proof of Theorem 5.2.5.

STEP 1: ACCOUNTING FOR THE LEAKAGE IN THE ERROR CORRECTION.

Using Property 5.5.1 *(5)*, we have

$$H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E O_{EC})_{\rho_{|\hat{\Omega}}} \geq H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho_{|\hat{\Omega}}} - \text{leak}_{EC}, \tag{5.67}$$

where $\text{leak}_{EC} = \text{rank}(\rho_{O_{\text{EC}}})$ represents the minimum amount of classical information that needs to be communicated from Alice to Bob in order to perform error correction.

Now the error correction leakage leak_{EC} is the same as derived in Equation (5.58).

STEP 2: BREAKING THE ENTROPY INTO SINGLE ROUNDS.

We first use Property 5.5.1 *(5)* in order to express the entropy of the state conditioned on the event $\hat{\Omega}$ in terms of the entropy of the unconditioned state

$$H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho_{|\hat{\Omega}}} \geq H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho} - 2\log\left(\frac{1}{p_{\hat{\Omega}}}\right). \tag{5.68}$$

We can now make use the additivity property of 2-Réyni entropy, Lemma 5.4.7, in order to bound $H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho}$. The assumption of collective attacks implies that the state under consideration has the tensor product form and therefore

$$H_2^{\uparrow}(A_1^n|X_1^n Y_1^n T_1^n E)_{\rho} \geq n\, H_2(A|XYTE)_{\rho}, \tag{5.69}$$

where now the single round entropy in consideration is the conditional collision entropy.

STEP 3: ESTIMATING THE ONE-ROUND ENTROPY.

Now it only remains to lower bound $H_2(A|XYTE)_{\rho}$. Theorem 5.4.10 shows that a tight lower bound for the conditional collision entropy as a function of the violation S coincides with the previously derived conditional min-entropy[107], eq.(5.31). Therefore, for a state ρ that wins the CHSH game with probability ω

$$H_2(A|XYTE)_{\rho} \geq -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{16\omega(1-\omega)-2}\right). \tag{5.70}$$

Now, either the expected winning probability of the system under consideration is smaller than $\omega_{exp} - \delta_{est} - \delta_{con}$, in which case the protocol aborts with probability higher

than $1-(\epsilon_{con}+\epsilon_{EC})$, or $p_{\hat{\Omega}} > \epsilon_{con}+\epsilon_{EC}$ which implies that the system has winning probability larger than $\omega_{exp}-\delta_{est}-\delta_{con}$, and

$$H_2(A|XYTE)_\rho \geq \tag{5.71}$$
$$-\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})(1-(\omega_{exp}-\delta_{est}-\delta_{con}))-2}\right).$$

In conclusion we have that, either Protocol 5.2.3 aborts with probability higher than $1-(\epsilon_{con}+\epsilon_{EC})$, or the probability of not aborting is greater than $(\epsilon_{con}+\epsilon_{EC})$ and a $(2\epsilon_{EC}+\epsilon_{PA})$-correct-and-secret key is generated of size:

$$\begin{aligned} l \geq n\Big[& -\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{16(\omega_{exp}-\delta_{est}-\delta_{con})(1-(\omega_{exp}-\delta_{est}-\delta_{con}))-2}\right) \\ & -(1-\gamma)h(Q)-\gamma h(\omega_{exp})\Big] \qquad (5.72) \\ & -\sqrt{n}\left(4\log\left(2\sqrt{2}+1\right)\sqrt{\log\frac{8}{\epsilon'^2_{EC}}}\right) \\ & -\log\left(\frac{8}{\epsilon'^2_{EC}}+\frac{2}{2-\epsilon'_{EC}}\right) \qquad (5.73) \\ & -\log\left(\frac{1}{\epsilon_{EC}}\right)-2\log\left(\frac{1}{2\epsilon_{PA}}\right)-2\log\left(\frac{1}{\epsilon_{con}+\epsilon_{EC}}\right). \end{aligned}$$

This establishes Theorem 5.2.5.

PROOF OF THEOREM 5.2.2

In this section we present the proof of Theorem 5.2.2, which establishes the size of a secure key that can be extracted from Protocol 5.2.1 for general coherent attacks. We follow closely the proof developed in [1, 41].

In Protocol 5.2.1, the number of rounds is not fixed. Instead, Protocol 5.2.1 has a fixed number of blocks m, such that the maximum number of rounds inside a block is set to $s_{\max}=\left\lceil\frac{1}{\gamma}\right\rceil$. This is a technicality introduced in [1, 41] in order to get a better prefactor for the overhead terms that scale with $\sqrt{n}$. For each block j Alice and Bob run the protocol until they have a test round or they reach the maximum number of rounds $s_{\max}$. At each round j_i Alice and Bob choose a random bit T_{j_i}, such that $P(T_{j_i}=1)=\gamma$, which determines whether they are going to test the CHSH inequality or make a key generation round. They repeat the process until they obtain $T_{j_i}=1$ or $i=s_{\max}$. With these constraints the expected number of rounds in a block is given by

$$\bar{s}=\frac{1-(1-\gamma)^{\left\lceil\frac{1}{\gamma}\right\rceil}}{\gamma}, \tag{5.74}$$

and the expected number of rounds is

$$n=m\bar{s}. \tag{5.75}$$

For details on the derivation of equations (5.74) and (5.75) see Ref. [41, Appendix B]

We now proceed to derive the key rates against a general coherent attack. In order to calculate the size of the key we need to estimate

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}}. \tag{5.76}$$

Now $\vec{A}_1^m$ denotes the total string of bits, expected to be of size n, and $\vec{A}_i$ denotes the string of outputs generated in the block i, and similarly for the other variables. In the following, we proceed step by step in order to lower bound $H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}}$ and we detail the changes introduced to the original analysis [1, 41].

STEP 1: ACCOUNTING FOR THE LEAKAGE IN THE ERROR CORRECTION. Similar to the proof of Protocol 5.2.3, we have that

$$H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m EO)_{\rho_{|\hat{\Omega}}} \geq H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} - \text{leak}_{EC}, \tag{5.77}$$

and

$$\text{leak}_{EC} \leq H_0^{\epsilon'_{EC}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m) + \log\left(\frac{1}{\epsilon_{EC}}\right) \tag{5.78}$$

$$\leq H_{\max}^{\frac{\epsilon'_{EC}}{2}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m) + \log\left(\frac{8}{{\epsilon'_{EC}}^2} + \frac{2}{(2-\epsilon'_{EC})}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right). \tag{5.79}$$

However, now we need to take into account for the fact that the number of rounds in the protocol is not fixed. Following the steps of Ref. [41], we first note that the number of rounds N obtained in an implementation of the Protocol 5.2.1 satisfies:

$$P[N \geq n+t] \leq \exp\left(-\frac{2t^2\gamma^2}{m(1-\gamma)^2}\right) := \epsilon_t, \tag{5.80}$$

where $n = m\bar{s}$ is the expected number of rounds and $t = \sqrt{-\frac{m(1-\gamma)^2\log\epsilon_t}{2\gamma^2}}$. Moreover, by the definition of smooth max-entropy one have that

$$H_{\max}^{\epsilon}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m N) \leq H_{\max}^{\epsilon-\sqrt{\epsilon_t}}(\vec{A}_1^m|\vec{B}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m N \leq n+t). \tag{5.81}$$

Note that N can be included in the entropy since it is completely determined by $\vec{T}_1^m$.

Now applying the asymptotic equipartition property, Theorem 5.4.6, to the maximal length $N = n+t$ we have

$$\text{leak}_{EC} \leq (\bar{n}+t)\cdot\left[(1-\gamma)h(Q) + \gamma h(\omega_{exp})\right] + \sqrt{\bar{n}+t}\,\nu_2 + \log\left(\frac{8}{{\epsilon'_{EC}}^2} + \frac{2}{(2-\epsilon'_{EC})}\right) + \log\left(\frac{1}{\epsilon_{EC}}\right),$$

where $\nu_2 = 4\log\left(2\sqrt{2}+1\right)\sqrt{2\log\left(\frac{8}{(\epsilon'_{EC}-2\sqrt{\epsilon_t})^2}\right)}$ and ϵ_t is a free parameter to be optimised.

If the error correction protocol does not abort, then

$$P(K_A \neq K_B) \leq \epsilon_{EC}. \tag{5.82}$$

And the completeness of the error correction protocol (*i.e.*, the probability of not aborting in an honest IID implementation) is given by $\epsilon^c_{EC} = \epsilon'_{EC} + \epsilon_{EC}$.

STEP 2: CHAIN RULE.

In Protocol 5.2.1, a statistical test is performed on the variable C_i which accounts for the condition of winning the CHSH game being satisfied or not. In order to use the Entropy Accumulation Theorem, we need to be able to infer the value of this variable C_i from the variables that appear in the smooth min-entropy we are calculating.

Here we choose to use a chain rule, relation (5.44), with the variable C_i itself, as opposed to using the variable B_i as is done in [41]. The reason is that the dimension of the variable C_i is smaller than B_i, as for each block the variable C_i assumes one out of three values. This leads to a slight improvement in rates achieved in the finite regime:

$$\begin{aligned} H_{\min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} &\geq H_{\min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \\ &\quad - H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{A}_1^m\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \qquad (5.83) \\ &\quad - 3\log\left(1-\sqrt{1-\left(\frac{\epsilon_s}{4p(\Omega)}\right)^2}\right) \\ &\geq H_{\min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \\ &\quad - H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \qquad (5.84) \\ &\quad - 3\log\left(1-\sqrt{1-\left(\frac{\epsilon_s}{4(\epsilon_{EA}+\epsilon_{EC})}\right)^2}\right). \end{aligned}$$

In inequality (5.84) we use the fact that $p(\Omega) \geq (\epsilon_{EA}+\epsilon_{EC})$ and that removing the conditioning on classical variables can only increase the entropy, which can be seen as a particular case of data processing, Property 5.5.1 *(1)*.

STEP 3: UPPER BOUND ON $H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$.

We can use the Entropy Accumulation Theorem to upper bound $H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$. In order to do that we only have to find a max-tradeoff function for a protocol with m

rounds. We have that for any distribution $\vec{p} = (p(1), p(0), p(\perp))$ of the variable C:

$$\begin{aligned} H(C_i|\vec{T}_i E)_{\rho_{|\hat{\Omega}}} &= p(\vec{T}_i = \vec{0}) H(C_i|\vec{T}_i = \vec{0}E)_{\rho_{|\hat{\Omega}}} \\ &\quad + p(\vec{T}_i \neq \vec{0}) H(C_i|\vec{T}_i \neq \vec{0}E)_{\rho_{|\hat{\Omega}}} \qquad (5.85) \\ &= p(\vec{T}_i \neq \vec{0}) H(C_i|\vec{T}_i \neq \vec{0}E)_{\rho_{|\hat{\Omega}}} \qquad (5.86) \\ &\leq h\left(\frac{p(1)}{1-p(\perp)}\right) = h\left(\frac{p(1)}{1-(1-\gamma)^{s_{\max}}}\right) = h(\omega), \qquad (5.87) \end{aligned}$$

where in (5.86) we use the fact that $H(C_i|\vec{T}_i = \vec{0}E) = 0$, and in (5.87) we use that $p(\vec{T}_i \neq \vec{0}) \leq 1$ and that $\frac{p(1)}{1-(1-\gamma)^{s_{\max}}} \equiv \omega$. Note that $h(\cdot)$ is a concave function.

Now we can take $f_{\max} = h(\omega_{exp} - \delta_{est})$ and $\|\nabla f_{\max}\|_\infty = \frac{1}{1-(1-\gamma)^{s_{\max}}} \times \frac{\partial h}{\partial \omega}\Big|_{\omega_{exp}-\delta_{est}}$, where ω_{exp} is the expected winning probability of the CHSH game in an honest implementation and δ_{est} accounts for the statistical confidence interval of the experiment. Using the Entropy Accumulation Theorem, Theorem 5.4.8, we have

$$H_{\max}^{\frac{\epsilon_s}{4p(\Omega)}}(C_1^m|\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}} \leq m\, h(\omega_{exp} - \delta_{est}) + \sqrt{m}\, v_1 \qquad (5.88)$$

where

$$v_1 = 2\left(\log 7 + \left\lceil \frac{|h'(\omega_{exp} + \delta_{est})|}{1-(1-\gamma)^{s_{\max}}} \right\rceil\right)\sqrt{1 - 2\log \epsilon_s}, \qquad (5.89)$$

and h' represents the derivative of the binary entropy function, $\frac{\partial h(\omega)}{\partial \omega}$.

STEP 4: LOWER BOUND ON $H_{min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$.

Finally, we apply the Entropy Accumulation Theorem to lower bound the term $H_{min}^{\frac{\epsilon_s}{p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m \vec{Y}_1^m \vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}$. Therefore we need to find a min-tradeoff function such that

$$f_{\min}(\vec{q}) \leq \inf_{\sigma_{R_{j-1}E} : \mathcal{M}_j(\sigma)_{C_j} = \vec{q}} H(\vec{A}_j C_j|\vec{X}_j \vec{Y}_j \vec{T}_j E)_{\mathcal{M}_j(\sigma)} \qquad (5.90)$$

Note that the length of each block is variable. However, we can consider that all the blocks have size $s_{\max}$ and set all the variables to $\perp$ for the rounds which are not performed.

First note that

$$H(\vec{A}_j C_j|\vec{X}_j \vec{Y}_j \vec{T}_j E) \geq H(\vec{A}_j|\vec{X}_j \vec{Y}_j \vec{T}_j E). \qquad (5.91)$$

And from now on, we follow the same steps as Ref. [41].

Using the chain-rule for Von Neuman, Property 5.5.1 *(5)*, entropy we have

$$H(\vec{A}_j|\vec{X}_j \vec{Y}_j \vec{T}_j E) = \sum_{i=1}^{s_{\max}} H(A_{j,i}|\vec{X}_j \vec{Y}_j \vec{T}_j E A_j{}_1^{i-1}). \qquad (5.92)$$

and for every $i \in [s_{\max}]$,

$$\begin{aligned} H(A_{j,i}|\vec{X}_j\vec{Y}_j\vec{T}_jEA_j{}_1^{i-1}) = \\ &= p(T_j{}_1^{i-1}=\vec{0})H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}=\vec{0}) \qquad (5.93)\\ &\quad + p(T_j{}_1^{i-1}\neq\vec{0})H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}\neq\vec{0}) \\ &= (1-\gamma)^{(i-1)}H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}=\vec{0}), \qquad (5.94) \end{aligned}$$

where we used the fact that $H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}\neq\vec{0}) = 0$. Therefore

$$\begin{aligned} H(\vec{A}_j|\vec{X}_j\vec{Y}_j\vec{T}_jE) = \qquad (5.95)\\ \sum_{i=1}^{s_{max}}(1-\gamma)^{(i-1)}H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}=\vec{0}). \end{aligned}$$

Each term $H(A_{j,i}|\vec{X}_j\vec{Y}_jEA_j{}_1^{i-1}T_j{}_i^{s_{\max}}, T_j{}_1^{i-1}=\vec{0})$ can be seen as the entropy of a single round. An expression for the entropy of a single round was derived for collective attacks in [16]. This gives us:

$$\begin{aligned} H(\vec{A}_jC_j|\vec{X}_j\vec{Y}_j\vec{T}_jE) = \qquad (5.96)\\ \sum_{i=1}^{s_{max}}(1-\gamma)^{(i-1)}\left[1-h\left(\frac{1}{2}+\frac{1}{2}\sqrt{16\omega_i(\omega_i-1)+3}\right)\right] \end{aligned}$$

such that

$$p(1) = \sum_{i=1}^{s_{max}}\gamma(1-\gamma)^{(i-1)}\omega_i. \qquad (5.97)$$

Now, in [41] it is proved that the minimum of (5.96) is achieved for

$$\omega_i^* = \frac{p(1)}{1-(1-\gamma)^{s_{\max}}} \quad \forall i, \qquad (5.98)$$

and therefore we have a min-tradeoff function:

$$g(\vec{p}) = s\left[1-h\left(\tfrac{1}{2}+\tfrac{1}{2}\sqrt{16\tfrac{p(1)}{1-(1-\gamma)^{s_{max}}}\left(\tfrac{p(1)}{1-(1-\gamma)^{s_{max}}}-1\right)+3}\right)\right]; \qquad (5.99)$$

for $\frac{p(1)}{1-(1-\gamma)^{s_{max}}} \in \left[\frac{3}{4}, \frac{2+\sqrt{2}}{4}\right]$.

Note that as $p(1) \to ((1-(1-\gamma)^{s_{\max}})\frac{2+\sqrt{2}}{4}$, the gradient of $g(\vec{p})$ tends to infinity, which compromises the $\sqrt{n}$ term that depends on the norm of the gradient of f. Since $g(\vec{p})$ is a convex function, the tangent line in any point $\vec{p}_t$ is a lower bound to $g(\vec{p})$. Therefore, as in [1, 41], we take the min-tradeoff function to be a tangent g in a point $\vec{p}_t$ to be

optimized[1]:

$$F_{\min}(p,p_t)=\frac{d}{dp(1)}g(p)\Big|_{\vec{p}_t}\cdot p(1)+\left(g(p_t)-\frac{d}{dp(1)}g(p)\Big|_{p_t}\cdot p_t(1)\right). \tag{5.100}$$

Then we have

$$H_{min}^{\frac{\epsilon_s}{4p(\Omega)}}(\vec{A}_1^m C_1^m|\vec{X}_1^m\vec{Y}_1^m\vec{T}_1^m E)_{\rho_{|\hat{\Omega}}}>m\cdot\eta_{opt}=\frac{\bar{n}}{\bar{s}}\cdot\eta_{opt}, \tag{5.101}$$

where

$$\eta_{opt}=\max_{\frac{3}{4}<\frac{\tilde{p}_t(1)}{1-(1-\gamma)^{s}max}<\frac{2+\sqrt{2}}{4}}\left[F_{\min}(\tilde{p},\tilde{p}_t)-\frac{1}{\sqrt{m}}\nu_3\right], \tag{5.102}$$

such that

$$\nu_3=2\left(\log\left(1+2\cdot 2^{s_{\max}}3\right)+\left\lceil\frac{d}{dp(1)}g(\tilde{p})\Big|_{p_t}\right\rceil\right)\sqrt{1-2\log\epsilon_s}. \tag{5.103}$$

Finally, the length of a secure key that can be extracted is given by

$$\begin{aligned}l\geq&\frac{\bar{n}}{\bar{s}}\eta_{opt}-\frac{\bar{n}}{\bar{s}}h(\omega_{exp}-\delta_{est})-\sqrt{\frac{\bar{n}}{\bar{s}}}\nu_1\\&-(\bar{n}+t)\cdot\left[(1-\gamma)h(Q)+\gamma h(\omega_{exp})\right]\\&-\sqrt{\bar{n}+t}\,\nu_2-\log\left(\frac{8}{{\epsilon'_{EC}}^2}+\frac{2}{(2-\epsilon'_{EC})}\right)-\log\left(\frac{1}{\epsilon_{EC}}\right)\\&-3\log\left(1-\sqrt{1-\left(\frac{\epsilon_s}{4}\right)^2}\right)-2\log\left(\frac{1}{2\epsilon_{PA}}\right).\end{aligned} \tag{5.104}$$

5.5.3. PROOF OF THEOREM 5.4.10

Theorem 5.4.10. *There exist a state ρ^*_{AB} and measurements for Alice and Bob such that, ρ^*_{AB} achieves violation S and the collision entropy of Alice's output A conditioned on Eve's quantum information E is*

$$H_2(A|E)_{\rho^*}=-\log\left(\frac{1}{2}+\frac{1}{2}\sqrt{2-\frac{S^2}{4}}\right). \tag{5.105}$$

Proof. The proof consists in exhibiting a state ρ^*_{AB} and measurements for Alice and Bob such that the lower bound given by eq.(5.31) is saturated. Our derivation is based on the

[1] In [1, 41] the authors consider the following min-tradeoff function

$$f_{\min}(\vec{p})=\begin{cases}g(\vec{p}) & \text{if } p_t(1)>p(1)\\ F_{\min}(\vec{p},\vec{p}_t)= & \text{if } p_t(1)\leq p(1)\end{cases}.$$

We remark that, since the gradient of $g(\vec{p})$ is an increasing function of $p(1)$, the optimum value for η_{opt} is always achieved for $p_t(1)\leq p(1)$.

techniques presented in Ref. [16], which led to a tight lower bound for the conditional von-Neumann entropy.

Let us consider that Alice and Bob share a Bell diagonal state ρ_{AB}

$$\rho_{AB} = \lambda_{00}\Phi_{00} + \lambda_{01}\Phi_{01} + \lambda_{10}\Phi_{10} + \lambda_{11}\Phi_{11} \tag{5.106}$$

where $\Phi_{ij} = |\Phi_{ij}\rangle\langle\Phi_{ij}|$ and $|\Phi_{ij}\rangle = I \otimes X^i Z^j \left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)$. We first prove the following result:

Lemma 5.5.4. *For a Bell-diagonal state where Alice performs a measurement in the Z-basis we have that*

$$H_2(A|XYE)_\rho \geq -\log\left(\frac{1}{2} + \sqrt{\lambda_{00}\lambda_{01}} + \sqrt{\lambda_{11}\lambda_{10}}\right). \tag{5.107}$$

Proof. Given a Bell diagonal state $\rho_{AB}(\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11})$, a purification $|\Psi\rangle_{ABE}$ of this state is given by

$$\begin{aligned} |\Psi\rangle_{ABE} = &\sqrt{\lambda_{00}}|\Phi_{00}\rangle_{AB}|e_1\rangle_E + \sqrt{\lambda_{01}}|\Phi_{01}\rangle_{AB}|e_2\rangle_E \\ &+ \sqrt{\lambda_{10}}|\Phi_{10}\rangle_{AB}|e_3\rangle_E + \sqrt{\lambda_{11}}|\Phi_{11}\rangle_{AB}|e_4\rangle_E. \end{aligned} \tag{5.108}$$

After Alice measures in the Z basis we have

$$\rho_{AE} = \frac{1}{2}|0\rangle\langle 0| \otimes \rho_{E|0} + \frac{1}{2}|1\rangle\langle 1| \otimes \rho_{E|1} \tag{5.109}$$

where

$$\rho_{E|0} = |\psi_1\rangle\langle\psi_1| + |\psi_2\rangle\langle\psi_2| \text{ and } \rho_{E|1} = |\psi_3\rangle\langle\psi_3| + |\psi_4\rangle\langle\psi_4|, \tag{5.110}$$

with non-normalized states

$$\begin{aligned} |\psi_1\rangle &= \left(\sqrt{\lambda_{00}}|e_1\rangle + \sqrt{\lambda_{01}}|e_2\rangle\right), \\ |\psi_2\rangle &= \left(\sqrt{\lambda_{10}}|e_3\rangle + \sqrt{\lambda_{11}}|e_4\rangle\right), \\ |\psi_3\rangle &= \left(\sqrt{\lambda_{10}}|e_3\rangle - \sqrt{\lambda_{11}}|e_4\rangle\right), \\ |\psi_4\rangle &= \left(\sqrt{\lambda_{00}}|e_1\rangle - \sqrt{\lambda_{01}}|e_2\rangle\right). \end{aligned}$$

The collision entropy of a cq-state ρ_{AE} is given by

$$H_2(A|E)_\rho = -\log \mathrm{tr}\left(\rho_E^{-1/2}\rho_{AE}\rho_E^{-1/2}\rho_{AE}\right), \tag{5.111}$$

which, evaluated for the state (5.109) gives

$$H_2(A|E)_\rho = -\log\left(\frac{1}{2} + \left(\sqrt{\lambda_{00}}\sqrt{\lambda_{01}} + \sqrt{\lambda_{10}}\sqrt{\lambda_{11}}\right)\right).$$

□

Now let us consider a Bell diagonal state ρ^*_{AB} such that

$$\lambda_{00} = R\cos\theta, \quad \lambda_{01} = R\sin\theta, \quad \lambda_{10} = \lambda_{11} = 0, \tag{5.112}$$
$$\text{s.t.} \quad \cos\theta + \sin\theta = \frac{1}{R}$$

which can hold for $R > \frac{1}{\sqrt{2}}$. This choice is inspired by the optimal strategy that maximizes the conditional von Neumann entropy as shown in [16].

For these parameters we have that

$$H_2(A|XYE)_{\rho^*} \geq -\log\left(\frac{1}{2} + R\sqrt{\frac{1}{2}\left(\frac{1}{R^2} - 1\right)}\right) \tag{5.113}$$

Finally, we know from [124] that for a state $\rho_{AB}(\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11})$, the maximal violation $S_{\max}$ of the CHSH inequality is given by

$$S_{\max} = \max\left\{2\sqrt{2}\sqrt{(\lambda_{00} - \lambda_{11})^2 + (\lambda_{01} - \lambda_{10})^2}, \right. \tag{5.114}$$
$$\left. 2\sqrt{2}\sqrt{(\lambda_{00} - \lambda_{10})^2 + (\lambda_{01} - \lambda_{11})^2}\right\}$$

and that this violation can be achieved with one of Alice's measurement being in the Z basis.

Therefore, for the state ρ^*_{AB}, specified by (5.112), and Alice and Bob performing the measurements that gives the maximum violation achievable for the CHSH inequality, we have that $S = 2\sqrt{2}R$. This implies

$$H_2(A|XYE)_{\rho^*} = -\log\left(\frac{1}{2} + \frac{1}{2}\sqrt{2 - \frac{S}{4}}\right). \tag{5.115}$$

□

REFERENCES

[1] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical device-independent quantum cryptography via entropy accumulation,* Nature Communications **9** (2018).

[2] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984) pp. 175 – 179.

[3] A. K. Ekert, *Quantum cryptography based on Bell's theorem,* Phys. Rev. Lett. **67**, 661 (1991).

[4] D. Dieks, *Communication by EPR devices,* Physics Letters A **92**, 271 (1982).

[5] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned,* Nature **299**, 802 (1982).

[6] V. Coffman, J. Kundu, and W. K. Wootters, *Distributed entanglement,* Phys. Rev. A **61**, 052306 (2000).

[7] D. Gottesman and H.-K. Lo, *Proof of security of quantum key distribution with two-way classical communications,* IEEE Transactions on Information Theory **49**, 457 (2003).

[8] H. F. Chau, *Practical scheme to share a secret key through a quantum channel with a* 27.6% *bit error rate,* Phys. Rev. A **66**, 060302 (2002).

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography,* Nature Communications **3** (2012), http://dx.doi.org/10.1038/ncomms1631.

[10] M. Hayashi and T. Tsurumaru, *Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths,* New Journal of Physics **14**, 093014 (2012).

[11] M. Tomamichel and A. Leverrier, *A largely self-contained and complete security proof for quantum key distribution,* Quantum **1**, 14 (2017).

[12] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, *Long-distance quantum key distribution in optical fibre,* New Journal of Physics **8**, 193 (2006).

[13] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Provably secure and practical quantum key distribution over 307 km of optical fibre,* Nature Photonics **9**, 163 (2015).

[14] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, *Satellite-relayed intercontinental quantum network,* Phys. Rev. Lett. **120**, 030501 (2018).

[15] A. Yao and D. Mayers, Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)(FOCS) (1998) p. 503.

[16] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *Device-independent quantum key distribution secure against collective attacks,* New Journal of Physics **11**, 045021 (2009).

[17] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems,* Phys. Rev. A **78**, 042333 (2008).

[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination,* Nature Photonics **4**, 686 (2010).

[19] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, *Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors,* New Journal of Physics **13**, 073024 (2011).

[20] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, *Full-field implementation of a perfect eavesdropper on a quantum cryptography system,* Nature Communications **2**, 349 (2011).

[21] A. Acín, N. Gisin, and L. Masanes, *From Bell's theorem to secure quantum key distribution,* Phys. Rev. Lett. **97**, 120405 (2006).

[22] A. Acín, S. Massar, and S. Pironio, *Efficient quantum key distribution secure against no-signalling eavesdroppers,* New Journal of Physics **8**, 126 (2006).

[23] V. Scarani, N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, *Secrecy extraction from no-signaling correlations,* Phys. Rev. A **74**, 042339 (2006).

[24] L. Masanes, *Universally composable privacy amplification from causality constraints,* Phys. Rev. Lett. **102**, 140501 (2009).

[25] E. Hänggi, R. Renner, and S. Wolf, Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010) pp. 216–234.

[26] S. Pironio, L. Masanes, A. Leverrier, and A. Acín, *Security of device-independent quantum key distribution in the bounded-quantum-storage model,* Phys. Rev. X **3**, 031007 (2013).

[27] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks,* Phys. Rev. Lett. **98**, 230501 (2007).

[28] L. Masanes, S. Pironio, and A. Acin, *Secure device-independent quantum key distribution with causally independent measurement devices,* Nature Communications **2**, 238 (2011).

[29] E. Hänggi and R. Renner, *Device-independent quantum key distribution with commuting measurements,* arXiv:1009.1833 (2010).

[30] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett, *Full security of quantum key distribution from no-signaling constraints,* IEEE Transactions on Information Theory **60**, 4973 (2014).

[31] J. Barrett, R. Colbeck, and A. Kent, *Unconditionally secure device-independent quantum key distribution with only two devices,* Phys. Rev. A **86**, 062326 (2012).

[32] B. W. Reichardt, F. Unger, and U. Vazirani, Proceedings of the 4th Conference on Innovations in Theoretical Computer Science, ITCS '13 (ACM, New York, NY, USA, 2013) pp. 321–322.

[33] U. Vazirani and T. Vidick, *Fully device-independent quantum key distribution,* Phys. Rev. Lett. **113**, 140501 (2014).

[34] C. A. Miller and Y. Shi, *Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices,* J. ACM **63**, 33:1 (2016).

[35] D. Unruh, Advances in Cryptology – CRYPTO 2013 (Springer Berlin Heidelberg, 2013) pp. 380–397.

[36] J. Ribeiro, G. Murta, and S. Wehner, *Fully general device-independence for two-party cryptography and position verification,* arXiv: 1609.08487 (2016), arXiv:1609.08487 [quant-ph] .

[37] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography,* Phys. Rev. Lett. **110**, 010503 (2013).

[38] M. Curty and H.-K. Lo, *Foiling covert channels and malicious classical post-processing units in quantum key distribution,* npj Quantum Information **5**, 14 (2019).

[39] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories,* Phys. Rev. Lett. **23**, 880 (1969).

[40] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, Proceedings. 19th IEEE Annual Conference on Computational Complexity, 2004. (2004) pp. 236–249.

[41] R. Arnon-Friedman, R. Renner, and T. Vidick, *Simple and tight device-independent security proofs,* arXiv: 1607.01797 (2016), arXiv:1607.01797 [quant-ph] .

[42] C. Portmann and R. Renner, *Cryptographic security of quantum key distribution,* arXiv: 1409.3525 (2014), arXiv:1409.3525 [quant-ph] .

[43] D. Mayers, Advances in Cryptology — CRYPTO '96 (Springer Berlin Heidelberg, 1996) pp. 343–357.

[44] D. Mayers, *Unconditional security in quantum cryptography,* J. ACM **48**, 351 (2001).

[45] H.-K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances,* Science **283**, 2050 (1999), http://science.sciencemag.org/content/283/5410/2050.full.pdf .

[46] P. W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,* Phys. Rev. Lett. **85**, 441 (2000).

[47] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries,* Theory of Cryptography, , 407 (2005).

[48] R. König and R. Renner, *A de Finetti representation for finite symmetric quantum states,* Journal of Mathematical Physics **46**, 122108 (2005).

[49] R. Renner, Security of quantum key distribution (Diss., ETH Zürich, Nr. 16242, 2005).

[50] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Bell nonlocality,* Rev. Mod. Phys. **86**, 419 (2014).

[51] M. Christandl, R. König, and R. Renner, *Postselection technique for quantum channels with applications to quantum cryptography,* Phys. Rev. Lett. **102**, 020504 (2009).

[52] F. Dupuis, O. Fawzi, and R. Renner, *Entropy accumulation,* arXiv: 1607.01796 (2016), arXiv:1607.01796 [quant-ph] .

[53] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, *Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres,* Nature **526**, 682 (2015).

[54] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, *Significant-loophole-free test of Bell's theorem with entangled photons,* Phys. Rev. Lett. **115**, 250401 (2015).

[55] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, *Strong loophole-free test of local realism,* Phys. Rev. Lett. **115**, 250402 (2015).

[56] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, *Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes,* Phys. Rev. Lett. **119**, 010402 (2017).

[57] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger, *Bell violation using entangled photons without the fair-sampling assumption,* Nature **497**, 227 (2013).

[58] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, *Detection-loophole-free test of quantum nonlocality, and applications,* Phys. Rev. Lett. **111**, 130406 (2013).

[59] D. N. Matsukevich, P. Maunz, D. L. Moehring, S. Olmschenk, and C. Monroe, *Bell inequality violation with two remote atomic qubits,* Phys. Rev. Lett. **100**, 150404 (2008).

[60] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random numbers certified by Bell's theorem,* Nature **464**, 1021 (2010).

[61] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition property,* IEEE Transactions on Information Theory **55**, 5840 (2009), 0811.1221 .

[62] F. Dupuis and O. Fawzi, *Entropy accumulation with improved second-order,* arXiv:1805.11652 (2018).

[63] J. F. Clauser and M. A. Horne, *Experimental consequences of objective local theories,* Phys. Rev. D **10**, 526 (1974).

[64] P. H. Eberhard, *Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment,* Phys. Rev. A **47**, R747 (1993).

[65] N. Gisin, S. Pironio, and N. Sangouard, *Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier,* Phys. Rev. Lett. **105**, 070501 (2010).

[66] D. Pitkanen, X. Ma, R. Wickert, P. van Loock, and N. Lütkenhaus, *Efficient heralding of photonic qubits with applications to device-independent quantum key distribution,* Phys. Rev. A **84**, 022325 (2011).

[67] M. Curty and T. Moroder, *Heralded-qubit amplifiers for practical device-independent quantum key distribution,* Phys. Rev. A **84**, 010304 (2011).

[68] E. Meyer-Scott, M. Bula, K. Bartkiewicz, A. Černoch, J. Soubusta, T. Jennewein, and K. Lemr, *Entanglement-based linear-optical qubit amplifier,* Phys. Rev. A **88**, 012327 (2013).

[69] K. P. Seshadreesan, M. Takeoka, and M. Sasaki, *Progress towards practical device-independent quantum key distribution with spontaneous parametric down-conversion sources, on-off photodetectors, and entanglement swapping,* Phys. Rev. A **93**, 042328 (2016).

[70] A. Máttar, J. Kołodyński, P. Skrzypczyk, D. Cavalcanti, K. Banaszek, and A. Acín, *Device-independent quantum key distribution with single-photon sources,* arXiv: 1803.07089 (2018).

[71] C. W. Chou, H. De Riedmatten, D. Felinto, S. V. Polyakov, S. J. Van Enk, and H. J. Kimble, *Measurement-induced entanglement for excitation stored in remote atomic ensembles,* Nature **438**, 828 (2005).

[72] I. Usmani, C. Clausen, F. Bussières, N. Sangouard, M. Afzelius, and N. Gisin, *Heralded quantum entanglement between two crystals,* Nature Photonics **6**, 234 (2012).

[73] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, *Entanglement of single-atom quantum bits at a distance.* Nature **449**, 68 (2007).

[74] J. Hofmann, M. Krug, N. Ortegel, L. Gérard, M. Weber, W. Rosenfeld, and H. Weinfurter, *Heralded entanglement between widely separated atoms,* Science **336**, 72 (2012).

[75] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, *Heralded entanglement between solid-state qubits separated by three metres,* Nature **497**, 86 (2013).

[76] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, and S. Faelt, *Generation of heralded entanglement between distant hole spins,* Nat. Phys. **12**, 218 (2016).

[77] R. Riedinger, A. Wallucks, I. Marinkovic, C. Löschnauer, M. Aspelmeyer, S. Hong, and S. Gröblacher, *Remote quantum entanglement between two micromechanical oscillators,* Nature **556**, 473 (2018).

[78] B. Hensen, N. Kalb, M. S. Blok, A. Dréau, A. Reiserer, R. F. L. Vermeulen, M. Markham, D. J. Twitchen, K. Goodenough, D. Elkouss, and S. Wehner, *Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis,* Scientific reports **6**, 30289 (2016).

[79] D. Hucul, I. V. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. M. Clark, and C. Monroe, *Modular entanglement of atomic qubits using photons and phonons,* Nature Physics **11**, 37 (2015).

[80] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, *Entanglement distillation between solid-state quantum network nodes,* Science **356**, 928 (2017), http://science.sciencemag.org/content/356/6341/928.full.pdf .

[81] P. C. Humphreys, N. Kalb, J. P. J. Morits, R. N. Schouten, R. F. L. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network,* Nature **558**, 268 (2018).

[82] A. Reiserer and G. Rempe, *Cavity-based quantum networks with single atoms and optical photons,* Rev. Mod. Phys. **87**, 1379 (2015).

[83] D. D. Awschalom, R. Hanson, J. Wrachtrup, and B. B. Zhou, *Quantum technologies with optically interfaced solid-state spins,* Nat. Photonics **12**, 516 (2018).

[84] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, *Repeated quantum error correction on a continuously encoded qubit by real-time feedback,* Nature communications **7**, 11526 (2016).

[85] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks,* Phys. Rev. A **97**, 062330 (2018).

[86] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics,* Physical Review A **71**, 060310 (2005).

[87] L. Robledo, L. Childress, H. Bernien, B. Hensen, P. F. A. Alkemade, and R. Hanson, *High-fidelity projective read-out of a solid-state spin quantum register,* Nature **477**, 574 (2011).

[88] L. Jiang, J. S. Hodges, J. R. Maze, P. C. Maurer, J. M. Taylor, D. G. Cory, P. R. Hemmer, R. L. Walsworth, A. Yacoby, A. S. Zibrov, and M. D. Lukin, *Repetitive Readout of a Single Electron Spin via Quantum Logic with Nuclear Spin Ancillae,* Science **326**, 267 (2009).

[89] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson, *Unconditional quantum teleportation between distant solid-state quantum bits,* Science **345**, 532 (2014).

[90] N. H. Wan, B. J. Shields, D. Kim, S. Mouradian, B. Lienhard, M. Walsh, H. Bakhru, T. Schröder, and D. Englund, *Efficient Extraction of Light from a Nitrogen-Vacancy Center in a Diamond Parabolic Reflector,* Nano letters **18**, 2787 (2018), 1711.01704 .

[91] A. Faraon, P. E. Barclay, C. Santori, K.-M. C. Fu, and R. G. Beausoleil, *Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity,* Nature Photonics **5**, 301 (2011).

[92] E. T. Campbell and S. C. Benjamin, *Measurement-based entanglement under conditions of extreme photon loss,* Phys. Rev. Lett. **101**, 130502 (2008).

[93] C. Cabrillo, J. I. Cirac, P. García-Fernández, and P. Zoller, *Creation of entangled states of distant atoms by interference,* Phys. Rev. A **59**, 1025 (1999).

[94] M. Bock, P. Eich, S. Kucera, M. Kreis, A. Lenhard, C. Becher, and J. Eschner, *High-fidelity entanglement between a trapped ion and a telecom photon via quantum frequency conversion,* Nature Communications **9** (2018), 10.1038/s41467-018-04341-2.

[95] A. Dréau, A. Tchebotareva, A. E. Mahdaoui, C. Bonato, and R. Hanson, *Quantum frequency conversion of single photons from a nitrogen-vacancy center in diamond to telecommunication wavelengths,* Phys. Rev. Applied **9**, 064031 (2018).

[96] E. Janitz, M. Ruf, M. Dimock, A. Bourassa, J. Sankey, and L. Childress, *Fabry-perot microcavity for diamond-based photonics,* Phys. Rev. A **92**, 043844 (2015).

[97] S. Bogdanović, S. B. Van Dam, C. Bonato, L. C. Coenen, A. M. J. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Lončar, and R. Hanson, *Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks,* Applied Physics Letters **110**, 1 (2017), 1612.02164 .

[98] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and R. J. Warburton, *Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond,* Phys. Rev. X **7**, 031040 (2017).

[99] S. Olmschenk, K. C. Younge, D. L. Moehring, D. N. Matsukevich, P. Maunz, and C. Monroe, *Manipulation and detection of a trapped* Yb^+ *hyperfine qubit,* Phys. Rev. A **76**, 052314 (2007).

[100] F. Henkel, M. Krug, J. Hofmann, W. Rosenfeld, M. Weber, and H. Weinfurter, *Highly efficient state-selective submicrosecond photoionization detection of single atoms,* Phys. Rev. Lett. **105**, 253001 (2010).

[101] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, *On quantum Rényi entropies: A new generalization and some properties,* Journal of Mathematical Physics **54**, 122203 (2013), http://dx.doi.org/10.1063/1.4838856 .

[102] R. Canetti, Proceedings 2001 IEEE International Conference on Cluster Computing (2001) pp. 136–145.

[103] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information,* IEEE Transactions on Information Theory **57**, 5524 (2011).

[104] M. Tomamichel, *Quantum Information Processing with Finite Resources - Mathematical Foundations,* SpringerBriefs in Mathematical Physics book series (BRIEFSMAPHY, volume 5) (2016), theorems and equations references according to arXiv: 1504.00233.

[105] L. Masanes, *Asymptotic violation of Bell inequalities and distillability,* Phys. Rev. Lett. **97**, 050503 (2006).

[106] B. Tsirelson, *Some results and problems on quantum Bell-type inequalities,* Hadronic Journal Supplement **8**, 329 (1993).

[107] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices,* Nature Communications **2**, 238 (2011), arXiv:1009.1567 [quant-ph] .

[108] A. Acín, S. Massar, and S. Pironio, *Randomness versus nonlocality and entanglement,* Phys. Rev. Lett. **108**, 100402 (2012).

[109] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, *Bell inequalities for arbitrarily high-dimensional systems,* Phys. Rev. Lett. **88**, 040404 (2002).

[110] M. Kessler and R. Arnon-Friedman, *Device-independent Randomness Amplification and Privatization,* arXiv: 1705.04148 (2017), arXiv:1705.04148 [quant-ph] .

[111] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin, *Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality,* Phys. Rev. Lett. **113**, 190402 (2014).

[112] J. Ribeiro, G. Murta, and S. Wehner, *Fully device-independent conference key agreement,* Phys. Rev. A **97**, 022307 (2018).

[113] N. D. Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states,* Phys. Rev. Lett. **65**, 1838 (1990).

[114] M. Ardehali, *Bell inequalities with a magnitude of violation that grows exponentially with the number of particles,* Phys. Rev. A **46**, 5375 (1992).

[115] A. V. Belinskiĭ and D. N. Klyshko, *Interference of light and Bell's theorem,* Physics-Uspekhi **36**, 653 (1993).

[116] M. Navascués, S. Pironio, and A. Acín, *Bounding the set of quantum correlations,* Phys. Rev. Lett. **98**, 010401 (2007).

[117] M. Navascués, S. Pironio, and A. Acín, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations,* New Journal of Physics **10**, 073013 (2008).

[118] P. J. Brown, S. Ragy, and R. Colbeck, *An adaptive framework for quantum-secure device-independent randomness expansion,* arXiv:1810.13346 (2018).

[119] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, *Chain rules for smooth min- and max-entropies,* IEEE Transactions on Information Theory **59**, 2603 (2013).

[120] P. Faist, *The entropy zoo,* `https://www.its.caltech.edu/~phfaist/entropyzoo`.

[121] G. Brassard and L. Salvail, Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings, edited by T. Helleseth (Springer Berlin Heidelberg, Berlin, Heidelberg, 1994) pp. 410–423.

[122] R. Renner and S. Wolf, Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings, edited by B. Roy (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 199–216.

[123] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, *Fundamental finite key limits for one-way information reconciliation in quantum key distribution,* Quantum Information Processing **16**, 280 (2017).

[124] R. Horodecki, P. Horodecki, and M. Horodecki, *Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition,* Physics Letters A **200**, 340 (1995).

6

OBLIVIOUS-TRANSFER IS HARDER THAN BIT-COMMITMENT IN REALISTIC MEASUREMENT-DEVICE INDEPENDENT SETTINGS

Jérémy RIBEIRO, Stephanie WEHNER

Among the most studied tasks in Quantum Cryptography one can find Bit Commitment (BC) and Oblivious Transfer (OT), two central cryptographic primitives. In this chapter we propose for the first time protocols for these tasks in the measurement-device independent (MDI) settings and analyze their security. We analyze two different cases: first we assume the parties have access to perfect single photon sources (but still experience noise and losses), and second we assume that they only have imperfect single photon sources. In the first case, we propose a protocol for both BC and OT and prove their security in the Noisy Quantum Storage model. Interestingly, in the case where honest parties do not have access to perfect single photon sources, we find that BC is still possible, but that it is "more difficult" to get a secure protocol for OT: We show that there is a whole class of protocols that cannot be secure. All our security analyzes are done in the finite round regime.

6.1. INTRODUCTION

Following the idea of device-independence we have proven in Chapter 3 security of Bit Commitment (BC) and Oblivious Transfer (OT) in the bounded/noisy quantum storage model in device-independent settings (see also [1]). However it is important to note that, in chapter 3, we assume that, even if the devices may behave in an arbitrary way, they do so in the same fashion in every use of the devices independently of the past. In other words we assume that the devices are memoryless. Other protocols [2, 3] are secure against a more powerful adversary but require different settings where they only achieve an imperfect bit commitment scheme. In general it is quite hard to prove device-independent security of protocols. In particular there is no known security proof for device-independent OT and BC in the settings presented in Refs. [1, 4] without the memoryless assumption. Experimental implementations of device-independent protocols are also a lot more demanding as discussed in Chapter 5 for quantum key distribution. In fact it is so demanding that, while many quantum key distribution and some (quantum) BC protocols have been implemented, there has not been any device-independent implementation of these protocols so far, not even assuming that the devices are memoryless.

These difficulties together with the fact that many physical attacks on the non-device-independent protocols [5, 6] are tampering with the measurement devices and not with the photon sources (or quantum state sources), has led Refs.[7] to introduce a weaker but more practical notion of device-independence called measurement-device-independence (MDI). Here only the measurement devices are treated as black boxes, not the photon sources that are still trusted. Since then many measurement-device-independent protocols have been implemented [8–12]. Typically, in a measurement-device-independent protocol, all the measurement devices are in a "measurement station" in between the parties (see Fig. 6.1). The parties will send BB84 type states to the measurement station which will perform a joint Bell measurement on the incoming qubits. As there is no assumption on the measurement devices located in the measurement station, we will always assume that the dishonest party can control the station (see Fig. 6.2a6.2b). This situation is different from MDI Quantum Key Distribution (QKD), where the dishonest party is always a third party who only controls the measurement station, but never Alice or Bob sources. In particular, in QKD, Alice and Bob can always trust each other, which is not the case for BC or OT.

However, the work on measurement-device-independence is focused on QKD [7–11], and as far as we know there is no proposed protocol for BC or OT in the measurement-device-independent settings. In this work we present protocols for BC and OT and analyze their security. Importantly, all our security proofs hold in the finite rounds regime and can be implemented with current state-of-the-art quantum technologies. We first analyze the situation where the honest parties have perfect single photon sources. Interestingly, in the case where honest parties do not have access to perfect single photon sources, we find that BC is still possible, but that it is "more difficult" to get a secure protocol for OT: We show that there is a whole class of protocols that cannot be secure. We present in the next section a detailed overview of our results.

6.2. RESULTS

In this section, we will present the results of our work. Formal statements and their proofs will be given in the Methods Section.

- We start by presenting the MDI protocols for OT and BC for the case where the honest parties have access to perfect single photon sources.
- Then we present and analyze the security of a protocol for BC where the honest parties only have imperfect single photon sources, *i.e.* multiphoton emissions are possible.
- Finally we show that there is a family of protocols that cannot be secure for OT in MDI settings when the honest parties are using imperfect single photon sources.

6.2.1. BIT COMMITMENT (BC) WITH PERFECT SINGLE PHOTON SOURCES

Before stating our result we briefly and informally remind the reader of the definition of a secure BC protocol. In this chapter we use a variant of bit commitment in which a random string is produced in the commit phase. In the open phase the party can only reveal this string. For more details see Chapter 2.

Definition 6.2.1 (Randomized String Commitment (informal))**.**
A protocol implements an (l,ϵ)*-Randomized String Commitment if it satisfies the following three conditions:*

Correctness *If both Alice and Bob are honest, the protocol outputs a classical state* $\rho_{C_1^l C_1^l F}$ *such that* $\rho_{C_1^l F}$ *is* ϵ*-close to* $\tau_{C_1^l} \otimes |accept\rangle\langle accept|_F$*, where* $\tau_{C_1^l} := \frac{\mathbb{1}}{2^l}$ *is maximally mixed and* C_1^l *is an* l*-bit-string.*

Security for Bob *If Bob is honest there exists a string* C_1^l *after the Commit phase, such that the probability that Alice opens to another string* $C_1^{l'} \neq C_1^l$*, and Bob accepts is smaller than* ϵ*.*

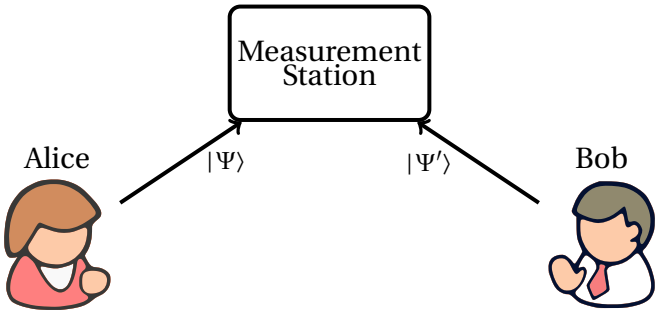
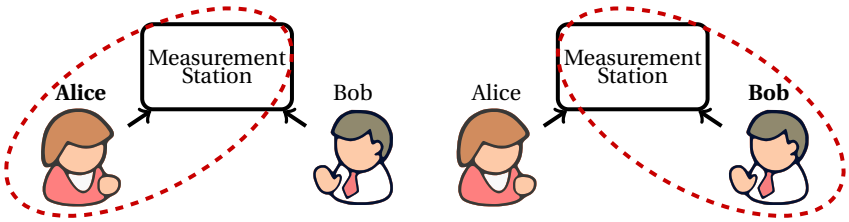


Figure 6.1: Schematic of a MDI protocol.



(a) Schematic of an MDI protocol with dishonest Alice. Alice has control over the measurement station, therefore we will treat Alice and the measurement station as one party.

(b) Schematic of an MDI protocol with dishonest Bob. Bob has control over the measurement station, therefore we will treat Bob and the measurement station as one party.

Figure 6.2: Schematic MDI protocol with dishonest Alice or dishonest Bob.

Security for Alice *If Alice is honest, then after the Commit phase and before the Open phase Bob is "ϵ-ignorant" about the string C_1^l that Alice has received during the Commit phase.*

In this Chapter we show that the protocol below implements a secure String Commitment scheme.

Theorem (Security of Protocol 6.2.2 (Informal))**.** *When honest players have access to perfect single photon sources, and if the dishonest party is assumed to hold a quantum memory that can store a quantum state of at most D qubits, Protocol 6.2.2 implements an $(l, 3\epsilon)-$Randomized String Commitment according to the above definition. In particular it does so using $\Omega\left(\frac{l+2\log(1/2\epsilon)+\ln(\epsilon^{-1})}{\lambda-h(\delta)}\right)$ many rounds of quantum communication, where $\lambda := f(-D/n) - 1/n$ (f is defined in eq. (6.1)), and $\delta = 2e_{\text{err}} + 2\alpha_2$, with e_{err} being the expected error rate between Alice's and Bob's strings (see step 3. of the Open phase of Protocol 6.2.5), n is the number of rounds of the protocol in which the measurement station has clicked, and α_2 is a term that accounts for statistical fluctuations $\alpha_2 = \mathcal{O}(n^{-1/2})$.*

The reader can find a formal version of this theorem in the Methods Section together with its proof, see Theorem 6.4.4. Intuitively – in the MDI settings with perfect single photon sources – the only difference for the security analysis as compare to the analysis of the protocols presented in Refs. [13, 14] is that honest Bob sends information to malicious Alice. However since we are guarantied (by assumption) that Bob sends BB84 states on single photons, we can use a purification argument in order to reduce the MDI situation to the one of Refs. [13, 14] (see Figure 6.5) where only Alice sends information to Bob.

We present below a protocol for Randomized String Commitment adapted from [13] to the measurement-device-independent case. In this protocol Alice and Bob will start with a preparation phase in which they send n states randomly chosen from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to the measurement station which will perform a Bell measurement on these qubits and broadcast the outcome. For the rounds in which Alice and Bob have

used the same basis to encode their states, the Bell measurement outcome tells Bob whether he has encoded the same bit as Alice in his qubit or the opposite bit. If they have used a different basis then the Bell measurement outcome does not give any information on their correlation. In order to force any dishonest party to store quantum information, both parties will wait a certain time Δt before Alice reveals to Bob which bases she has used to prepare her qubits. This allows Bob to compute the set of rounds $\mathscr{I} \subseteq [n]$ where they have used the same bases. Bob will discard the rounds that do not belong to $\mathscr{I}$. From there, they will only use classical communication to extract a random committed string C_1^l in the Commit phase, and to reveal this string in the Open phase.

For the following protocol, we will use a randomly generated $[n,k,d]$-linear code $\mathscr{C} \subseteq \{0,1\}^n$ with fixed rate $R := k/n$ to describe Protocol 6.2.2 and to analyze its security. This does not affect the efficiency of the protocol since the honest parties do not need to decode: We only need to use this code to impose that two strings with the same syndrome have Hamming distance at least d. We denote $\mathrm{Syn} : \{0,1\}^n \mapsto \{0,1\}^{n-k}$ for the function that outputs the parity-check syndrome of the code $\mathscr{C}$. In this protocol we use the two following shorthand notations $\alpha_1 := \sqrt{\frac{\ln \epsilon^{-1}}{2n}}$, $\alpha_2 := \sqrt{\frac{\ln \epsilon^{-1}}{2(1/2-\alpha_1)n}}$. Let $f(\cdot)$ be the function defined as follows.

$$f(x) := \begin{cases} x & \text{if } x \geq 1/2 \\ g^{-1}(x) & \text{if } x < 1/2, \end{cases} \tag{6.1}$$

where $g(x) := h(x) + x - 1$ and $h(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

Protocol 6.2.2 (Randomized String Commitment)**.**
Inputs: *security parameter $\epsilon > 0$, length of the committed string $l > 0$, bound on the size of the adversary's quantum memory D, e_{err} is the expected error rate that should be observed between Alice's an Bob strings $X_{\mathscr{I}}$ and $\hat{X}_{\mathscr{I}}$ (see below).*

Preparation phase

Choose the number n of rounds that click, such that $n \geq \frac{l+2\log(1/2\epsilon)+\ln(\epsilon^{-1})}{\lambda - h(\delta)}$, where $\lambda := f(-D/n) - 1/n$, and $\delta = 2e_{\mathrm{err}} + 2\alpha_2$.

1. *For round i (until the number of rounds in which the measurement station has clicked is higher than n):*
   - *Alice chooses $X_i \in_R \{0,1\}$ and $\Theta_i \in_R \{0,1\}$ uniformly at random, and prepares and sends the state $|X_i\rangle_{\Theta_i}$ (where $|0\rangle_0 := |0\rangle, |1\rangle_0 := |1\rangle, |0\rangle_1 := |+\rangle, |1\rangle_1 := |-\rangle$) to the measurement station.*
   - *Bob chooses $\hat{X}_i \in_R \{0,1\}$ and $\hat{\Theta}_i \in_R \{0,1\}$ uniformly at random and prepares and sends the state $|\hat{X}_i\rangle_{\hat{\Theta}_i}$ (where $|0\rangle_0 := |0\rangle, |1\rangle_0 := |1\rangle, |0\rangle_1 := |+\rangle, |1\rangle_1 := |-\rangle$) to the measurement station.*
   - *The measurement station performs a Bell measurement on the two states it receives, and broadcasts the outcome, or whether the measurement failed. Depending on the outcome, Bob chooses whether he should flip his bit or not.*

2. *Alice and Bob discard all the rounds where a failure has been announced. Let's call n the remaining number of rounds. Alice has strings X_1^n and $\Theta_1^n \in \{0,1\}^n$, and Bob has strings $\hat{X}_1^n$ and $\hat{\Theta}_1^n \in \{0,1\}^n$.*
3. *Both parties wait for a time Δt.*
4. *Alice sends Θ_1^n over to Bob.*
5. *Bob computes the set $\mathscr{I} \subseteq [n]$ of rounds i where $\Theta_i = \hat{\Theta}_i$. Bob discards all the rounds $j \notin \mathscr{I}$. Let's then call $\hat{X}_{\mathscr{I}}$ the string formed by all the remaining bits $\hat{X}_i$ with $i \in \mathscr{I}$.*

   Note that when there is no noise we have that $\forall\, i \in \mathscr{I}\ X_i = \hat{X}_i$. In practice there are always errors: We will call e_{err} the expected error rate between X_i and $\hat{X}_i$ (for $i \in \mathscr{I}$), in other words e_{err} is the expected fraction of error between $X_{\mathscr{I}}$ and $\hat{X}_{\mathscr{I}}$.

Commit Phase

1. *Bob checks whether $m := |\mathscr{I}| \geq 1/2 \cdot n - \alpha_1$. If it is not the case Bob aborts the protocol.*
2. *Alice chooses a random $[n,k,d]$-linear code $\mathscr{C}$ (for fixed n and k) and computes $w = Syn(X_1^n)$ and sends it to Bob.*
3. *Alice picks a random 2-universal hash function $r \in_R \mathscr{R}$ and sends it to Bob.*
4. *Alice outputs $C_1^l := \text{Ext}(X_1^n, r)$ where $\text{Ext}(\cdot,\cdot)$ is a randomness extractor from the 2-universal family of functions.*

Open phase

1. *Alice sends X_1^n to Bob.*
2. *Bob computes its syndrome and checks if it agrees with w he received from Alice in the Commit phase. If they disagree Bob aborts the protocol.*
3. *Bob checks that the number of rounds $i \in \mathscr{I}$ where X_1^n and $\hat{X}_{\mathscr{I}}$ do not agree lies in the interval $]e_{\text{err}} - \alpha_2, e_{\text{err}} + \alpha_2[$. If not, Bob aborts the protocol, otherwise Bob accepts, and he outputs $C_1^l := \text{Ext}(X_1^n, r)$ where $\text{Ext}(\cdot,\cdot)$ is a randomness extractor from the 2-universal family of function.*

In order to satisfy the security definition for Randomized String Commitment, when the protocol aborts, the honest parties will continue the protocol as if they were not aborting – in particular they do not announce the abort event until the end of the protocol – and in the end honest Bob always rejects the commitment and output a uniformly random value to $\tilde{C}_1^l$, and honest Alice outputs a uniformly random value for C_1^l.

6.2.2. OBLIVIOUS TRANSFER (OT) WITH PERFECT SINGLE PHOTON SOURCES

Before stating our result we briefly and informally remind the reader of the definition we use for a secure OT protocol. Here we will use a randomized variantion of OT in which strings are transfered. For more details see Chapter 2.

Definition 6.2.3 (Randomized String Transfer (informal))**.** *A protocol implements an (l,ϵ)-Randomized 1-out-2 Oblivious String Transfer if it satisfies the following three conditions:*

Correctness *If Alice and Bob are honest the protocol's output state $\rho_{(S_0,S_1),(S_C,C)}$ is such that the reduced state $\rho_{S_0,S_1,C}$ is ϵ-close to $\tau_{S_0}\otimes\tau_{S_1}\otimes\tau_C$, where τ_R denotes the maximally mixed state on register R, and S_0, S_1 are two l-bit-strings.*

Security for Alice (hiding) *If Alice is honest, then Alice should get two l-bit-strings S_0 and S_1 such that there exists a binary random variable $\tilde{C}$ such that Bob is "ϵ-ignorant" about the bit string $S_{1-\tilde{C}}$. We say that the protocol is $\epsilon-$hiding.*

Security for Bob (binding) *If Bob is honest then he should receive a random bit C and an l-bit-string $\hat{S}_C$, such that Alice is "ϵ-ignorant" about C. We say that the protocol is $\epsilon-$binding.*

In this work we show that Protocol 6.2.4 presented below implements a secure Randomized Oblivious Transfer.

Theorem (Randomized 1-out-2 OT (Informal))**.** *When honest parties have access to perfect single photon sources, Protocol 6.2.4 implements an (l,ϵ)-Randomized 1-out-2 Oblivious String Transfer according to the above definition in the Bounded Quantum Storage Model. In particular it does so using a linear (in the length l of Alice's strings $|S_0| = |S_1| = l$) number of rounds of quantum communication. More precisely, the number n of quantum communication rounds must satisfy $n \geq 2\,\frac{l+D+1-2\log(1-\sqrt{1-\epsilon^2})}{\lambda-h(e_{\text{err}})-\bar{\mathcal{O}}(n^{-1/2})}$, where e_{err} is the expected error rate between Alice's and Bob's measurement outcome in Protocol 6.2.4, and $\lambda := 1/2-\delta'$ with $\delta' = (2-\log(\sqrt{(32\ln\epsilon^{-1})/n}))\sqrt{(32\ln\epsilon^{-1})/n}$*

The reader can find a formal version of this theorem in the Methods Section together with its proof, see Theorem 6.4.9. Intuitively – in the MDI settings with perfect single photon source – using a purification argument on the states sent by Bob, we can essentially reduce the security proof of our protocol to the security proofs of the trusted device protocol presented in Ref. [13] in which all devices are trusted. However we need to be careful because we also want to take into account noise which has not been done in Ref. [13].

The protocol presented below is also adapted from [13]. For the following Protocol, let $\alpha_1 := \sqrt{\frac{\ln\epsilon^{-1}}{2n}}$ be a term accounting for statistical fluctuations.

Protocol 6.2.4 (Randomized 1-out-2 OT)**.**
Inputs: *security parameter $\epsilon > 0$, the length l of the strings Alice receives, the bound (expressed in qubits) on the adversaries memory D, expected error rate e_{err} between Alice's and Bob's strings $X_{\mathcal{I}}$ and $\hat{X}_{\mathcal{I}}$ defined below.*

Preparation phase *They first choose the number of rounds n in which the station clicks, such that $n \geq 2\frac{l+D+1-2\log(1-\sqrt{1-\epsilon^2})}{\lambda-h(e_{\text{err}})-\mathcal{O}(n^{-1/2})}$. Then Alice and Bob do the same as in the preparation phase of Protocol 6.2.2. At this point Alice has a string X_1^n, and Bob has a string $\hat{X}_{\mathcal{I}}$ and the set $\mathcal{I} \subseteq [n]$.*

Post Processing

1. *Bob checks whether $|\mathcal{I}| \geq (1/2-\alpha_1)n =: m$. If this is the case he randomly truncates $\mathcal{I}$ such that $|\mathcal{I}| = m$. Otherwise he aborts.*
2. *Bob picks a random subset of $\mathcal{I}^c$ of size m called $\mathcal{I}_{\text{Bad}}$. Bob chooses a bit C uniformly at random. He then renames $(\mathcal{I}, \mathcal{I}_{\text{Bad}})$ into (I_C, I_{1-C}). Bob sends (I_0, I_1) to Alice.*
3. *Alice sends Bob error correction information for the strings X_{I_0} and X_{I_1}.*
4. *Bob uses the error correction information O to correct his string $\hat{X}_{\mathcal{I}}$.*
5. *Alice chooses two 2-universal hash functions $r_0, r_1 \in_R \mathcal{R}$ uniformly at random and sends them to Bob.*
6. *Alice outputs $(S_0, S_1) := \big(\text{Ext}(X_{I_0}, r_0), \text{Ext}(X_{I_1}, r_1)\big)$, and Bob outputs $(\hat{S}_C, C) := \big(\text{Ext}(X_{I_C}, r_C), C\big)$.*

In order to satisfy the security definition for OT, when an honest party aborts the protocol, the aborting party will continue the protocol as if they were not aborting – in particular, they do not announce the abort event until the end of the protocol – except that in the end, when the abort event is announced all honest parties assign to their outputs uniformly random values.

6.2.3. BIT COMMITMENT WITH IMPERFECT SINGLE PHOTON SOURCES

In this section we present a protocol that implements String Commitment when the honest parties do not have access to perfect single photon sources (Protocol 6.2.5), and we state the security of this protocol in the Noisy Quantum Storage Model. In this situation, the multiphoton emissions can leak – to dishonest Alice – information about the bases Bob used in his encoding. As a consequence, malicious Alice could take advantage of that by selectively announcing all single photon emissions as "lost", and keep only the rounds where she has information on the bases used by Bob. Malicious Bob can do the same to get some advantage over honest Alice. To prevent this, and make sure that most of the rounds that are kept in the end correspond to single photon emission rounds we will use the decoy states technique [15] similar to [16]. This will allow the honest party to estimate an upper-bound on the number of rounds that are kept in the end and which correspond to multiphoton emissions.

Examples of photon sources are lasers. They produce coherent states that can be

written in the Fock basis as follows:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \tag{6.2}$$

where $|n\rangle$ is the photon number eigenstate associated to photon number n, and $\alpha \in \mathbb{C}$. The intensity is the average number of photons of such a state, and is given by $|\alpha|^2$. As in some MDI QKD experiments [7, 8, 10] one can use a randomized phase coherent state in order to turn the laser into an imperfect single photon source. A randomized phase coherent state is a coherent state where $\alpha = re^{i\phi}$ with $r > 0$ and where ϕ is chosen uniformly at random in $[0, 2\pi[$. To anyone that does not know which phase has been picked, this state is equivalent to the mixed state $\rho_{|\alpha|^2} = \sum_{n=0}^{\infty} e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n|$. When one wants to produce single photons, one can use an attenuated laser that produces states with a low average number of photon, *i.e.* with small $|\alpha|^2$. For example for $|\alpha|^2 = 0.1$, the state $\rho_{|\alpha|^2}$ is essentially a mixture of $|0\rangle\langle 0|$ with probability ≈ 0.905, $|1\rangle\langle 1|$ with probability $p_1 \approx 0.0905$, and multiphoton emissions with probability $p_{\geq 2} \approx 0.0045$, which gives a fraction of $\approx 5\%$ of multiphoton emissions conditioned on emitting at least one photon, which means that the source mostly (95% of non 0 emissions) emits single photons and and emits a small amount of multiphoton states (about 5% of non 0 photon emissions). In a protocol like MDI BC we encode the state in some degree of freedom like polarization. This is a problem for the rounds where multiple photons have been emitted. When only one photon is emitted the possible states Bob can encode are $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and therefore the state sent from Bob to Alice conditioned on a choice of basis, $\theta = 0$ or $\theta = 1$ are $\rho_{|\theta=0} = 1/2(|0\rangle\langle 0| + |1\rangle\langle 1|) = \mathbb{1}/2 = 1/2(|+\rangle\langle +| + |-\rangle\langle -|) = \rho_{|\theta=1}$, meaning that Alice cannot guess which basis Bob has used to encode his state. On the contrary, if for example two photons have been emitted the states are $\rho_{|\theta=0} = 1/2(|00\rangle\langle 00| + |11\rangle\langle 11|) \neq 1/2(|++\rangle\langle ++| + |--\rangle\langle --|) = \rho_{|\theta=1}$ meaning that Alice can guess the basis used with non 0 advantage. This is a problem since security against dishonest Alice rely on her being ignorant about Bob's basis information. In particular we want to avoid the case where dishonest Alice measures the photon number of the incoming state from Bob, and chooses to announce failure only if she receives single photon. This is why we use decoy states: They will allow us to estimate how many single photon rounds have been reported as failure.

For BC in the case where honest parties use imperfect single photon sources, Protocol 6.2.5 can be used. The main difference as compare to Protocol 6.2.2 is the use of q additional decoy states in the "preparation phase". Alice (Bob) can use different intensities[1] for the state she (he) sends. Among these intensities one will correspond to the "signal" state and will be denoted a_s (b_s), while the others will be the "decoy" states with intensities $a \in \{a_{d_1} \dots a_{d_q}\}$ ($b \in \{b_{d_1} \dots b_{d_q}\}$). In Protocol 6.2.5 we will call $n_1^A + n_{\geq 2}^A$ ($n_1^B + n_{\geq 2}^B$) the number of rounds where Alice (Bob) has used a "signal" state – *i.e.* a state with intensity a_s (b_s) – and where the measurement station reported the measurement as successful. n_1^A (n_1^B) is the number of these states where Alice (Bob) has sent 1 photon, and $n_{\geq 2}^A$ ($n_{\geq 2}^B$)

[1] We remind the reader that intensities correspond to the mean number of photons produced by the source. For a (randomized phase) coherent state the intensity is given by $|\alpha|^2$. In many practical cases the intensity of the source can be chosen.

is the number of these rounds where Alice (Bob) has sent ≥ 2 photons. Note that at the end of Step 1 of the "preparation phase", and because we do not consider dark counts in this chapter, Alice (Bob) knows the value of $n_1^A + n_{\geq 2}^A$ ($n_1^B + n_{\geq 2}^B$). However even if she (he) knows the sum $n_1^A + n_{\geq 2}^A$ ($n_1^B + n_{\geq 2}^B$), she (he) does not know the individual terms n_1^A (n_1^A) and $n_{\geq 2}^A$ ($n_{\geq 2}^B$) of this sum. Alice (Bob) will only be able to estimate a lower-bound L_{A1} (L_{B1}) on n_1^A (n_1^B) by using the decoy states. Since $n_1^A + n_{\geq 2}^A$ ($n_1^B + n_{\geq 2}^B$) is known to Alice (Bob), this lower-bound gives automatically an upper-bound $U_{A2} = n_1^A + n_{\geq 2}^A - L_{A1}$ ($U_{B2} = n_1^B + n_{\geq 2}^B - L_{B1}$) on $n_{\geq 2}^A$ ($n_{\geq 2}^B$).

In the following we will write p_a (p_b) for the probability that Alice (Bob) prepares a signal of intensity $a \in \{a_s, a_{d_1} \dots a_{d_q}\}$ ($b \in \{b_{a_s}, b_{d_1} \dots b_{d_q}\}$). When the identity of the emitter is not determined, the intensity will be denoted i (meaning that $i = a$ is the emitter is Alice or $i = b$ is the emitter is Bob). The probability that an emitter emits k photons will be denoted p_k (e.g. if $k = 1$ then we will write p_1 etc.). The probability that the emitter emits more than k photons will be denoted $p_{\geq k}$ (e.g. $p_{\geq 2}$). We will also mix the two above notations when talking about conditional events. For example, the probability that Alice emits 2 photons conditioned on choosing signal intensity a will be denoted $p_{2|a}$.

In this chapter we show that Protocol 6.2.5 below is secure, in particular we show the following.

6

Theorem (Multiphoton emission round number estimation (Informal))**.** *Using q possible intensities for the decoy states, it is possible for the honest party $H \in \{Alice, Bob\}$ to estimate a lower-bound L_{H1} on the number of rounds – among the ones that are not discarded at the end of the preparation phase – in which his source has emitted a single photon. We give an analytical expression for L_{H_1} when $q = 2$ in the formal version of theorem: Theorem 6.4.13. Equivalently the honest party can estimate an upperbound U_{H2} on the number of rounds – among the ones that are not discarded at the end of the preparation phase – in which his source has emitted multiple photons.*

A formal statement can be found in the Methods Section: Theorem 6.4.13. Its proof is given in Technical Details Section 6.5.2. The above theorem is an essential ingredient to prove the following security theorem.

Theorem (Security of Protocol 6.2.5 (Informal))**.** *If the adversary holds a quantum memory that cannot store more than D qubits, Protocol 6.2.5 implements an $(l, \epsilon)-$Randomized 1-out-2 Oblivious String Transfer as defined in Definition 6.2.1. In particular it does so using a number N of quantum communication rounds that is linear in the length l of the strings S_0 and S_1. More precisely N must satisfy $(p - \sqrt{\ln(\epsilon^{-1})/2N})\, N \geq n^\star$ where $n^\star$ is smallest integer solution to $n \geq \frac{l + 2\log(1/2\epsilon) + \ln(\epsilon^{-1})}{\lambda - h(\delta)}$, where p is the probability that any given round $i \in [N]$ is not discarded in the preparation phase when both parties are honest, $\lambda := f(-D/n) - (\gamma + \alpha_4^A) - 1/n$ with n being the length of honest Alice's string X_1^n produced at the end of the "preparation phase", and δ is a function of the expected error rate e_{err} between Alice's and Bob's measurement outcome of the "preparation phase". The exact expression of δ is given in the formal version of this theorem: Theorem 6.4.12.*

A formal version of this theorem together with its proof are given in the Methods Section: Theorem 6.4.12.

In Protocol 6.2.5 and its security analysis we will use the following notations: $\epsilon \in]0,1[$, and $f_{a_s}, f_{b_s} \in [0,1]$ are fractions defined in Step 2 of Protocol 6.2.5. α_1, α_2 are the same as in Section 6.2.1. As for α_1, α_2 the terms $\beta^A, \beta^B, \alpha_4^A, \alpha_4^B$ account for statistical fluctuation. They all are $\mathcal{O}(1/\sqrt{N})$ where N is the number of rounds of the protocol. Their exact expressions are given in Theorem 6.4.12. As in Protocol 6.2.2 $\mathscr{C}$ is an random $[n,k,d]$-linear code and $\mathrm{Syn} : \{0,1\}^n \mapsto \{0,1\}^{n-k}$ is the function that outputs the parity-check syndrome of code $\mathscr{C}$.

In order to satisfy the security definition for Randomized String Commitment (Def. 6.2.1), when the protocol aborts, the honest parties will continue the protocol as if they were not aborting – in particular they do not announce the abort event until the end of the protocol – and in the end honest Bob always rejects the commitment and assigns a uniformly random value to his output $\tilde{C}_1^l$, and honest Alice assigns a uniformly random value to her output C_1^l.

Protocol 6.2.5 (Randomized String Commitment with decoy states)**.**
Inputs: *The security parameter $\epsilon > 0$, the parameter $\gamma \in [0, 1/2]$ that essentially measures how good the single photon sources are, the length l of the string that will be produced by the protocol, the maximum size (expressed in qubits) of the adversary's quantum memory D, the expected error rate e_{err} between Alice's and Bob's string $X_{\mathscr{I}}$ and $\hat{X}_{\mathscr{I}}$, the probability distributions $(p_{a_s}, p_{a_{d_1}}, \ldots, p_{a_{d_q}})$ and $(p_{b_s}, p_{b_1}, \ldots, p_{b_q})$ that Alice and Bob use intensities $\{a_s, a_{d_1}, \ldots, a_{d_q}\}$ and $\{b_s, b_{d_1}, \ldots, b_{d_q}\}$ respectively.*

Preparation phase

Alice and Bob agree on a number N of rounds. N must satisfy $(p - \sqrt{\ln(\epsilon^{-1})/2N})\, N \geq n^*$, where n^* the smallest positive integer solution to the inequality eq. (6.26), and where p is the probability that any given round $i \in [N]$ is not discarded in the preparation phase when both parties are honest.

1. *For round $i \in [N]$:*
   - *Alice chooses $X_i \in_R \{0,1\}$ and $\Theta_i \in_R \{0,1\}$ uniformly at random, and chooses intensity $a \in \{a_s, a_{d_1} \ldots a_{d_q}\}$ with some probability distribution p_a. Alice prepares a quantum signal of intensity a, encoding X_i in the basis Θ_i, and sends it over to the measurement station.*
   - *Bob chooses $\hat{X}_i \in_R \{0,1\}$ and $\hat{\Theta}_i \in_R \{0,1\}$ uniformly at random, and chooses intensity $b \in \{b_s, b_{d_1} \ldots b_{d_q}\}$ with some probability distribution p_b. Bob prepares a quantum signal of intensity b, encoding $\hat{X}_i$ in the basis $\hat{\Theta}_i$, and sends it over to the measurement station.*
   - *The measurement station performs a Bell measurement on the two states it receives, and publicly reveals the outcome, or whether the measurement failed.*
2. *Alice and Bob publicly announce the intensities they have used for all the rounds $i \in [N]$ (the order in which this is announced is not important). Alice checks that among the rounds where she has used intensity a_s and the*

6

measurement succeeded, the fraction f_{b_s} of rounds where Bob has used intensity b_s is higher than $p_{b_s} - \beta^A$. Bob checks that among the rounds where he has used intensity b_s and the measurement succeeded, the fraction f_{a_s} of rounds where Alice has used intensity a_s is higher than $p_{a_s} - \beta^B$. If this is not the case, Alice or Bob abort the protocol.

3. *Using the decoy states Alice estimates a lower-bound L_{A1} for n_1^A (this is given by Lemma 6.4.13), the number of rounds where the Bell measurement has not been announced as a failure and where Alice emitted 1 photon with intensity a_s. If $\frac{U_{A2}}{f_{b_s}(n_1^A + n_{\geq 2}^A)} \geq \gamma + \alpha_4^A$ Alice aborts the protocol.*
4. *Using the decoy states Bob estimates a lower-bound for n_1^B (this is given by Lemma 6.4.13), the number of rounds where the Bell measurement has not been announced as a failure and where Bob emitted 1 photon with intensity b_s. If $\frac{U_{B2}}{f_{a_s}(n_1^B + n_{\geq 2}^B)} \geq \gamma + \alpha_4^B$ Bob aborts the protocol.*
5. *Alice and Bob discard all the rounds where a failure has been announced, and where the intensities used by Alice and Bob are not a_s and b_s. Let's call the remaining number of rounds n. Alice has strings X_1^n and $\Theta_1^n \in \{0,1\}^n$, and Bob has strings $\hat{X}_1^n$ and $\hat{\Theta}_1^n \in \{0,1\}^n$. Note that $n = f_{b_s} \times (n_1^A + n_{\geq 2}^A) = f_{a_s} \times (n_1^B + n_{\geq 2}^B)$. Alice and Bob check that $n \geq \frac{l + 2\log(1/2\epsilon) + \ln(\epsilon^{-1})}{\lambda - h(\delta)}$, and otherwise abort the protocol.*
6. *Both parties wait for a time Δt.*
7. *Alice sends Θ_1^n over to Bob.*
8. *Bob computes the set $\mathscr{I} \subseteq [n]$ of rounds i where $\Theta_i = \hat{\Theta}_i$. Bob discards all the rounds $j \notin \mathscr{I}$. Let's then call $\hat{X}_{\mathscr{I}}$ the string formed by all the remaining bits $\hat{X}_i$ with $i \in \mathscr{I}$.*

   Note that when there is no noise we have that $\forall i \in \mathscr{I}\ X_i = \hat{X}_i$. In practice there are always errors: We will call e_{err} the expected errors rate between X_i and $\hat{X}_i$ (for $i \in \mathscr{I}$).

Commit Phase

1. *Bob checks whether $m := |\mathscr{I}| \in [1/2 \cdot n - \alpha_1, 1/2 \cdot n + \alpha_1]$. If this is not the case Bob aborts.*
2. *Alice chooses a random $[n,k,d]$-linear code $\mathscr{C}$ (for fixed n and k) and computes $w = Syn(X_1^n)$ and sends it to Bob.*
3. *Alice picks a random 2-universal hash function $r \in_R \mathscr{R}$ and sends it to Bob.*
4. *Alice outputs $C_1^l := \text{Ext}(X_1^n, r)$ where $\text{Ext}(\cdot,\cdot)$ is a randomness extractor from the 2-universal family of function.*

Open phase

1. *Alice sends X_1^n to Bob.*
2. *Bob computes its syndrome and checks if it agrees with w he received from Alice in the Commit phase. If they disagree Bob aborts.*
3. *Bob checks that the number of rounds $i \in \mathscr{I}$ where X_1^n and $\hat{X}_{\mathscr{I}}$ do not agree lies in the interval $]e_{\text{err}} - \alpha_2, e_{\text{err}} + \alpha_2[$. If not, Bob aborts the protocol, otherwise he outputs $C_1^l := \text{Ext}(X_1^n, r)$ where $\text{Ext}(\cdot,\cdot)$ is a randomness extractor from the 2-universal family of function.*

We require that $(p - \sqrt{\ln(\epsilon^{-1})/2N})\, N \geq n^\star$, for $n^\star$ statisfaying $n \geq \frac{l+2\log(1/2\epsilon)+\ln(\epsilon^{-1})}{\lambda - h(\delta)}$ only to make sure there are enough rounds to produce $l-$bits final strings in a secure way. p is the probability that a round is not discarded in the honest scenario, and it can be expressed a function of the experimental parameters: The round won't be discarded if both players sent a signal state for this round, which happens with probability $p_{a_s} \times p_{b_s}$, and if the measurement station did not reported this round as failure which happens with probability $1 - p_{\text{fail}|a_s b_s}$, so $p = p_{a_s} \times p_{b_s} \times (1 - p_{\text{fail}|a_s b_s})$.

6.2.4. OT WITH AN IMPERFECT SINGLE PHOTON SOURCES

In this section we will prove that MDI Oblivious Transfer is "not easy" in practical settings. Indeed in practice photon sources are not perfect *i.e.* they have some probability $p_{\geq 2}$ to emit more than one photon. If now one considers a protocol containing a preparation phase similar to the one of Protocol 6.2.4, but where now Bob has an imperfect single photon source, it becomes possible for a malicious Alice to deduce from the states she receives from Bob, some of the bases Θ_i that have been used in Bob's encoding. As we will explain below this is due to the fact that when more than one photon are emitted by Bob's source, a dishonest Alice can distinguish states encoded in the standard and the Hadamard basis, which is not possible to do when a single photon is emitted. This is a leakage of information that has heavy consequences on the feasibility of an OT protocol as explained below.

We will illustrate how this leakage of information can break security of a protocol, by describing what happens to Protocol 6.2.4 when Alice is malicious and Bob holds an imperfect single photon source. After this we will generalize the reasoning.

Dishonest Alice's end goal is to guess correctly the value of bit C that Bob will get at the end of the protocol. Moreover, Alice being malicious implies that Alice has full control over the measurement station, and therefore everything Bob sends to the measurement station can be considered in Alice's possession. Let us now start with the preparation phase of Protocol 6.2.4. In this phase of the protocol, Bob sends BB84 states[2] to the measurement station, or equivalently to dishonest Alice. But contrary to section 6.2.2 Bob now holds an imperfect single photon source. This means that in some of the rounds, more than one photon are sent to Alice. This becomes a problem because if, for

[2] $|X_i\rangle_{\Theta_i}$ which correspond to encoding in the basis $\hat{\Theta}_i$, where $\hat{\Theta}_i = 0$ corresponds to the standard basis and $\hat{\Theta}_i = 1$ corresponds to the Hadamard basis

example, the source has emitted two photons, then the state Alice receives conditioned on Bob preparing it in the standard basis is $1/2(|00\rangle\langle 00| + |11\rangle\langle 11|)$, while if we condition the state on being prepared in the Hadammard basis it is $1/2(|++\rangle\langle ++| + |--\rangle\langle --|)$. These two states are not the equal, and therefore Alice can use these states to guess the basis Θ_i that Bob has used to encode the state. When a single photon is used this is not a problem since $1/2(|0\rangle\langle 0| + |1\rangle\langle 1|) = \mathbb{1}/2 = 1/2(|+\rangle\langle +| + |-\rangle\langle -|)$: the two cases – Bob prepares the state in the standard or the Hadamard basis – are perfectly indistinguishable. Moreover, the more photons are emitted by the source, the easier it is for Alice to guess correctly which basis Bob has used. To be conservative, for each round in which multiple photons have been emitted we will consider that malicious Alice knows exactly Bob's choice of basis $\hat{\Theta}_i$.

At the end of the preparation phase malicious Alice sends a string Θ_1^n[3] to Bob. Bob uses the string Θ_1^n he received from Alice and his own choice of bases described by the string $\hat{\Theta}_1^n$ to compute the set $\mathscr{I} := \{i \in [n] : \Theta_i = \hat{\Theta}_i\}$, which is the set of rounds in which Bob's choice of bases matches the value of the bit malicious Alice has sent to him, and where n denotes the total number of rounds. He also erases all the bits $\hat{X}_i$ he has used to encode the states he has sent to the station for all i such that $i \notin \mathscr{I}$. At this point Bob holds the set $\mathscr{I}$ and the string $\hat{X}_{\mathscr{I}}$ which is formed by all the bits $\hat{X}_i$ he has used in the round $i \in \mathscr{I}$. Remember that Malicious Alice knows the value of $\hat{\Theta}_i$ in some of the rounds, and therefore knows whether these rounds correspond to rounds in $\mathscr{I}$ or not. We call I_G the set of rounds for which Alice knows that they are in $\mathscr{I}$ and I_B the set of rounds for which she knows that they are not in $\mathscr{I}$. The choice bit C that has to be created by the protocol is chosen uniformly at random by Bob. He then uses this bit C to rename the sets $(\mathscr{I}, \mathscr{I}^c)$ – where $\mathscr{I}^c$ denotes the complement of $\mathscr{I}$ – into (I_C, I_{1-C}), where C takes value in $\{0,1\}$. In other words, if Bob chooses $C = 0$ then $(\mathscr{I}, \mathscr{I}^c)$ is renamed into (I_0, I_1), and if he chooses $C = 1$, $(\mathscr{I}, \mathscr{I}^c)$ is renamed into (I_1, I_0).

After the preparation phase, Bob sends (I_0, I_1) to (malicious) Alice. Revealing these two sets to Alice does not reveal in itself the value of bit C. However, there has been a leakage of information in the preparation phase, and from this leakage Alice knows the set I_G and I_B defined above, she can compare this two sets I_G and I_B with the sets I_0 and I_1 she has received from Bob. But by definition of I_G we must have $I_G \subset \mathscr{I} = I_C$ and $I_G \cap \mathscr{I}^c = \emptyset$. Therefore she can get the value of C: if $I_G \subset I_0$ then $C = 0$, and if $I_G \subset I_1$ then $C = 1$. Therefore Protocol 6.2.4 is not secure if Bob holds an imperfect single photon source.

In the following we will generalize the settings to show that the argument presented above holds for more general protocols than Protocol 6.2.4. To do so we will abstract the structure of the protocol, as well as the meaning of the registers (e.g. the registers I_G and I_B)we use in the attack. The notation will stay very similar to what we have presented above, and the main intuition behind the attack remains the same. Our impossibility result holds for any protocol satisfying Assumption 6.2.6.

The statement we will make is expressed in in terms of asymptotic security, *i.e.* we will say that Alice can cheat if she has a non-negligible advantage in guessing Bob's bit C

[3] The way Alice chooses the value for Θ_1^n has no importance, and we will therefore consider Θ_1^n as a fully random string in this argument.

(see Theorem 6.4.20 below). A function is said to be "negligible" (in some variable n) if it is smaller than $1/n^a$ (for any $a > 0$ and for n large enough). Similarly we will say that a probability p is overwhelming if $1 - p$ is negligible.

In order to generalize the attack on Protocol 6.2.4 we have seen above, we work in a model (see Fig. 6.3) where Alice and Bob have already run a quantum phase of a protocol, that has given registers X_1^n to honest Alice and $X_{\mathscr{I}}, \mathscr{I}$ to Bob. X_1^n is a bit string and $X_{\mathscr{I}}$ is a substring of X_1^n whose bits are the ones corresponding the set of indices $\mathscr{I} \subseteq [n]$. One can typically think of a "quantum phase" as being the preparation phase of Protocols 6.2.4 & 6.2.5 for example.

If Alice is dishonest we assume that she has recorded – during this quantum phase – information leaked by the imperfection of Bob's source. We model this leakage of information by giving dishonest Alice two extra registers (I_G, I_B) that correspond to two sets of indices correlated with $\mathscr{I}$. When Bob is dishonest we simply assume that he holds the cq-registers KQ such that his min-entropy on Alice's string X_1^n is smaller than honest Bob's one. Since we work in the bounded storage model we assume $\log \dim Q \leq D$.

After this quantum phase of the protocol, we assume that Alice and Bob run a classical post-processing. One such post-processing is the post-processing of Protocol 6.2.4. When a party is dishonest we assume he will in fact be semi-honest during the post processing, meaning that he will run the post-processing honestly but record all the information he has received or sent. We prove that if such a protocol is correct and secure against dishonest Bob, then Protocol 6.2.7 gives dishonest Alice a (semi-honest) strategy to use her extra input registers (I_G, I_B) she got from the quantum phase and all the communication she recorded during the post-processing in order to guess honest Bob's output bit C with non-negligible advantage.

We will describe the set of messages going from Bob to Alice by the random variable M_{BA}. The messages from Alice to Bob will be described by the random variable M_{AB}. The random variable composed of these two variables will be called M. In other words $M := (M_{AB}, M_{BA})$.

The output of honest Alice is $(S_0, S_1) := (f_0(X_1^n, M), f_1(X_1^n, M)) \in \{0,1\} \times \{0,1\}$, where f_0 and f_1 are two functions determined by the protocol. Tipically, these functions are the composition of error correction with a randomness extractor. The output of honest Bob is $(C, S_C) := (g(X_{\mathscr{I}}, \mathscr{I}, M), \tilde{g}(X_{\mathscr{I}}, \mathscr{I}, M))$, where g and $\tilde{g}$ are two other functions determined be the protocol. These four functions model the operations that honest Alice and Bob have to perform according to the protocol they are running.

We construct an attack where Alice is semi-honest (or equivalently "honest but curious"), that is, she will execute the post-processing part of the protocol honestly but keep all the information that she has exchanged with Bob so that she can in the end compute whatever she is interested in, which in this case is C. Our result holds under two assumptions stated below. This restricts the applicability of our theorem. However, we argue in the Discussion Section that these assumptions should still be sufficiently general for any practical purpose.

Assumptions 6.2.6 (Informal)**.** *In order to prove the theorem below we need two assumptions.*

1. *The messages sent between Alice and Bob during the post-processing contain infor-*

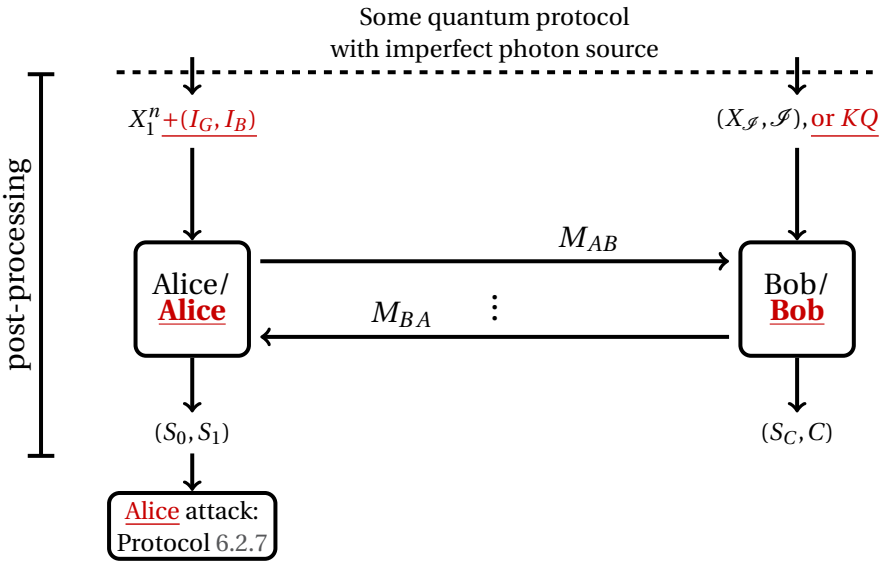


Figure 6.3: Schematic view of the classical post-processing between (dishonest) Alice and (dishonest) Bob. Before the post-processing Alice and Bob have run an unspecified quantum protocol which gave them their inputs: X_1^n +(I_G, I_B) for (dishonest) Alice, and $(X_{\mathscr{I}}, \mathscr{I})$, or KQ for (dishonest) Bob.
When Alice is dishonest, we will consider that she is "honest but curious" at the post-processing level, meaning that Alice will run the post-processing honestly with Bob, but she will record all communication M_{AB}, M_{BA} and use them at the end together with her extra-input (I_G, I_B), to extract more information than what she should get out of the protocol. To do so she will use the strategy described in Protocol 6.2.7

mation about the pair of sets set (I_0, I_1)[4] *of bits of* X_1^n *on which function* f_0 *and* f_1 *depend, but without revealing the value of Bob's bit* C*. Alice can compute these sets thanks to a function* F*.*

2. *There is a non-negligible probability that,*

$$\begin{cases} \text{the intersection between the set } I_G \cup I_B \text{ and } I_0 \setminus I_1 \text{ is not empty} \\ \text{and} \\ \text{the intersection between the set } I_G \cup I_B \text{ and } I_1 \setminus I_0 \text{ is not empty.} \end{cases}$$

If we define κ *being the minimum length of the two intersections above, we can rephrase this condition by saying that, there is a non-negligible probability that* $\kappa \geq 1$*.*

The sets I_G, I_B *are the sets dishonest Alice gets from the leakage of the quantum part of the protocol. The sets* I_0, I_1 *are the sets correlated to set* $\mathscr{I}$ *and bit* C *that do not reveal value of bit* C *as long as* $\mathscr{I}$ *is completely unknown from Alice. Of course since dishonest Alice has extra information* I_G, I_B *correlated to* $\mathscr{I}$*, Alice is not ignorant about* $\mathscr{I}$*: She therefore*

[4] Remember that in Protocol 6.2.4 sets (I_0, I_1) correspond to the renaming of the sets $(\mathscr{I}, \mathscr{I}^c)$ that bob sends to Alice

has some information about the bit C, which as we will see allows her to cheat. The reader can find a more formal version of these assumptions in the Methods Section: Assumption 6.4.19.

Theorem (Dishonest Alice cheating (Informal))**.** *If a quantum protocol between Alice and Bob that implements OT is such that it leaks some information* (I_G, I_B) *to dishonest Alice in the quantum phase (before the classical post-processing), and if this protocol is correct and secure against dishonest Bob, then there exists a strategy for dishonest Alice that allows her to cheat, i.e. she can guess Bob's bit C with non-negligible advantage. This strategy runs as follows: Dishonest Alice runs honestly the post processing phase with Bob, but records all messages sent and received during this post-processing. At the end of the post-processing she will use all this messages together with her extra information* (I_G, I_B) *in order to locally run the procedure described in Protocol 6.2.7. This procedure outputs her guess for Bob's bit C.*

The reader can find a formal version of this theorem in the Methods Section, together with its proof: Theorem 6.4.20.

We recall that when Alice is dishonest she holds some extra set I_G (and I_B), which in a protocol like Protocol 6.2.4 would typically correspond to the multiphoton rounds where dishonest Alice has inferred that Bob has used the same basis as she did (or a different basis for I_B). So at the end of the post-processing she will execute the strategy detailed in Protocol 6.2.7, where she starts by computing the two sets I_0 and I_1. She will then choose uniformly at random – thanks to random bit r – whether she later wants to sample at random an index in $\mathscr{S}_0 := I_0 \setminus I_1 \cap (I_G \cup I_B)$ or in $\mathscr{S}_1 := I_1 \setminus I_0 \cap (I_G \cup I_B)$. At this point Alice samples uniformly at random an index in $\mathscr{S}_r$, and checks whether this round is in I_G or in I_B. If it is in I_G then Alice's guess for Bob's bit C will be r, and otherwise she guesses $1-r$. More formally Alice proceeds as follows.

Protocol 6.2.7 (Dishonest Alice's strategy)**.**
Inputs: x_1^n, m, I_G, I_B.
Outputs: b.

- *Alice computes* $(I_0, I_1) = F(x_1^n, m)$.
- *Alice checks that* $I_0 \setminus I_1 \cap (I_G \cup I_B) \neq \emptyset$ *and* $I_1 \setminus I_0 \cap (I_G \cup I_B) \neq \emptyset$. *If this is not the case Alice outputs* $b \in_R \{0,1\}$ *uniformly at random, otherwise she continues with the protocol.*
- *Alice sample a bit* r *uniformly at random.*
- *Alice chooses an index* $i_r \in I_r \setminus I_{1-r} \cap (I_G \cup I_B)$ *uniformly at random.*
- *Alice checks whether* $i_r \in I_G$ *or* $i_r \in I_B$. *If* $i_r \in I_G$ *then Alice outputs* $b = r$ *and she outputs* $b = 1 - r$ *otherwise.*

Alice's output bit b represents Alice's guess for the bit C that honest Bob got from the protocol.

Intuitively the sets I_0, I_1 carry information about the correlations Alice and Bob share at the beginning of the post-processing, but not about Bob's final output C. In particular these sets say that if their initial (honest) inputs are such that Bob knows the bits of X_1^n on positions given by I_0 then $C = 0$, and if he initially knows the bits of X_1^n on positions given by I_1 then $C = 1$. However since honest Alice does not know which bits of X_1^n Bob knows (she is ignorant about $\mathscr{I}$), it does not say anything about the actual value of Bob's output C. Dishonest Alice however gets extra inputs (I_G, I_B) that precisely gives her information about which are the bits Bob knows. As a consequence by cross-referencing these two pieces of information dishonest Alice can get some advantage in guessing bit C.

6.3. DISCUSSION

In the previous section we show that all protocols that satisfy the two assumptions given in Assumptions 6.2.6 (or more formally Assumption 6.4.19) cannot be secure against dishonest Alice. We believe that the class of protocols that satisfy these conditions is general enough to encompass most (if not all) of the protocols that are currently implementable with current technology. In this section we argue in this direction.

We first point out that it should not be possible to get a fully general impossibility theorem, since we have shown that when having a sufficiently good single photon source it is possible to devise a secure protocol (see Theorem 6.4.9). As a consequence one can only prove statements about more restrictive classes of protocols. This is what we have done in the previous section. However we have analyzed these protocols under Assumptions 6.2.6, and it is not clear how restrictive Assumptions 6.2.6 are. In the following, we argue that most practical protocols will satisfy these assumptions.

First, let us spell out some of the implicit assumptions made for our theorem that necessarily limit the range of its applicability. In the model we use (see Fig. 6.3), it is clear that the classical post-processing operated by Alice and Bob runs on bit strings $(X_1^n, X_{\mathscr{I}}, \ldots)$ and of sets of indices "$\mathscr{I}, \ldots$", however we think that the reasoning used for our theorem can be extended to more general inputs. In this model, we also only start by looking at the attack directly at a post-processing part of the protocols. This is convenient since it allows our theorem to be valid for various quantum implementations that could have run before the post-processing. Of course this assumes that the protocols end with a fully classical post-processing phase. As a consequence our proof only applies for such protocols. However, even though these implicit assumptions limit the applicability of our theorem, we believe that this is enough for any practical implementation.

Let us now go to the core of our assumptions, *i.e.* let us look at conditions given in Assumptions 6.2.6. The first assumption is, informally, that there exists a way for dishonest Alice to compute, from X_1^n and M, sets of indices (I_0, I_1) that correspond to the

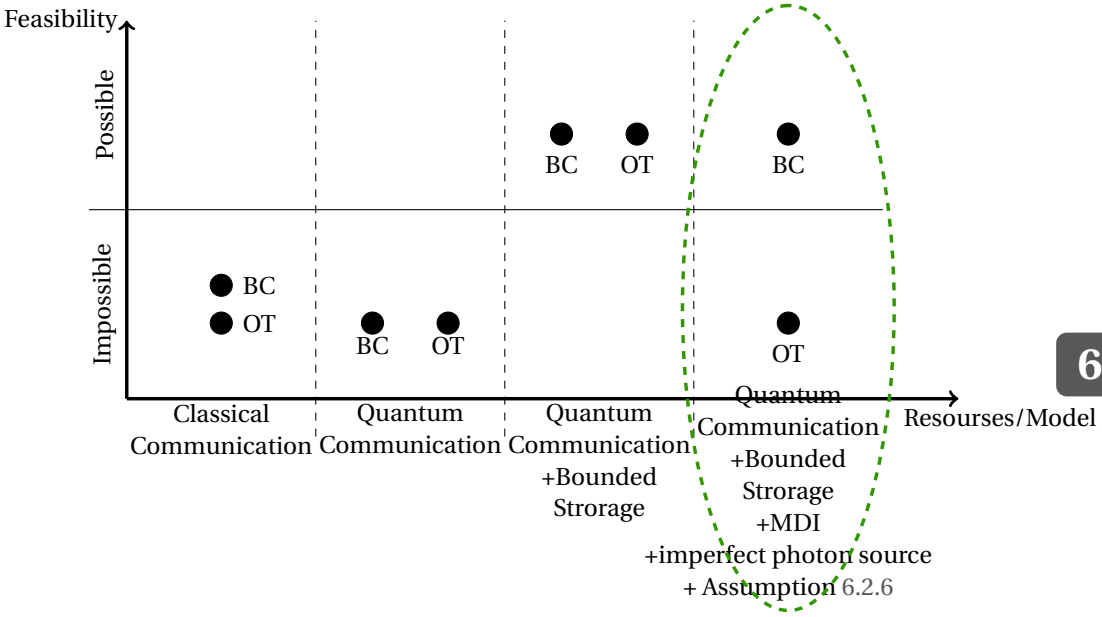


Figure 6.4: Schematic representation of the "Feasibility" of OT and BC depending on the resources/model used in the protocol. In the first column neither BC nor OT are possible, but since OT can be used in order to get BC but not the comtrary, OT is somewhat a harder problem, which is why it is below BC. When quantum communication are possible then OT and BC are equivalent (represented at the same level) but still impossible. In the third column we add the Bounded Storage assumption, which makes both protocol possible. They are still equivalent. In the last column we add that quantum communication between the parties are made in the MDI settings, and we assume that the parties do not have perfect single photon source. In this case BC is possible (see Theorem 6.4.12) but OT is not (see Theorem 6.4.20).

positions in the string X_1^n where the functions f_0 and f_1 are dependent on the value of the bits located at these positions.

The second assumption can be reformulated as follows. If, for a fraction of rounds, some information is leaked then there is a non-negligible probability that $\kappa \geq 1$ (see Assumptions 6.2.6).

We now argue that these two condition are not very restrictive.

- Indeed we conjecture that the first assumption should always hold: In order for the protocol to be correct, intuitively the set of messages exchanged in the protocol represented by the random variable M should contain the information that "tells" the functions f_0 and f_1 how they should act on the bits of X_1^n, and on which of these bits they should operate. This suggests that Alice can also retrieve this information, *i.e.* compute (I_0, I_1). We do not give a formal proof of this statement, that is why it is taken as an assumption. In a protocol like Protocol 6.2.4 it is clear that this condition is satisfied since Bob explicitly sends the pair (I_0, I_1) to Alice.

- If the second assumption was not satisfied then – at least intuitively – Bob is able to know (with overwhelming probability) which rounds leak information (multiphoton emission rounds) and therefore choose the sets I_0 and I_1 (or sufficiently influence the protocol) such that $\kappa = 0$. But then Bob could effectively get an almost perfect (except with negligible probability) single photon source, by preventing any multiphoton emission from leaving his lab. In a protocol like the ones we have presented in the previous sections, Bob does not know in which rounds his source has emitted multiple photons, therefore there will be in the end with very high probability multiphoton rounds that are kept.

For these reasons we believe that our impossibility result applies to most (if not all) currently implementable OT protocols.

In the presence of quantum communication, it is known that OT and BC are equivalent [17, 18], meaning that from one of these tasks one can build a secure protocol for the other. However the construction used, implicitly assumes a trusted device setting, and as a consequence this construction does not necessarily prove equivalence between OT and BC in MDI settings. Since we prove earlier in this chapter that BC is secure (in the bounded/noisy quantum storage model), if our impossibility result for OT generalizes, MDI settings (without a single photon source), it would be the first quantum setting where one can prove security for BC but not for OT with the same adversarial model (see Fig. 6.4), *i.e.* it would be a quantum setting in which OT and BC are not equivalent.

6.4. METHODS

In this section we present and prove security statement for the protocols presented in the results sections. We start by stating theorems and lemmas that will be useful in our proofs. Then we proof security for BC and OT when the honest players have perfect photon sources. We continue by giving the security proof for BC when the honest parties only have imperfect single photon sources. We finally prove that a class of protocols cannot be secure for OT when using imperfect single photon sources.

Remark 6.4.1. *For simplicity, all our statements and proofs are expressed in the Bounded Storage model, but can easily be extended to the Noisy Storage Model as explained in Chapter 2.*

6.4.1. USEFUL LEMMAS AND THEOREMS

Here, we give useful theorems that we will use as tools for our proofs.

Using the ideas from [13, 14] we will use random codes to prove the security of Bit Commitment. We give here one useful property of these random codes, which can be viewed as a tradeoff between the minimal distance d of the code and its rate R.

Theorem 6.4.2 ([19])**.** *For a randomly generated $[n,k,d]$ binary linear code with rate $R := k/n$, the minimum distance d satisfies,*

$$\Pr(d \leq \delta n) \leq 2^{(R-C_\delta)n}, \text{ for } 0 \leq \delta \leq 1, \tag{6.3}$$

where $C_\delta := 1 - h(\delta)$ and $h(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

The following min-entropy splitting lemma intuitively states that for a classical distribution $P_{X_0X_1Z}$, if the min-entropy (conditioned on Z) on (X_0, X_1) is large then it must be the case that the random variable X_{1-C} has high min-entropy too, where C is a binary random variable.

Lemma 6.4.3 (Min-entropy splitting [20, 21])**.** *Let X_0, X_1, Z be three random variables with distribution $P_{X_0X_1Z}$. Let $1 > \epsilon > 0$. If*

$$H_{\min}^{\epsilon}(X_0X_1|Z) \geq K, \tag{6.4}$$

then there exists a binary random variable C such that,

$$H_{\min}^{4\epsilon}(X_{1-C}|CZ) \geq K/2 - 1 + 2\log(1-\sqrt{1-\epsilon^2}). \tag{6.5}$$

6.4.2. BIT COMMITMENT (BC) WITH PERFECT SINGLE PHOTON SOURCES

In this section we present the security proof for Protocol 6.2.2 which implements BC when honest parties have perfect single photon sources. In particular we prove Theorem 6.4.4 below. The security proof is mostly the same as in [13, 14], the only differences are that in our Protocol 6.2.2 we are guaranteed that the sources emit single photons, so we do not need to care about multiphoton emissions, and that because we want the security to hold even in the presence of noise, we adapt the simulator argument of [13]. More over we use a more recent lower bound [22] on the min-entropy.

Theorem 6.4.4 (Security of Protocol 6.2.2)**.** *Let $\epsilon > 0$ be a security parameter, $e_{\text{err}} \in [0, 1/2[$ is the expected error rate of the protocol, and let $l \in \mathbb{N}$, $l > 0$ be the length of the string we want to commit. Let us call n the number of quantum communication rounds in which the measurement station has clicked in Protocol 6.2.2, and let $\alpha_2 := \sqrt{\frac{\ln\epsilon^{-1}}{2(1/2-\alpha_1)n}}$, $\alpha_1 := \sqrt{\frac{\ln\epsilon^{-1}}{2n}}$ which account for statistical fluctuations. Let Q be dishonest Bob's quantum register, K his classical register, and D be such that $\log\dim(Q) \leq D$. Let $\mathscr{C}$ be a randomly generated-$[n,k,d]$ linear code with fixed n and k and rate $R := k/n$. We choose the rate of*

code $\mathscr{C}$ to be $R = \ln(\epsilon)/n + 1 - h(\delta)$, where $\delta := 2e_{\text{err}} + 2\alpha_2$. Let $\lambda := f(-D/n) - 1/n$ be a lowerbound on the ϵ-smooth min-entropy rate of honest Alice's string X_1^n conditioned on (malicious) Bobs information KQ, where f is defined in eq. (6.7).

If

$$n \geq \frac{l + 2\log(1/2\epsilon) + \ln(\epsilon^{-1})}{\lambda - h(\delta)}, \tag{6.6}$$

then Protocol 6.2.2 *implements a* $(l, 3\epsilon)-$*Randomized String Commitment.*

Proof. When the two parties are honest and conditioned on not aborting, one can check that the protocol is correct. When the two parties are honest, they can abort in two places. Either they abort in the frst step of the Commit phase or in the third phase of the Open phase. In the first case Bob aborts if $|\mathscr{F} < 1/2n - \alpha_1|$. By the definition of α_1 and Hoeffding inequality, this happens with probabolity at most ϵ. Similarility in step 3 of the Open phase Bob aborts the protocol if he observe an error rate that does not lie in the interval $[e_{\text{err}} - \alpha_2, e_{\text{err}} + \alpha_2]$, which by Hoeffding inequality happens with probability at most 2ϵ. Putting this two potential abort events together, the honest parties have a probability at most 3ϵ to abort, which proves correctness.
Lemma 6.4.6 proves that Protocol 6.2.2 is 3ϵ-hiding.
Lemma 6.4.8 together with Theorem 6.4.2 show that Protocol 6.2.2 is $2\epsilon-$binding. □

6

In the following with will prove Lemmas 6.4.6 and 6.4.8, which state security for honest Alice and for honest Bob respectively.

Security for Alice: When Bob is dishonest we will assume that he controls the measurement station, therefore we treat the measurement station and Bob as one single party (Fig. 6.2b). Note that this reduces to the trusted device scenario in which Bob is dishonest [13, 14, 22]. As a consequence several results from Refs. [14, 22] can be reused here.

In fact, the situation in this section is even simpler in the sense that we consider that the honest party (Alice) has access to a perfect single photon source. This, together with the fact that we use a lower bound [22] on the min-entropy that does not depends on the specifics of the state but only on the structure of Alice's measurements, prevents Bob from gaining any advantage by (selectively) discarding rounds. We discuss this in more details in Technical Details Section 6.5.1.

Let $f(\cdot)$ be the following function.

$$f(x) := \begin{cases} x & \text{if } x \geq 1/2 \\ g^{-1}(x) & \text{if } x < 1/2, \end{cases} \tag{6.7}$$

where $g(x) := h(x) + x - 1$ and $h(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

Lemma 6.4.5 (from [22])**.** *Let $\epsilon \geq 0$. If Alice is honest, and Bob has a bounded quantum memory Q (his quantum register Q has dimension at most 2^D) then at the end of the preparation phase, the smooth min-entropy of Bob on Alice string is*

$$H_{\min}^{\epsilon}(X_1^n|QK)_\rho \geq \lambda n, \tag{6.8}$$

where $\lambda = f(-D/n) - 1/n - \log(2/\epsilon^2)/n$, and K is Bob's classical register.

Since in the protocol Alice sends the syndrome of her string X_1^n to Bob, we need this syndrome to be sufficiently small in order to keep the entropy relatively high so that the protocol is secure against dishonest Bob. On the other hand, we need the distance of the code to be sufficiently large in order to tolerate errors that might occur between honest Alice and honest Bob. As in Ref. [14] we use a random code: They have sufficiently small syndrome with high distance for our purpose, and since the honest party are not using any decoding we do not need an efficiently decodable code.

Lemma 6.4.6 (Security against Dishonest Bob, similar as in Ref. [14])**.** *Let $\epsilon \in]0,1[$. Let Q be Bob's quantum memory such that $\log\dim(Q) \leq D$. Let $\mathscr{C}$ be a random $[n,k,d]$-linear code with rate $R := k/n$. If n satisfyies*

$$\begin{cases} \lambda - 1 + R > 0 \\ \textit{and,} \\ n \geq \frac{l+2\log(1/2\epsilon)}{\lambda-1+R}. \end{cases} \tag{6.9}$$

If Alice is honest, then the protocol is 3ϵ-hiding.

Proof. Using Lemma 6.4.5 we obtain that after the Commit phase, Bob's entropy on Alice's string X_1^n is,

$$H_{\min}^{\epsilon}(X_1^n|QK\mathsf{Syn}(X_1^n))_\rho \geq (\lambda - 1 + R)n, \tag{6.10}$$

where R is the rate of the code $\mathscr{C}$, *i.e.*, and the length of the syndrome being $n-k = (1-R)n$. This together with the leftover hash Lemma 2.3.6 leads us to

$$\rho_{C_1^l, QK\mathsf{Syn}(X_1^n)} \approx_{\epsilon'} \tau_{C_1^l} \otimes \rho_{QK\mathsf{Syn}(X_1^n)}, \tag{6.11}$$

where $\tau_{C_1^l}$ is the maximally mixed state on C_1^l, and

$$\epsilon' = 2\epsilon + \frac{1}{2}2^{-\frac{1}{2}(H_{\min}^{\epsilon}(X_1^n|QK\mathsf{Syn}(X_1^n))-l)}. \tag{6.12}$$

If $\lambda - 1 + R > 0$, then by choosing n sufficiently large we can have $\epsilon' \leq 3\epsilon$, meaning that Protocol 6.2.2 is 3ϵ-hiding. □

Security for Bob:

Figure 6.5 tells us that the protocol where it is dishonest Alice that sends half of an EPR pair to Bob produces the exact same state as Protocol 6.2.2 when Alice is dishonest. We can therefore adapt the analysis of [13] to the presence of noise, which leads us to the following lemma.

Lemma 6.4.7 (Similar to Theorem III.5 of [13])**.** *If Bob is honest, then at the end of the preparation phase, there exists an ideal state $\sigma_{A\bar{X}_1^n\mathscr{J}}$ between (dishonest) Alice and Bob such that:*

- $\sigma_{A\bar{X}_1^n\mathscr{J}} = \sigma_{A\bar{X}_1^n} \otimes \tau_{\mathscr{J}}$
- $\rho_{AB} = \sigma_{A(\bar{X}_{\mathscr{J}}\mathscr{J})}$,

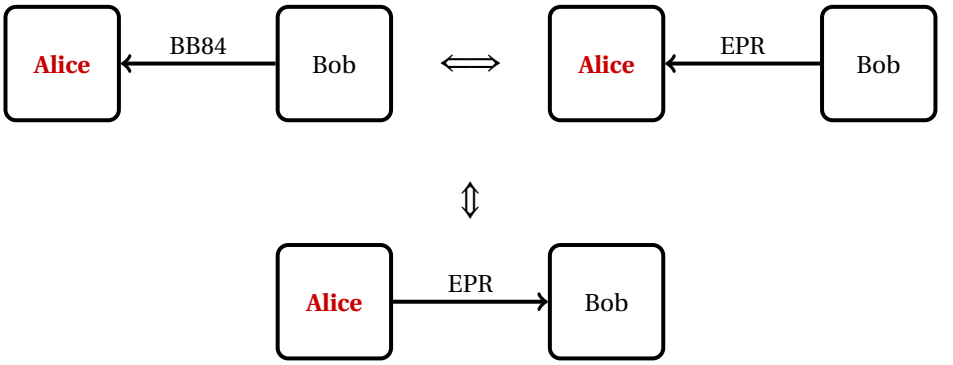


Figure 6.5: When honest Bob has access to a single photon source and Alice is dishonest, the three situations depicted are equivalent: In the first Bob chooses the bases $\hat{\Theta}_1^n$ and $\hat{X}_1^n$ uniformly at random, and sends a BB84 type state, as described in Protocol 6.2.2. The second picture depicts the equivalent scenario where he sends half of an EPR pair to Alice, and gets $\hat{X}$ and $\hat{\Theta}$ by measuring the other half. This scenario itself is equivalent to the last where it is (dishonest) Alice that sends half of the EPR pair. If some noise acts on the qubit sent by Bob to Alice in the first scenario, this can be seen as Alice applying a "noise map" on the half of the EPR pair she keeps before applying a measurement in the third scenario. In this virtual scenario, the other half of the EPR pair is assumed to be sent (measured) to (by) Bob without any noise.

where $\tau_{\mathscr{I}}$ is the maximally mixed state on $\mathscr{I}$, ρ_{AB} is the real state produced by the protocol between (dishonest) Alice and Bob, and where the registers (A,B) are identified with $(A,\bar{X}_{\mathscr{I}}\mathscr{I})$.

Proof (Sketch). We will place ourselves in the virtual scenario of Figure 6.5 where Alice sends the states to Bob. Here, contrary to [13] we want to take care of the noise that might affect the quantum signal and measurements, therefore the simulator introduced in Ref. [13] has to be slightly modified.

In order to prove the existence of an ideal state σ, in Ref. [13] the authors introduce a virtual protocol where a simulator lies between dishonest Alice and honest Bob. This simulator will measure the states sent from Alice to Bob, thus creating the register $\bar{X}_1^n$ and then send an "honest" state to Bob. Then they show that the ideal state σ created by this virtual protocol satisfies the two relations of Lemma 6.4.7 with the real state ρ of the real protocol.

In our case Fig. 6.5 tells us that the noise will only be on the half of the EPR pair kept by Alice, and that the qubit sent to Bob is not affected by any noise. Therefore if the simulator measures it and reencodes it honestly (and without noise) a qubit corresponding to its outcome and choice of measurement basis, the two relations of this lemma will be satisfied. □

From here on, reusing the argument in Refs. [13, 14] we get the final statement for Bob's security.

Lemma 6.4.8. *Let $\epsilon > 0$. Let $\mathscr{C}$ be an $[n,k,d]$-code with minimum distance d that satisfies,*

$$d \geq 2(e_{\text{err}} + 2\alpha_2)n \underset{n\to\infty}{\sim} 2e_{\text{err}}n, \tag{6.13}$$

with $\alpha_2 := \sqrt{\frac{\ln\epsilon^{-1}}{2(1/2-\alpha_1)n}}$, $\alpha_1 := \sqrt{\frac{\ln\epsilon^{-1}}{2n}}$, *then Protocol 6.2.2 either aborts before the open phase or is* ϵ*-binding according to definition 6.5.3. Note that the protocol specifies what the honest parties have to do when aborting. What they do during an abort event enforces security definition 6.5.3 to be also satisfied when the protocol aborts.*

Proof. We again follow the reasoning from [13, 14]. According to Lemma 6.4.7 there exists a random variable $\bar{X}_1^n$, such that Bob knows $\bar{X}_{\mathscr{I}}$ and $\mathscr{I}$. Now if Alice wants to cheat she needs to send to Bob a string $X_1^n \neq \bar{X}_1^n$ such that $\mathsf{Syn}(X_1^n) = w$ which implies that $d_H(\bar{X}_1^n, X_1^n) \geq d/2$ (see [13, Lemma IV.4]), where $d_H(\cdot)$ is the hamming distance. Therefore Alice has to flip at least $d/2$ bits from $\bar{X}_1^n$ in such a way that $d_H(\bar{X}_{\mathscr{I}}, X_{\mathscr{I}}) \leq (e_{\text{err}} + \alpha_2)m$. However Alice is ignorant about which bits Bob knows. As a consequence the situation is equivalent to where $\mathscr{I}$ is chosen after that Alice has chosen which bits she wanted to flip. This is a sampling problem, which means that we can use Hoeffding's inequality [23] to estimate the number W of bits in $\mathscr{I}$ that Alice will flip:

$$\Pr\left(W \leq m(d/2n - \alpha_2)\right) \leq \exp(-m\alpha_2^2) \leq \exp\left(-m\sqrt{\frac{\ln\epsilon^{-1}}{2m}}^2\right) =: \epsilon. \tag{6.14}$$

Therefore if,

$$d \geq 2(e_{\text{err}} + 2\alpha_2)n \tag{6.15}$$

$$\Rightarrow m(d/2n - \alpha_2) \geq (e_{\text{err}} + \alpha_2)m \tag{6.16}$$

then by using eqs. (6.14) and (6.16) we get $\Pr(W < (e_{\text{err}} + \alpha_2)m) \leq \epsilon$ meaning that Alice's attempt in cheating is detected (and Bob will not accept) with probability $\geq 1 - \epsilon$. □

6.4.3. OBLIVIOUS TRANSFER (OT) WITH PERFECT SINGLE PHOTON SOURCES

In this section we present and prove Theorem 6.4.9 stating security for Protocol 6.2.4 which implements a Randomized Oblivious String Transfer when the honest parties have access to single photon sources. The security proof closely follows the security proofs from [13, 24]. Indeed the main difference in our case is simply to show that security of our protocol can be reduced to the security of [24]. This is the case because when Bob is dihonest, he controls the measurement station so we are in a situation where Alice sends BB84 states to dishonest Bob, and security from [24] in this case. When Alice is dishonest we use the fact that sources emit single photons together with a purification argument in order to reduce the security of our protocol to the one of [24].

Theorem 6.4.9. *Let* $\epsilon > 0$ *and let* $l = |S_0| = |S_1|$, *and* $\alpha_1 := \sqrt{\frac{\ln\epsilon^{-1}}{2n}}$. *If the number of* n *of quantum communication rounds in which the measurement station has clicked satisfies condition* (6.17), *the Protocol 6.2.4 implements an 1-out-2 Randomized* $(l, 8\epsilon)-$*Oblivious String Transfer (see Def. 6.5.4).*

Proof. Let's first check correctness with honest Alice and honest Bob. Note that conditioned on not aborting the protocol is $\epsilon-$correct. Indeed the only case where the protocol is not correct conditionned on not aborting is when the error correction procedure fails

to correct Bob's string which happens with probability at most ϵ. We then prove that when both parties are honest, the protocol aborts with probability at most 2ϵ. Indeed an abort event happens either if $|\mathscr{I}| < m$ which happens with probability at most ϵ, or if the error correction procedure aborts which happens with probability at most ϵ. As a consequence the protocol aborts with probability at most 2ϵ, and since conditioned on not aborting it is $\epsilon-$correct, it implies that overall the protocol is $3\epsilon-$correct.
According to Lemma 6.4.10, the protocol is $8\epsilon-$secure for honest Alice.
According to Lemma 6.4.11, the protocol is $(\epsilon = 0)-$secure for honest Bob. □

In the following we state and prove Lemmas 6.4.10 and 6.4.11 which state security for honest Alice and for Honest Bob respectively.

Security for Alice: Since the preparation phase of Protocols 6.2.2 and 6.2.4 are the same, we will use similar bounds as in Lemma 6.4.5 [13] to lower bound the entropy on X_1^n. However we will not use the exact same bounds because we afterwards want to use the min-entropy splitting lemma that is valid only on purely classical states. As a consequence we will first use a chain rule (Theorem 2.3.9) to get rid of Bob's quantum memory and then lower bound the entropy.

Lemma 6.4.10. *Let Bob be dishonest with a bounded quantum memory denoted Q such that $\log\dim(Q) \leq D$ for some D. Let $l := |S_0| = |S_1|$ be the length of the two strings S_0 and S_1. If*

$$n \geq 2\frac{l + D + 1 - 2\log(1-\sqrt{1-\epsilon^2})}{\lambda - \text{leak}_O - 2\alpha_1} \tag{6.17}$$

where $\text{leak}_O := |O|$ is the size of the error correction information Alice sends to Bob, then Protocol 6.2.4 is 8ϵ-secure for Alice, with $\lambda = 1/2 - 2\delta'$, $\delta' = \left(2-\log(\sqrt{(32\ln\epsilon^{-1})/n})\right)\sqrt{(32\ln\epsilon^{-1})/n}$ [13, eq. (19)].

Proof. Protocol 6.2.4 is designed in such a way that it is sufficient to prove that there exists a binary random variable C such that the entropy $H_{\min}^{\epsilon}(X_{I_{1-C}}|KQCO)$ at the end of the preparation phase is sufficiently high. Indeed after the preparation phase Alice and Bob will use a randomness extractor on X_{I_0} and on X_{I_1}, meaning that if the above mentioned entropy is high enough then Bob will be ignorant of at least one of the two "extracted" strings, which is what we want from the security definition. In order to bound this entropy, we will start by bounding $H_{\min}^{\epsilon}(X_{I_0}X_{I_1}|KO)$ where the quantum register Q is not used, and we will reintroduce it later using a min-entropy chain rule (Theorem 2.3.9).

Note that $X_1^n = X_{\mathscr{I}}X_{\mathscr{I}_{\text{Bad}}}X_{\text{remaining}} = X_{I_0}X_{I_1}X_{\text{remaining}}$. By definition of $\mathscr{I}$ and $\mathscr{I}_{\text{Bad}}$, we have that $|X_{\text{remaining}}| = n - 2m = 2\alpha_1 n$. Therefore

$$H_{\min}^{\epsilon}(X_{I_0}X_{I_1}|KO) = H_{\min}^{\epsilon}(X_{\mathscr{I}}X_{\mathscr{I}_{\text{Bad}}}|KO) \geq H_{\min}^{\epsilon}(X_1^n|KO) - 2\alpha_1 n. \tag{6.18}$$

By using the previous bound together with the min-entropy splitting lemma (Lemma 6.4.3), we get that there exists a binary random variable C such that,

$$H_{\min}^{4\epsilon}(X_{I_{1-C}}|KOC) \geq (H_{\min}^{\epsilon}(X_1^n|KO) - 2\alpha_1 n)/2 - 1 + 2\log(1-\sqrt{1-\epsilon^2}). \tag{6.19}$$

Using the min-entropy chain rule (Theorem 2.3.9) on the register Q ($|Q| \leq D$) and combining it with eq. (6.19) we conclude that

$$H_{\min}^{4\epsilon}(X_{I_{1-C}}|KCOQ) \geq H_{\min}^{4\epsilon}(X_{I_{1-C}}|KOC) - |Q| \tag{6.20}$$

$$\geq (H_{\min}^{\epsilon}(X_1^n|KO) - 2\alpha_1 n)/2 - 1 + 2\log(1-\sqrt{1-\epsilon^2}) - D, \tag{6.21}$$

where C is defined by the use of the min-entropy splitting lemma in eq. (6.19).

We will now again use the chain rule (Theorem 2.3.9) to get rid of the register O, and we will call $\text{leak}_O := |O|$ the maximum leakage due to error correction, and we get

$$H_{\min}^{\epsilon}(X_1^n|KO) \geq H_{\min}^{\epsilon}(X_1^n|K) - \text{leak}_O. \tag{6.22}$$

inserting this into the previous inequality gives,

$$H_{\min}^{4\epsilon}(X_{I_{1-C}}|KCOQ) \geq (H_{\min}^{\epsilon}(X_1^n|K) - \text{leak}_O - 2\alpha_1 n)/2 - 1 + 2\log(1-\sqrt{1-\epsilon^2}) - D. \tag{6.23}$$

The amount of error correction information leak_O sent during the protocol can be predetermined by considering the necessary amount of error correction information the parties need when they are both honest, *i.e.* when both parties (and the measurement station) act in an identically and independently distributed (IID) and trusted manner, and where all the errors come from an i.d.d. noise – an "honest noise". Indeed if the parties are honest – and if leak_O is sufficiently large – they will be able to correct their string with probability ($\geq 1-\epsilon$), making the protocol correct. If Bob is not honest, since the amount of error correction information is fixed, then the leakage of information is also fixed no matter what strategy he uses. The question is now, how large is "sufficiently large" to allow honest Alice and Bob to correct their string with high probability? This question has been answered in Refs.[25, 26] where it is shown that one can take

$$\text{leak}_O = H_{\max}^{\epsilon}(X_{I_0}|\hat{X}_{I_0}C=0)_{\rho_{\text{honest}}} + H_{\max}^{\epsilon}(X_{I_1}|\hat{X}_{I_1}C=1)_{\rho_{\text{honest}}} = 2H_{\max}^{\epsilon}(X_{I_0}|\hat{X}_{I_0}C=0)_{\rho_{\text{honest}}},$$

where the entropies are evaluated on the state ρ_{honest} produced by the protocol when both parties are honest.

One can then lower-bound $H_{\min}^{\epsilon}(X_1^n|K)$ using [13, eq. (19)] (see also [27]),

$$H_{\min}^{\epsilon}(X_1^n|K) \geq \lambda n,$$

with $\lambda = 1/2 - 2\delta$, $\delta = \left(2 - \log(\sqrt{(32\ln\epsilon^{-1})/n})\right)\sqrt{(32\ln\epsilon^{-1})/n}$. Since $H_{\max}^{\epsilon}(X_{I_0}|\hat{X}_{I_0}C=0)_{\rho_{\text{honest}}}$ is evaluated on honest i.i.d parties we can upper-bound the max-entropy using the equipartition Theorem [28], getting $2H_{\max}^{\epsilon}(X_{I_0}|\hat{X}_{I_0}C=0)_{\rho_{\text{honest}}} \leq 2h(e_{\text{err}})n/2 + \mathcal{O}(\sqrt{n}) = h(e_{\text{err}})n + \mathcal{O}(\sqrt{n})$ where e_{err} is the error rate between Alice's string X_{I_0} and Bob's string $\hat{X}_{I_0}$.

Using (6.23) and the fact that $S_{1-C} := \text{Ext}(X_{I_{1-C}}, r_{1-C})$ we can invoke the leftover hash lemma 2.3.6 to get that,

$$\rho_{S_C Q S_{1-C}} \approx_{8\epsilon} \sigma_{S_C QC} \otimes \tau_{S_{1-C}}, \tag{6.24}$$

where $\tau_{S_{1-C}}$ denotes the maximally mixed state on S_{1-C}. □

Security for Bob: Once again the preparation phase is the same as for Protocol 6.2.2, therefore we also use Lemma 6.4.7 to show that the protocol is secure for Bob. Intuitively this is true because at the end of the preparation phase, Alice is ignorant about $\mathscr{I}$, and after that no information about C is leaked.

Lemma 6.4.11. *If Bob is honest, then Protocol 6.2.4 satisfies the security definition for Bob.*

Proof (Informal). Since the ideal state satisfies $\sigma_{A\bar{X}_1^n\mathscr{I}} = \sigma_{A\bar{X}_1^n} \otimes \tau_{\mathscr{I}}$ and that the only information sent from Bob to Alice is (I_0, I_1), there is no leakage on the value of C, therefore Alice remains ignorant about C. In other words the state $\sigma_{A'S_0S_1C}$ created by applying Protocol 6.2.4 (with dishonest Alice) on the ideal state $\sigma_{A\bar{X}_1^n\mathscr{I}}$, satisfies the condition $\sigma_{A'S_0S_1C} = \sigma_{A'S_0S_1} \otimes \tau_C$.

Also since from Lemma 6.4.7 $\sigma_{A(X_{\mathscr{I}}\mathscr{I})} = \rho_{A(X_{\mathscr{I}}\mathscr{I})}$ and that the same operations are applied in the ideal and real scenario (on the registers $AX_{\mathscr{I}}\mathscr{I}$) we get that $\sigma_{A'S_CC} = \rho_{A'S_CC}$. □

6

6.4.4. BIT COMMITMENT WITH AN IMPERFECT SINGLE PHOTON SOURCES

In this section we present security proof for Protocol 6.2.5 which implements String Commitment when honest parties have imperfect single photon sources. In particular we prove Theorem 6.4.12 below. The proof is essentially the same as for Theorem 6.4.4, but of course since we are now dealing with imperfect single photon sources, we need to be more careful the rounds where the honest party sends multiple photons. Indeed in this case the malicious party could try to selectively discard the rounds where he receives less information, typically the single photon rounds, and only keep the rounds that might leak some information, the multiphoton rounds. To prevent that we add decoy states in the preparation phase, which will allow the honest party to check how many multiphoton rounds are kept at the end of the preparation phase as compare to the single photon rounds. If to many multiphoton rounds are kept at the end of the preparation phase, the honest party aborts the protocol.

Theorem 6.4.12. *Let $\epsilon, \varepsilon, \hat{\varepsilon}, \epsilon_1$ be as defined in Lemma 6.4.13, and let $\gamma, e_{\text{err}} \in [0, 1/2[$. The values of the parameters γ and e_{err} can be chosen by estimating the parameters honest devices. Let N be the total number of quantum communication rounds of the preparation phase of Protocol 6.2.5, let n_k^H be the number of these rounds in which party H's source ($H \in \{Alice, Bob\}$) has produced k photons and in which the measurement station has clicked, and let n be the number of communication rounds that are not discarded at the end of the preparation phase. Let $\alpha_2 := \sqrt{\frac{\ln\epsilon^{-1}}{2(1/2-\alpha_1)n}}$, $\alpha_1 := \sqrt{\frac{\ln\epsilon^{-1}}{2n}}$, $\alpha_1'' := \sqrt{\frac{\ln\epsilon^{-1}}{2(1-\gamma-\alpha_4^B)n}}$,*

$\alpha_1' := \min\left[1/2; \frac{\alpha_1+(1-\gamma-\alpha_4^B)\alpha_1''}{\gamma+\alpha_4^B}\right]$, $\alpha_3 := \sqrt{\frac{\ln\epsilon^{-1}}{2n\left[1/2-\alpha_1''-(1/2+\alpha_1')(\gamma+\alpha_4^B)\right]}}$. *Let*

$$\begin{aligned}
&\beta^A := \sqrt{\ln(1/\epsilon)/(2(n_1^A+n_{\geq 2}^A))}, \text{ we will assume that } \beta^A \leq p_{b_s}/2,\\
&\beta^B := \sqrt{\ln(1/\epsilon)/(2(n_1^B+n_{\geq 2}^B))}, \text{ we will assume that } \beta^B \leq p_{a_s}/2,\\
&\alpha_4^A := (2/p_{bs}+1/f_{b_s})\beta^A,\\
&\alpha_4^B := (2/p_{a_s}+1/f_{a_s})\beta^B.
\end{aligned}$$

Let $\mathscr{C}$ be a randomly generated $[n,k,d]$ (with fixed n and k) linear code with rate $R := k/n$. We choose this code such that the rate $R = \ln(\epsilon)/n + 1 - h(\delta)$, where $\delta := 2\left[(1/2+\alpha_1')(\gamma+\alpha_4^B)+\alpha_3+\frac{(e_{\text{err}}+\alpha_2)(1/2+\alpha_1)}{(1/2-\alpha_1')(1-\gamma-\alpha_4^B)}\right]$. Let Q be Bob's quantum register, and let D be such that $\log\dim(Q) \leq D$. Let $\lambda := f(-D/n)-(\gamma+\alpha_4^A)-1/n$ lower-bound the ϵ-smooth min-entropy rate $(H_{\min}^{\epsilon}(X_1^n|QK)_\rho)/n$ except with probability $16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$, where f is defined in eq. (6.33).
If the single photon sources used by honest parties are sufficiently good, i.e.

$$\begin{cases} p_{\geq 2|a_s}/(1-p_{0|a_s}) \leq p_{b_s}\gamma, \\ \text{and} \\ p_{\geq 2|b_s}/(1-p_{0|b_s}) \leq p_{a_s}\gamma, \end{cases} \tag{6.25}$$

and if $(p-\sqrt{\ln(\epsilon^{-1})/2N})N \geq n^*$, where n^* the smallest positive integer solution to the following inequality[5]*,*

$$n \geq \frac{l+2\log(1/2\epsilon)+\ln(\epsilon^{-1})}{\lambda-h(\delta)}, \tag{6.26}$$

and where p is the probability that a round $i \in [N]$ is not discarded in the preparation phase when both parties are honest, then Protocol 6.2.5 implements a $\left(l, 9\epsilon+32(\epsilon+\varepsilon+\hat{\varepsilon})+16\epsilon_1\right)$−1-out-2-Randomized String Commitment.

Proof. Let's start with correctness. First of all note that conditioned on not aborting the protocol is correct. We now show that when both parties are honest the protocols aborts with probability smaller than $9\epsilon+32(\epsilon+\varepsilon+\hat{\varepsilon})+16\epsilon_1$, which implies that the protocol is $(9\epsilon+32(\epsilon+\varepsilon+\hat{\varepsilon})+16\epsilon_1)$−correct. Using Hoeffding inequality it is easy to check that the honest parties will abort with probability at most 2ϵ at step 2 of the preparation phase.

If the two parties are honest with sources such that $p_{\geq 2|a_s}/(1-p_{0|a_s}) \leq p_{b_s}\gamma$ (for Alice) and $p_{\geq 2|b_s}/(1-p_{0|b_s}) \leq p_{a_s}\gamma$ (for Bob), then the probability to abort at step 3 is at most $\epsilon+16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$ and at most $\epsilon+16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$ at step 4. Indeed in step 3, using Hoeffding inequality one can check that with probability at most ϵ, we have $\frac{n_{\geq 2}^A}{n_1^A+n_{\geq 2}^A} \leq p_{b_s}\gamma+\beta^A$. By dividing the expression by f_{b_s} and using that conditioned on not aborting in the previous steps $f_{b_s} \geq p_{b_s}-\beta^A$ we get $\frac{n_{\geq 2}^A}{f_{b_s}(n_1^A+n_{\geq 2}^A)} \leq \frac{p_{b_s}}{p_{b_s}-\beta^a}+1/f_{b_s}\beta^A$. Using that

[5] Remember that the parameters like λ, δ etc. depend on n

except with probability $16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$ we have $U_{A2} \geq n^A_{\geq 2}$ and that for $1/p_{b_s}\beta^A \leq 1/2$ we have $1/(1-1/p_{b_s}\beta^A) \leq 1+2/p_{b_s}\beta^A$ we get the desired result. An analog proof holds for step 4. Again by Hoeffding inequality, there is a probability at most ϵ to abort at step 5.

Using again Hoeffding inequality one can check that Bob will abort the protocol with probability at most 2ϵ at step 1 of the Commit phase and with probability at most 2ϵ at phase 3 of the open phase. Over all the protocol aborts with probability at most $9\epsilon + 32(\epsilon+\varepsilon+\hat{\varepsilon})+16\epsilon_1$.
Security for honest Alice is given in Lemma 6.4.15. Security for honest Bob is given in Lemma 6.4.17. □

Before proving security for honest Alice (Lemma 6.4.15) and for honest Bob (Lemma 6.4.17), we need to prove that the honest party $H \in \{Alice, Bob\}$ can always find a lower-bound L_{H1} on n^H_1, the number rounds where H has emitted a single photon and has sent a "signal" state. This is what the following lemma shows. You can find its proof in Technical Details Section 6.5.2.

Lemma 6.4.13. *Let $x^i_{o,\theta}$ be the "observed" number of rounds where H has prepared a signal of intensity i in the basis θ and where the measurement station (or the dishonest party) reported outcome $o \neq$ failure. Let $\epsilon, \epsilon_1 > 0$, and $\varepsilon, \hat{\varepsilon}$ such that $\forall(o,\theta)$, $(2\varepsilon^{-1})^{1/\zeta_{o,\theta,L}} \leq \exp(3/(4\sqrt{2}))^2$ and $(\hat{\varepsilon}^{-1})^{1/\zeta_{o,\theta,L}} < \exp(1/3)$, with $\zeta_{o,\theta,L} := x^i_{o,\theta} - \sqrt{\sum_i x^i_{o,\theta}/2\ln(1/\epsilon)}$. Let $\Delta_{i,o,\theta} := g(x^i_{o,\theta}, \varepsilon^4/16)$, $\hat{\Delta}_{i,o,\theta} := g(x^i_{o,\theta}, \hat{\varepsilon}^{3/2})$, and $g(x,y) := \sqrt{2x\ln(y^{-1})}$. Then if $q = 2$ (q is the number of decoy states used during the protocol i.e. $i \in \{i_s, i_{d_1}, i_{d_2}\}$) we have,*

$$n^H_1 \geq L_{H1} := \sum_{o,\theta} \left[p_{i_s|k=1} \, |S_{1,o,\theta}|_{\min} - g(p_{i_s|k=1} \, |S_{1,o,\theta}|_{\min}, \epsilon_1) \right] \tag{6.27}$$

except with probability $16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$, where $|S_{1,o,\theta}|_{\min}$ is given by,

$$|S_{1,o,\theta}|_{\min} := \min(V_1, V_2, V_3, V_4), \tag{6.28}$$

with

$$V_1 = \frac{p_{i_{d_1}|k\geq 2}(x^{i_{d_2}}_{o,\theta} + \Delta_{i_{d_2},o,\theta}) - p_{i_{d_2}|k\geq 2}(x^{i_{d_1}}_{o,\theta} + \Delta_{i_{d_1},o,\theta})}{p_{i_{d_1}|k=1}p_{i_{d_2}|k\geq 2} - p_{i_{d_1}|k\geq 2}p_{i_{d_2}|k=1}} \tag{6.29}$$

$$V_2 = \frac{p_{i_{d_1}|k\geq 2}(x^{i_{d_2}}_{o,\theta} - \hat{\Delta}_{i_{d_2},o,\theta}) - p_{i_{d_2}|k\geq 2}(x^{i_{d_1}}_{o,\theta} + \Delta_{i_{d_1},o,\theta})}{p_{i_{d_1}|k=1}p_{i_{d_2}|k\geq 2} - p_{i_{d_1}|k\geq 2}p_{i_{d_2}|k=1}} \tag{6.30}$$

$$V_3 = \frac{p_{i_{d_1}|k\geq 2}(x^{i_{d_2}}_{o,\theta} + \Delta_{i_{d_2},o,\theta}) - p_{i_{d_2}|k\geq 2}(x^{i_{d_1}}_{o,\theta} - \hat{\Delta}_{i_{d_1},o,\theta})}{p_{i_{d_1}|k=1}p_{i_{d_2}|k\geq 2} - p_{i_{d_1}|k\geq 2}p_{i_{d_2}|k=1}} \tag{6.31}$$

$$V_4 = \frac{p_{i_{d_1}|k\geq 2}(x^{i_{d_2}}_{o,\theta} - \hat{\Delta}_{i_{d_2},o,\theta}) - p_{i_{d_2}|k\geq 2}(x^{i_{d_1}}_{o,\theta} - \hat{\Delta}_{i_{d_1},o,\theta})}{p_{i_{d_1}|k=1}p_{i_{d_2}|k\geq 2} - p_{i_{d_1}|k\geq 2}p_{i_{d_2}|k=1}}. \tag{6.32}$$

One can compute tighter bounds using more decoy states (i.e. for $q > 2$). For more details see Technical Details Section 6.5.2.

For simplicity we will, in the following, continue the security analysis for the case where $q = 2$. The above lemma will allow us to prove the following security lemmas: Lemma 6.4.15 proves security for honest Alice, and Lemma 6.4.17 proves security for honest Bob.

Security for Alice: When Alice is honest almost nothing changes except that Bob's entropy about Alice's string is smaller by roughly γn bits. As a consequence lemma 6.4.5 has to be changed.

Let $f(\cdot)$ be the following function.

$$f(x) := \begin{cases} x & \text{if } x \geq 1/2 \\ g^{-1}(x) & \text{if } x < 1/2, \end{cases} \tag{6.33}$$

where $g(x) := h(x) + x - 1$ and $h(x) := -x\log(x) - (1-x)\log(1-x)$ is the binary entropy.

Lemma 6.4.14. *Let $\epsilon, \varepsilon, \hat{\varepsilon}, \epsilon_1$ be as defined in lemma 6.4.13. If Alice is honest (but uses a non-perfect photon source), and Bob has a bounded quantum memory Q (his quantum register Q has dimension at most D) then at the end of the preparation phase, and if Alice did not abort, the smooth min-entropy of Bob on Alice string is,*

$$H_{\min}^{\epsilon}(X_1^n|QK)_\rho \geq \lambda n \tag{6.34}$$

with probability higher than $1 - 16(\epsilon + \varepsilon + \hat{\varepsilon}) - 8\epsilon_1$, where $\lambda := f(-D/n) - (\gamma + \alpha_4^A) - 1/n$ [22], and K is Bob's classical register.

Here we have used that – as proven in Theorem 6.4.13 – with probability higher than $1 - 16(\epsilon + \varepsilon + \hat{\varepsilon}) - 8\epsilon_1$ dishonest Bob gets at most $(\gamma + \alpha_4^A)n$ extra bits of information due to the leakage information on the bases used by Alice.

We can then reuse Lemma 6.4.6 with the only difference that we have to include the probability that Alice emits 2 or more photons in more than $(\gamma + \alpha_4^A)n$ "non-failure" rounds.

Lemma 6.4.15 (Security against Dishonest Bob)**.** *Let $\epsilon, \varepsilon, \hat{\varepsilon}, \epsilon_1$ be as defined in Lemma 6.4.13. Let Q be Bob's quantum memory such that $\dim(Q) \leq D$, and the rate R of the code $\mathscr{C}$ be such that,*

$$n \geq \frac{l + 2\log(1/2\epsilon)}{\lambda - 1 + R}. \tag{6.35}$$

If Alice is honest, then Protocol 6.2.5 (with $q = 2$) either aborts or is $[3\epsilon + 16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1]$-hiding. Note that when the honest Alice aborts she is required to output uniformly random strings, so that the security definition 6.5.3 is also satisfied when the protocol aborts. In fact when aborting the ideal and the real state are equal.

Proof. The proof is exactly the same as in Lemma 6.4.6, except that we add $16(\epsilon + \varepsilon + \hat{\varepsilon}) + 8\epsilon_1$ to the failure probability, which corresponds to the probability that there are more than $(\gamma + \alpha_4^A)n$ rounds where at least 2 photons have been emitted (see Theroem 6.4.13), and where λ has value given by Lemma 6.4.14. □

Security for Bob:

We will start by stating a lemma similar to Lemma 6.4.7, adapted to the case of an imperfect single photon source.

Lemma 6.4.16. *When Bob is honest, at the end of the preparation phase, there exist a state* $\sigma_{\bar{X}_1^n A\mathscr{I}}$ *such that*

- $\sigma_{\bar{X}_1^n AI} = \sigma_{A\bar{X}_1^n I'} \otimes \tau_{I''}$
- $\rho_{AB} = \sigma_{A(\bar{X}_{\mathscr{I}}\mathscr{I})}$,

where τ *denotes the maximally mixed state,* I' *is the register encoding the set of rounds where Alice got extra information from the emission of multiple photons, and* I'' *is the register encoding the set of rounds in* $\mathscr{I}$ *where Alice did not get any information. Formally the registers* I' *and* I'' *are such that* $I' \otimes I'' = \mathscr{I}$. ρ_{AB} *is the real state produced by the protocol between (dishonest) Alice and Bob, and where the registers* (A, B) *are identified with* $(A, \bar{X}_{\mathscr{I}}\mathscr{I})$.

In the following we will use the same reasoning as in Lemma 6.4.8, adapting it to the case where the multiphoton emissions are possible.

Intuitively when Bob is honest but uses a non-perfect single photon source dishonest Alice basically knows, for a fraction γ of the rounds, whether they belong to $\mathscr{I}$ or not. Using similar notations as in Lemma 6.4.8, this knowledge will help dishonest Alice when she will have to flip $d/2$ bits from $\bar{X}_1^n$. Indeed she can flip the $\approx (\gamma/2)n$ bits that she knows not to be in $\mathscr{I}$. For the $\approx d/2 - (\gamma/2)n$ remaining bits, she will flip bits that are not the $\approx (\gamma/2)n$ she knows to be in $\mathscr{I}$.

Lemma 6.4.17. *Let* $\epsilon, \varepsilon, \hat{\varepsilon}, \epsilon_1$ *be as defined in Lemma 6.4.13. Let* α_1, α_2 *be the same as in Lemma 6.4.8, and* α_4^B *as defined in Protocol 6.2.5. Let* $\alpha_1'' := \sqrt{\frac{\ln \epsilon^{-1}}{2(1-\gamma-\alpha_4^B)n}}$, $\alpha_1' := \min\left[1/2; \frac{\alpha_1+(1-\gamma-\alpha_4^B)\alpha_1''}{\gamma+\alpha_4^B}\right]$, $\alpha_3 := \sqrt{\frac{\ln \epsilon^{-1}}{2n\left[1/2-\alpha_1''-(1/2+\alpha_1')(\gamma+\alpha_4^B)\right]}}$. *Let* $\mathscr{C}$ *be an* $[n, k, d]$*-code with minimum distance* d *that satisfies,*

$$d \geq 2\left[(1/2+\alpha_1')(\gamma+\alpha_4^B) + \alpha_3 + \frac{(e_{\text{err}}+\alpha_2)(1/2+\alpha_1)}{(1/2-\alpha_1')(1-\gamma-\alpha_4^B)}\right] n \underset{n\to\infty}{\sim} \left(\gamma + \frac{2e_{\text{err}}}{1-\gamma}\right) n. \tag{6.36}$$

Then when Bob is honest, Protocol 6.2.2 either aborts or is $[\epsilon + 16(\epsilon+\varepsilon+\hat{\varepsilon}) + 8\epsilon_1]$*-binding according to definition 6.5.3. Since when honest Bob aborts he is requied to reject the opening and output a random string* $\tilde{C}_1^l$*, the security definition is automatically satisfied when honest Bob aborts the protocol.*

Proof (Sketch). From Lemma 6.4.13 we know that except with probability $16(\epsilon+\varepsilon+\hat{\varepsilon}) + 8\epsilon_1$, dishonest Alice gets information on at most $(\gamma+\alpha_4^B)n$ bits.

Except with probability ϵ, at most a fraction $(1/2+\alpha_1')$ of them are not in $\mathscr{I}$, so Alice can flip them without Bob being able to detect this. We can compute this fraction by noticing that on rounds where 1 photon has been emitted (there are at leat $(1-\gamma-\alpha_4^B)n$ of them), the probability of each of these rounds to be in $\mathscr{I}$ is 1/2 and is independent

of Alice's information. Therefore, by Hoeffding inequality, the number of these rounds being in $\mathscr{I}$ should be $\leq 1/2+\alpha_1''$, except with probability ϵ. Moreover, if the protocol does not abort then the total number of rounds in $\mathscr{I}$ is $m \leq (1/2+\alpha_1)n$. Combining this with the fact that $1/2+\alpha_1' \leq 1$ gives the expression for α_1'.

At least $d/2-(1/2+\alpha_1')(\gamma+\alpha_4^B)n$ bits remains for Alice to flip. However she knows that she should flip these remaining bits on the position on which she did not get any information during the preparation phase. There are $\geq (1-\gamma-\alpha_4^B)n$ such positions. Therefore Alice's choice of bit flip is equivalent to uniformly sampling without replacement $d/2-(1/2+\alpha_1')(\gamma+\alpha_4^B)n$ positions out of $\geq (1-\gamma-\alpha_4^B)n$ to estimate the number W of bits that Alice chooses to flip while being in a position in the set $\mathscr{I}$. As for Lemma 6.4.8 this is equivalent to first fixing Alice's bit flip and then choosing the position that are in $\mathscr{I}$ among the $(1-\gamma-\alpha_4^B)n$ available positions. Using Hoeffding inequality we get that,

$$\Pr\Big(W < n\big[1/2-\alpha_1''-(1/2+\alpha_1')(\gamma+\alpha_4^B)\big](d/2n-(1/2+\alpha_1')(\gamma+\alpha_4^B)-\alpha_3)\Big) \tag{6.37}$$

$$\leq \exp\big(-2n\big[1/2-\alpha_1''-(1/2+\alpha_1')(\gamma+\alpha_4^B)\big]\alpha_3^2\big) = \epsilon. \tag{6.38}$$

Now if

$$d \geq 2\left[(1/2+\alpha_1')(\gamma+\alpha_4^B)+\alpha_3+\frac{(e_{\text{err}}+\alpha_2)(1/2+\alpha_1)}{(1/2-\alpha_1')(1-\gamma-\alpha_4^B)}\right]n, \tag{6.39}$$

then with probability $\geq 1-\epsilon-16(\epsilon+\varepsilon+\hat{\varepsilon})-8\epsilon_1$,

$$W \geq n\big[1/2-\alpha_1''-(1/2+\alpha_1')(\gamma+\alpha_4^B)\big](d/2n-(1/2+\alpha_1')(\gamma+\alpha_4^B)-\alpha_3) \tag{6.40}$$

$$\geq (e_{\text{err}}+\alpha_2)(1/2+\alpha_1)n \geq (e_{\text{err}}+\alpha_2)m. \tag{6.41}$$

This means that if eq. (6.39) is satisfied there is a probability at most $\epsilon+16(\epsilon+\varepsilon+\hat{\varepsilon})+8\epsilon_1$ that Alice can cheat and make Bob accept. □

6.4.5. OT WITH AN IMPERFECT SINGLE PHOTON SOURCE

In this section we state more formally our impossibility result for a secure Oblivious Transfer protocol. In particular we show that if a protocol satisfy Assumption 6.4.19, then Protocol 6.2.7 allows dishonest Alice to cheat.

INFORMAL DESCRIPTION OF THE SETTINGS

We recall that dishonest Alice's goal is to guess correctly the bit C that is given to honest Bob by the protocol (the protocol gives him an random bit C and a bit string S_C). In section 6.2.4 we already give a simple example on how an attack could work on a protocol like Protocol 6.2.4. Here we explain informally what is the general form of the protocols to which our impossibility result applies. In the next section we will make this setup definition more precise. Our impossibility result applies to protocols of the following form.

First phase In a first phase, called the quantum phase, Alice and Bob can used classical and quantum communication. This phase outputs string X_1^n to Alice and a string

$X_{\mathscr{I}}$ and set of indices $\mathscr{I}$ to Bob, where $X_{\mathscr{I}}$ is a string formed by the bits of the string X_1^n that are placed at indices in $\mathscr{I}$. In order to model the leakage of information due to the multiphoton emissions (see section 6.2.4) we assume that Alice receives two extra sets of indices I_G and I_B. This two sets are correlated to the set $\mathscr{I}$. In particular we will consider elements of I_G are more likely to belong to $\mathscr{I}$ than elements in I_B. In the simple example of Section 6.2.4, dishonest Alice could compute these sets from the leakage information concerning the bases Bob has used in this phase. Moreover, in this specific example we had that $I_G \subseteq \mathscr{I}$ and $I_G \subseteq \mathscr{I}^c$, where $\mathscr{I}^c$ is the complement of $\mathscr{I}$.

Second phase The second phase of the protocol is purely classical, that is they only send classical messages. Alice and Bob should use the data they got from the first phase in order to compute the desired strings (S_0, S_1) and bit C that the OT protocol should produce (see Definition 6.2.3).

Note that we don't specify the specific form for the first phase, we simply require that it outputs the strings X_1^n, $X_{\mathscr{I}}$ and the set $\mathscr{I}$ with some probability distribution, as well as the extra sets I_G and I_B when Alice is dishonest. The strategy we use to break security of MDI OT protocols is a semi-honest strategy. This means that Alice will essentially run the protocol honestly[6] but record all the information from the communication between her and Bob. In particular, in the quantum phase Alice extracts – from the quantum signal Bob sends to the measurement station – information about set I_G and I_B before applying the measurement that the station should normally apply. Of course our attack rely on the fact that the set I_G and I_B are sufficiently large so that Alice gets enough statistics to have a good guess of Bob's bit C. In other word we need that Bob's photon source leaks enough information. This is captured in the second equation of eq. (6.42) in Assumptions 6.4.19.

After this quantum phase, we assume that Alice and Bob can post process the data they received from the quantum phase, by using purely classical communication. Since we assume that dishonest Alice is semi-honest, we will assume that she runs the post-processing honestly but records all the information she receives from, or sends to Bob.

In the post-processing of Protocol 6.2.4 Bob chooses uniformly at random the bit C, and then renames the sets $\mathscr{I}$ and $\mathscr{I}^c$ into I_0 and I_1 in such a way that $\mathscr{I} = I_C$. Bob then sends (I_0, I_1) to Alice. The information (I_0, I_1) sent by Bob to Alice, should not by itself reveal bit C. But because Alice holds the extra sets I_G and I_B, she can determine which set from (I_0, I_1) corresponds to set $\mathscr{I}$, and therefore she learns the value of bit C. In the general settings, we will simply assume that from all the information Alice has she can compute two sets I_0 and I_1 such that $I_C \subseteq I$ and $I_{1-C} \nsubseteq \mathscr{I}$. This is the second assumption in Assumptions 6.4.19.

In the following sections, we describe in details how we generalize this idea of attack to a more general settings.

SETTINGS DEFINITION

In this section we defined the settings in which our theorem holds. Theorem 6.4.20, states that any protocol that has the form we describe below, and that is correct, and

[6] She still has full control over the measurement station. In particular everything that Bob sends to the measurement station is considered to be in dishonest Alice's possession.

secure against Bob, can be attacked by dishonest Alice. That is, it is always possible for Alice to correctly guess Bob' bit C with sufficiently high probability. Dishonest Alice's cheating strategy in is given in Protocol 6.2.5.

In this section, all the random variables mentioned in Section 6.4.5, $X_1^n, \mathscr{I}, I_0, I_1, C, \ldots$ will be redefined in a more abstract manner

In order to prove our result we will forget about the quantum part of the OT protocol, and start directly in a scenario, in which Alice and Bob share from the start the type of correlation they would have had by running a preparation phase similar to Protocol 6.2.4.

In particular we will assume that the Preparation phase gives the following to Alice and Bob:

Honest Alice Alice gets a random bit string X_1^n with probability distribution $P_{X_1^n}$.

Honest Bob Bob gets a random subset $\mathscr{I} \subseteq [n]$ with probability distribution $P_{\mathscr{I}}$, and the string $X_{\mathscr{I}}$, whose bits are the bits of X_1^n that are indexed by $i \in \mathscr{I}$.

When one of the parties is dishonest we will assume they have the following additional information as input:

Dishonest Alice Dishonest Alice gets the same X_1^n as when she was honest, plus the sets $I_G, I_B \subseteq [n]$, which are sets of indices satisfying the following:
$I_G \cap I_B = \emptyset$ and $|I_G \cup I_B| = \gamma n$ for some $\gamma \in]0,1[$.
$\forall\, i \in I_G \cup I_B$

- **If** $i \in \mathscr{I}$ **then** $i \in I_G$ with probability $1/2(1+\mu)$ or $i \in I_B$ with probability $1/2(1-\mu)$.
- **If** $i \notin \mathscr{I}$ **then** $i \in I_G$ with probability $1/2(1-\mu)$ or $i \in I_B$ with probability $1/2(1+\mu)$.

γ represents the faction of rounds in which more than two photons have been emitted (we should have $\gamma \approx p_{\geq 2}/(1-p_0)$, the probability that more than two photons are emitted when at least one is emitted). $\mu \in]0,1]$ models Alice's probability of guessing Bob's basis conditioned on receiving several photons from Bob.

Note that this definition can be seen as first giving $I_G \cup I_B$ to Alice and then giving her I_G and I_B through the probabilistic process described above.

Dishonest Bob When Bob is dishonest we will assume that he holds a classical register K and a quantum register Q such that his min-entropy rate $\frac{H_{\min}(X_1^n|KQ)}{n}$ is smaller than the one of honest Bob.

Let M_{BA} be the random variable that describes the set of the messages sent from Bob to Alice, and M_{AB} be the random variable that describes the messages sent from Alice to Bob. The random variable composed of these two variables will be called M, in other words $M := (M_{AB}, M_{BA})$.

The output of honest Alice is $(S_0, S_1) := (f_0(X_1^n, M), f_1(X_1^n, M)) \in \{0,1\}^l \times \{0,1\}^l$, where f_0 and f_1 are two functions. The output of honest Bob is $(C, S_C) :=$

$(g(X_{\mathscr{I}},\mathscr{I},M),\tilde{g}(X_{\mathscr{I}},\mathscr{I},M))$, where g and $\tilde{g}$ are two other functions. These four functions model the operations that honest Alice and Bob have to perform according to the protocol they are running.

Before estimating Alice's cheating probability (see Theorem 6.4.20), we will need the following definition.

Definition 6.4.18. *Let $J \subseteq [n]$ be a set of indices. Let f_0, f_1 be the functions defined above. We will say that J stabilises a function f_a ($a \in \{0,1\}$) with respect to (w.r.t.) random string X_1^n and random variable M when the value (x_1^n, m) of random variable (X_1^n, M) is such that J stabilises f_a w.r.t. x_1^n and m. We will say that J stabilises the function f_a w.r.t. x_1^n and m if $x_{J^c} \mapsto f_a((x_{J^c}, x_J), m)$ is constant for all x_{J^c} s.t. $\Pr\big((X_1^n, M) = ((x_{J^c}, x_J), m)\big) \neq 0$, where (x_{J^c}, x_J) denotes the string composed of the bits x_J of and x_{J^c} at the positions corresponding to the sets J and J^c.*

Intuitively this definition captures the notion of a function f depending only on the values of the bits of X_1^n at positions indexed by the set $J \subseteq [n]$.

ASSUMPTIONS AND MAIN THEOREM

6

In this section we state the assumptions we make to prove our theorem and prove Theorem 6.4.20. Since we assume Alice is semi-honest her cheating strategy consists in making her guess on Bob's bit C using all the information she has collected during the protocol. Therefore we can consider that her cheating strategy is an algorithm she runs at the end of the protocol on all her data. The cheating strategy we use is described in Protocol 6.2.7. The basic idea of the protocol is the following. At the end of the protocol Alice has the two sets I_0 and I_1 that are correlated to bit C and set $\mathscr{I}$ in the following way. If $C = 0$ then $I_0 \subseteq \mathscr{I}$ and $I_1 \nsubseteq \mathscr{I}$. If $C = 1$ the situation is reversed (see previous section)[7]. In themselves, these sets do not reveal the value of bit C since Alice should not know anything about set $\mathscr{I}$. However, since there has been information leakage during the protocol, she does know something about set $\mathscr{I}$. She knows that indices in I_G are more likely to belong to $\mathscr{I}$ than the ones in I_B, and this allows her to guess with some probability which set I_0 or I_1 is a subset of $\mathscr{I}$, and therefore it allows her to guess the value of bit C. Let us state more precisely the assumptions we use to prove Theorem 6.4.20.

Let $\mathfrak{P}_F$ be the following statement: "$\exists F(\cdot,\cdot)$ such that $F(X_1^n, M) =: (I_0, I_1)$ where $I_0, I_1 \subseteq [n]$ are such that I_C stabilizes f_C but not f_{1-C} (w.r.t. (X_1^n, M)), and I_{1-C} stabilizes f_{1-C} but not f_C (w.r.t. (X_1^n, M))", where $C := g(X_1^n, \mathscr{I}, M)$."

If $\mathfrak{P}_F$ is true then one can define $\alpha \in]0,1]$ such that $|I_{1-C} \setminus I_C \cap (I_G \cup I_B) \cap \mathscr{I}| = (1-\alpha)|I_{1-C} \setminus I_C \cap (I_G \cup I_B)|$, *i.e.* α is the fraction of rounds in $I_{1-C} \setminus I_C \cap (I_G \cup I_B)$ that are not in $\mathscr{I}$.

Assumptions 6.4.19. *Let $I_0, I_1, C, M, X_1^n, \mathscr{I}, I_G, I_B, \alpha$, and μ be as defined above. Let $\delta \in]0, 1/2]$. Let $\kappa := \min\big(\big|I_0 \setminus I_1 \cap (I_G \cup I_B)\big|; \big|I_1 \setminus I_0 \cap (I_G \cup I_B)\big|\big)$. Let Ω_κ be the event: "$\kappa \geq 1$". We*

[7] They have to be correlated to C in this way for the OT protocol to be correct, and secure against dishonest Bob.

assume in Theorem 6.4.20 that:

$$\begin{cases} \mathfrak{P}_F \text{ is true,} \\ \\ \Pr(\Omega_\kappa) \text{ is non-negligible in } n, \end{cases} \tag{6.42}$$

Now we can state and prove our theorem that shows that Protocol 6.2.7 is a strategy that allows dishonest Alice to to cheat.

Theorem 6.4.20. *Let $I_0, I_1, C, M, X_1^n, \mathscr{I}, I_G, I_B, \alpha$, and μ be as defined above. Let $\delta \in]0, 1/2]$. Let $\kappa := \min\left(\left|I_0 \setminus I_1 \cap (I_G \cup I_B)\right|; \left|I_1 \setminus I_0 \cap (I_G \cup I_B)\right|\right)$. Let Ω_κ be the event: "$\kappa \geq 1$". Let P_{guess} be the maximum probability that Alice correctly guesses Bob's bit C.*

If Assumptions 6.4.19 are satisfied by the protocol run between Alice and Bob, and if this protocol is correct, and secure against dishonest Bob, then dishonest Alice's strategy presented in Protocol 6.2.7 allows Alice to guess C with probaility $P_{\text{guess}} = 1/2 + \text{adv}$, where adv *satisfies*

$$\text{adv} \geq \Pr\left(\Omega_\kappa\right) \times \alpha\mu. \tag{6.43}$$

We can also prove that $\alpha \geq 1/n$, which is not negligible in n.

Proof. In order to prove the theorem we will lower bound Alice's guessing probability P_{guess}, for a protocol satisfying Assumptions 6.4.19. In particular we want to show that P_{guess} is larger than $1/2$ by a non-negligible amount. Before doing that let us spell out important consequences of a protocol being correct and secure against Bob.

Because we assume that $\mathfrak{P}_F$ is true, the sets $(I_0, I_1) := F(X_1^n, M)$ are well defined. In order to get correctness we should have that $I_C \subseteq I$, and for having security against Bob it is necessary that $I_{1-C} \nsubseteq I$, where C is the bit held by honest Bob that Alice tries to guess. Let us call b the bit that corresponds to dishonest Alice's guess of Bob's bit C. We can then write,

$$\begin{aligned} P_{\text{guess}} = \Pr(b = C) &= \Pr(\Omega_\kappa)\Pr(b = C|\Omega_\kappa) + (1 - \Pr(\Omega_\kappa))\Pr(b = C|\neg\Omega_\kappa), && (6.44) \\ &\geq \Pr(\Omega_\kappa)\Pr(b = C|\Omega_\kappa) + (1 - \Pr(\Omega_\kappa))1/2. && (6.45) \end{aligned}$$

From Assumptions 6.4.19 we have that $\Pr(\Omega_\kappa)$ is not negligible. Intuitively, saying that $\Pr(\Omega_\kappa)$ is not negligible ensures that there has been information leakage during the quantum phase of the protocol. If $\Pr(\Omega_\kappa)$ were negligible we already know by Theorem 6.4.9 that a protocol like Protocol 6.2.4 would be secure. As a consequence, we will focus on computing $\Pr(b = C|\Omega_\kappa)$.

In Protocol 6.2.7, Alice chose uniformly at random an index $i_r \in I_r | I_{1-r} \cap (I_G \cup I_B)$ and check whether i_r ends up in I_G or I_B. The idea is that if $r = C$ the probability that i_r ends up in I_G is slightly higher than the one of ending up in I_B. If $r = 1 - C$ it biased towards ending up in I_B. Therefore if she outputs $b = r$ when $i_r \in I_G$, and outputs $b = 1 - r$ if $i_r \in I_B$ she will have a probability of guessing correctly bit C slightly higher than $1/2$, which is what we are trying to prove.

Note that the event Ω_κ depends on the "value" of the set $I_G \cup I_B$, but is completely independent on how $I_G \cup I_B$ is partitioned into the sets I_G and I_B. In particular the probability for a round in $I_G \cup I_B$ to be in I_G is independent of Ω_κ.

Let us now write Alice's guessing probability conditioned on Ω_κ, with r and i_r as defined by Protocol 6.2.7:

$$P_{\text{guess}|\Omega_\kappa} = \Pr(b = C|\Omega_\kappa) \tag{6.46}$$

$$= \Pr(r = C|\Omega_\kappa)\Pr(i_r \in I_G|r = C,\Omega_\kappa) + \Pr(r = 1-C|\Omega_\kappa)\Pr(i_r \in I_B|r = 1-C,\Omega_\kappa), \tag{6.47}$$

where r is a uniformly random bit chosen by Alice in Protocol 6.2.7. As a consequence, $\Pr(r = C|\Omega_\kappa) = \Pr(r = 1-C|\Omega_\kappa) = 1/2$. From the definition of I_G and I_B, and their independence from Ω_κ we get that,

$$\Pr(i_r \in I_G|r = C,\Omega_\kappa) = \Pr(i_r \in I_G|r = C) = 1/2(1+\mu), \tag{6.48}$$

$$\Pr(i_r \in I_B|r = 1-C,\Omega_\kappa) = \Pr(i_r \in I_B|r = 1-C) = 1 - 1/2\alpha(1-\mu) - 1/2(1-\alpha)(1+\mu). \tag{6.49}$$

Plugging this into the expression for $P_{\text{guess}|\Omega_\kappa}$ we get that:

$$P_{\text{guess}|\Omega_\kappa} = 1/2\big(1/2(1+\mu) + 1 - 1/2\alpha(1-\mu) - 1/2(1-\alpha)(1+\mu)\big) = 1/2(1+\alpha\mu). \tag{6.50}$$

As expected the probability that Alice correctly guesses the value of bit C is a bit higher than $1/2$.

Combining this with the fact that $\kappa \geq 1$ is true with probability $\Pr(\Omega_\kappa)$ leads to eq. (6.43). That is, Alice's overall probability of guessing correctly bit C is still slighly higher than $1/2$, namely is is higher than,

$$1/2 + \Pr(\Omega_\kappa) \times \alpha\mu.$$

As we stated earlier $I_{1-C} \nsubseteq \mathscr{I}$, meaning that at least one index in I_{1-C} is not in $\mathscr{I}$, and since $I_{1-C} \setminus I_C \cap (I_G \cup I_B)$ cannot be larger than the total length of the string X_1^n (which is obviously n), we must have $\alpha \geq 1/n$.

□

6.5. TECHNICAL DETAILS

6.5.1. WHY DOESN'T DISHONEST BOB GET ANY ADVANTAGE BY SELECTIVELY DISCARDING ROUNDS WHEN ALICE USES A PERFECT SINGLE PHOTON SOURCE?

In this section we explain why for our proof we can consider that we can simply evaluate the min-entropy bound of Lemma 6.4.5 as if Bob were honest in choosing which rounds he announces to be lost. In other words we explain why dishonest Bob can't get any advantage by selectively discarding rounds.

In Protocol 6.2.2, Alice sends n' BB84 states to Bob using a perfect single photon source. This, by purification of the states she sends, is equivalent as to Alice preparing n' EPR pairs, and sending half of each pairs to dishonest Bob, and randomly measuring

her halfs of EPR pairs in the X or Z basis. This allows us to delay Alice's measurements to the end of the preparation phase.

The bound we use for the min-entropy is independent of the details of the state. Indeed the bound works as follows. For any state ρ_{A^nE} (for some $n \in \mathbb{N}$), if Alice's measurements (modeled by the CPTP map $\mathcal{M}_{A_1^n \mapsto X_1^n}$) on the systems A_1^n (outputting bit string X_1^n) satisfy some condition (that is indeed satisfied when Alice randomly measures in the X or Z basis [22]), then $H_{\min}^{\epsilon}(X_1^n|E)_{\mathcal{M}(\rho)} \geq B(H_{\min}(A_1^n|E)_{\rho}/n) \cdot n$, where $B(\cdot)$ is some function that bounds the min-entropy rate.

Since the bounds applies to any state, one can then choose $\rho_{A_1^nE}$ to be the state of the protocol after that Bob (holding register $E = KQ$, where K is classical and Q is the quantum state in his memory) has stored quantum information and after he has announced which rounds are kept and which are not, but before Alice has measured. Using the bounded storage assumption ($\log\dim(Q) \leq D$) we can bound $H_{\min}(A_1^n|E)_{\rho} \geq -D$. This leads us to $H_{\min}^{\epsilon}(X_1^n|E)_{\mathcal{M}(\rho)} \geq B(-D/n) \cdot n$ as stated in Lemma 6.4.5. Note that this bound is evaluated on the state conditioned on Bob keeping some particular rounds, but the bound does not depend on the strategy he uses for choosing which rounds he keeps and which he discards.

For Protocol 6.2.4 the same reasoning apply. Indeed even though we use a different bound, the bound we use is also independent of the details states on which the entropy is evaluated.

6

6.5.2. PROOF OF LEMMA 6.4.13

In this section we will explain how the honest party $H \in \{A, B\}$ can use the decoy states in order to estimate a lower-bound L_{H1} on n_1^H. To do so we will use techniques inspired by [29]. In the following we will detail the analysis considering that Alice is honest. The case when Bob is honest follows the same structure.

First we can observe that Protocol 6.2.5 is equivalent to a virtual protocol where Alice first chooses the number k of photons she is sending according to a probability distribution p_k, and the encoding basis with probability p_θ, and only after the station reveals the measurement outcome o she chooses the signal intensity $a \in \{a_s, a_{d_1} \dots a_{d_q}\}$ according to probability distribution $p_{a|k}$ (this choice in independent from θ and outcome o). The probability distribution p_k and $p_{a|k}$ in the virtual protocol can be deduced from the distribution p_a, and $p_{k|a}$ of Protocol 6.2.5 via Bayes' rule.

As a consequence for any set $S_{k,o,\theta}^A$ of rounds where Alice has emitted k photons encoded in the basis θ ($\theta = 0$ for the standard basis, and $\theta = 1$ for the Hadamard basis) and the measurement station (or dishonest Bob) reported measurement outcome o (with $o \neq$ failure), each subset of $S_{k,o,\theta}^A$ corresponding to intensity a can be seen as a random sample of $S_{k,o,\theta}^A$. Therefore we can use (classical) random sampling theory to estimate L_{A1}, like Chernoff's bound for example. In particular we will use the following lemma proven in Ref. [29],

Lemma 6.5.1. *Let $X_1, \dots, X_n$ be n independent Bernoulli random variables such that $\Pr(X_i = 1) = p_i$, and let $X := \sum_i X_i$ and $\zeta := \mathbb{E}(X) = \sum_i p_i$. Let x be the observed outcome of X for a certain trial and $\Gamma := x - \sqrt{n/2 \ln(1/\epsilon)}$ for a certain $\epsilon > 0$. If $\varepsilon, \hat{\varepsilon} > 0$ are such that*

$(2\varepsilon^{-1})^{1/\zeta_L} \leq \exp(3/(4\sqrt{2}))^2$ *and* $(\hat{\varepsilon}^{-1})^{1/\zeta_L} < \exp(1/3)$ *then x satisfies,*

$$x = \zeta + \delta, \tag{6.51}$$

except with probability $\epsilon + \varepsilon + \hat{\varepsilon}$*, where* $\delta \in [-\Delta, \hat{\Delta}]$*, with* $\Delta := g(x, \varepsilon^4/16)$*,* $\hat{\Delta} := g(x, \hat{\varepsilon}^{3/2})$ *and* $g(x,y) := \sqrt{2x\ln(y^{-1})}$*. Here* $\varepsilon(\hat{\varepsilon})$ *denotes the probability that* $x < \zeta - \Delta$ $(x > \zeta + \hat{\Delta})$*.*

This lemma is a variation of the Chernoff's bound, where the bounds on the fluctuations $\Delta(\hat{\Delta})$ do not depend on the expectation value $\zeta := \mathbb{E}(X)$ of the random variable X, but only on the observed value x of X (and the epsilons).

Let $S^A_{k,o,\theta}$ be the set of rounds as defined above, and let $X^a_{i|k,o,\theta}$ be 1 if the i^{th} element of $S^A_{k,o,\theta}$ corresponds to an emission of a state (from honest Alice) with intensity a, and 0 otherwise. Let

$$X^a_{o,\theta} = \sum_k \sum_{i=1}^{|S^A_{k,o,\theta}|} X^A_{i|o,k,\theta}, \tag{6.52}$$

with $\zeta^a_{o,\theta} := \mathbb{E}(X^a_{o,\theta}) = \sum_k p_{a|k}\, |S^A_{k,o,\theta}|$. Let $x^a_{o,\theta}$ be an observed outcome of $X^a_{\theta,o}$. Then applying Lemma 6.5.1 we have that for some $(2\varepsilon^{-1})^{1/\Gamma^a_{o,\theta}} \leq \exp(3/(4\sqrt{2}))^2$, $(\hat{\varepsilon}^{-1})^{1/\Gamma^a_{o,\theta}} < \exp(1/3)$ with

$$\Gamma^a_{o,\theta} = x^a_{o,\theta} - \sqrt{\sum_a x^a_{o,\theta}/2\ln(1/\epsilon)}, \tag{6.53}$$

the following must be satisfied:

$$x^a_{o,\theta} = \sum_k p_{a|k} |S^A_{k,o,\theta}| + \delta_{a,o,\theta}, \tag{6.54}$$

except with probability $\epsilon + \varepsilon + \hat{\varepsilon}$, where $\delta_{a,o,\theta} \in [\Delta_{a,o,\theta}, \hat{\Delta}_{a,o,\theta}]$, with $\Delta_{a,o,\theta} = g(x^a_{o,\theta}, \varepsilon^4/16)$ and $\hat{\Delta}_{a,o,\theta} = g(x^a_{o,\theta}, \hat{\varepsilon}^{3/2})$.

Since $n^A_1 = \sum_{o,\theta} n^A_{1|o,\theta}$ it is enough to find a lower bound on $n^A_{1|o,\theta}$ for all values of (o,θ) in order to find a lower bound L_{A1} on n^A_1. Then using concentration bounds one can write that for each value of (o,θ)

$$n^A_{1|o,\theta} \geq p_{a_s|k=1} |S^A_{1,o,\theta}| - g(p_{a_s|k=1}|S^A_{1,o,\theta}|, \epsilon_1), \tag{6.55}$$

except with probability ϵ_1. For a fixed value of (o,θ) one can find a lower-bound on $|S^A_{1,o,\theta}|$ by minimizing $|S^A_{1,o,\theta}|$ under the constraints given by eq. (6.54). This can be solved by using linear programming [30], or we can use a simplified version of this reasoning to find analytical (but looser) bounds. This is what we will be doing in the following section.

SIMPLE ANALYTICAL BOUND

In this section we propose to find a simple analytical bound on n^A_1, using the reasoning and methods of the previous section. To do so we will minimize $|S^A_{1,o,\theta}|$ for a fixed value

for (o,θ). Moreover we will restrict ourselves to the use of only 2 decoy states and one signal state, *i.e.* $a \in \{a_s, a_{d_1}, a_{d_2}\}$.

In the previous section we have split the rounds into many sets $S_{k,o,\theta}$ (1 set for each value of k). Here we split the round into two sets $S^A_{1,o,\theta}$ and $S^A_{\geq 2,o,\theta}$.

With this in mind we can rewrite equation (6.54) as the following system of inequalities,

$$\begin{cases} x^{a_{d_1}}_{o,\theta} + \Delta_{a_{d_1},o,\theta} \geq p_{a_{d_1}|k=1} \cdot |S^A_{1,o,\theta}| + p_{a_{d_1}|k\geq 2} \cdot |S^A_{\geq 2,o,\theta}| \\ x^{a_{d_1}}_{o,\theta} - \hat{\Delta}_{a_{d_1},o,\theta} \leq p_{a_{d_1}|k=1} \cdot |S^A_{1,o,\theta}| + p_{a_{d_1}|k\geq 2} \cdot |S^A_{\geq 2,o,\theta}| \\ x^{a_{d_2}}_{o,\theta} + \Delta_{a_{d_2},o,\theta} \geq p_{a_{d_2}|k=1} \cdot |S^A_{1,o,\theta}| + p_{a_{d_2}|k\geq 2} \cdot |S^A_{\geq 2,o,\theta}| \\ x^{a_{d_2}}_{o,\theta} - \hat{\Delta}_{a_{d_2},o,\theta} \leq p_{a_{d_2}|k=1} \cdot |S^A_{1,o,\theta}| + p_{a_{d_2}|k\geq 2} \cdot |S^A_{\geq 2,o,\theta}| \end{cases} \tag{6.56}$$

Each of the four inequalities represents half a space delimited by a straight line in $\mathbb{R}^2$. The two first inequalities define a region delimited by two parallel lines, and the two last inequalities define another region delimited by two other parallel lines. The set of four inequalities is then the intersection of these two regions, see Fig. 6.6. Since we are optimizing a linear function with linear constraints the minimum is reached for one of the extreme points of this region. Each of these points corresponds to the solution of the system of equations formed by two of the inequalities from (6.56) (one for decoy state 1 and one for decoy state 2) by changing symbols $\leq, \geq$ into $=$. Since there are two equations for each decoy state, the number of extreme points must be 4. They can be found analytically by solving this system of equations. In the end the lower-bound L_{A1} is given by,

$$L_{A1} = \sum_{o,\theta} \left[p_{a_s|k=1} \, |S_{1,o,\theta}|_{\min} - g(p_{a_s|k=1} \, |S_{1,o,\theta}|_{\min}, \epsilon_1) \right], \tag{6.57}$$

where $|S_{1,o,\theta}|_{\min}$ is given by,

$$|S_{1,o,\theta}|_{\min} = \min(V_1, V_2, V_3, V_4), \tag{6.58}$$

with

$$V_1 = \frac{p_{a_{d_1}|k\geq 2}(x^{a_{d_2}}_{o,\theta} + \Delta_{a_{d_2},o,\theta}) - p_{a_{d_2}|k\geq 2}(x^{a_{d_1}}_{o,\theta} + \Delta_{a_{d_1},o,\theta})}{p_{a_{d_1}|k=1} p_{a_{d_2}|k\geq 2} - p_{a_{d_1}|k\geq 2} p_{a_{d_2}|k=1}} \tag{6.59}$$

$$V_2 = \frac{p_{a_{d_1}|k\geq 2}(x^{a_{d_2}}_{o,\theta} - \hat{\Delta}_{a_{d_2},o,\theta}) - p_{a_{d_2}|k\geq 2}(x^{a_{d_1}}_{o,\theta} + \Delta_{a_{d_1},o,\theta})}{p_{a_{d_1}|k=1} p_{a_{d_2}|k\geq 2} - p_{a_{d_1}|k\geq 2} p_{a_{d_2}|k=1}} \tag{6.60}$$

$$V_3 = \frac{p_{a_{d_1}|k\geq 2}(x^{a_{d_2}}_{o,\theta} + \Delta_{a_{d_2},o,\theta}) - p_{a_{d_2}|k\geq 2}(x^{a_{d_1}}_{o,\theta} - \hat{\Delta}_{a_{d_1},o,\theta})}{p_{a_{d_1}|k=1} p_{a_{d_2}|k\geq 2} - p_{a_{d_1}|k\geq 2} p_{a_{d_2}|k=1}} \tag{6.61}$$

$$V_4 = \frac{p_{a_{d_1}|k\geq 2}(x^{a_{d_2}}_{o,\theta} - \hat{\Delta}_{a_{d_2},o,\theta}) - p_{a_{d_2}|k\geq 2}(x^{a_{d_1}}_{o,\theta} - \hat{\Delta}_{a_{d_1},o,\theta})}{p_{a_{d_1}|k=1} p_{a_{d_2}|k\geq 2} - p_{a_{d_1}|k\geq 2} p_{a_{d_2}|k=1}}. \tag{6.62}$$

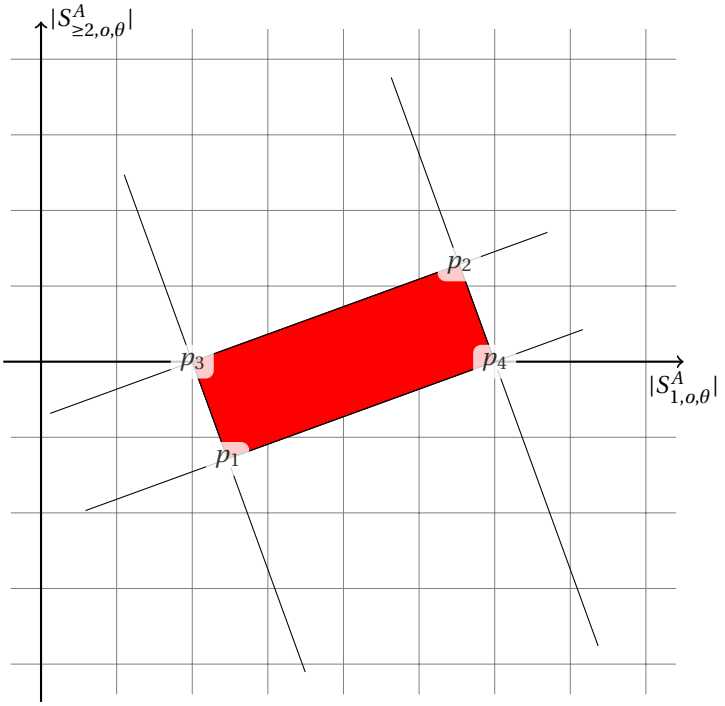


Figure 6.6: Each of the line is defined by one of the four inequalities in (6.56). The red region is the set of points that satisfies the four linear constraints from (6.56). Since we are optimizing a linear function with linear constraints, by linear programming we know that the optimum is reached for one of the four extreme points p_1, p_2, p_3, p_4, which are at the intersection of the lines. In the particular case of this figure $\min |S^A_{1,o,\theta}|$ is reached in p_3.

6.5.3. FORMAL SECURITY DEFINITIONS FOR OT AND BC

In this section you can find the formal definitions for Randomized String Commitment and for Randomized 1-out-2 (l,ϵ)-Oblivious String Transfer. These definitions come directly from Refs. [13].

Remark 6.5.2 (on the abort events)**.** *The careful reader will see that the definitions below do not mention any abort event. In fact our protocols specify the action a party has to take when he wants to abort. In particular we ask the aborting party to output uniformly random outcomes, so that even when aborting the security definitions are satisfied.*

Definition 6.5.3 (Randomized String Commitment)**.** *Let τ_R denote the maximally mixed state on a register R.*

An (l,ϵ)-Randomized String commitment scheme is a protocol between Alice and Bob that satisfies the following three properties.

Correctness *When both parties are honest, then there exists a state $\sigma_{C_1^l C_1^l F}$, called the ideal state that is defined as:*

- $\sigma_{C_1^l F} := \tau_{C_1^l} \otimes |accept\rangle\langle accept|_F$,
- *The real state produced by the protocol $\rho_{C_1^l \tilde{C}_1^l F}$ is ϵ-close to the ideal state $\sigma_{C_1^l C_1^l F}$,*

$$\rho_{C_1^l \tilde{C}_1^l F} \approx_\epsilon \sigma_{C_1^l C_1^l F}.$$

Security for Alice (against dishonest Bob) *When Alice is honest, Bob is ignorant about C_1^l before the Open phase:*

$$\rho_{C_1^l B} \approx_\epsilon \tau_{C_1^l} \otimes \rho_B.$$

The protocol is then said to be ϵ-hidding.

Security for Bob (against dishonest Alice) *After the Commit phase and before the Open phase, there exists an ideal state $\sigma_{C_1^l AB}$ such that for any Open algorithm, describe by the CPTP maps $\mathcal{O}_{\mathcal{AB}}$, in which Bob is honest, we have:*

- *Bob almost never accepts $\tilde{C}_1^l \neq C_1^l$:*
  for $(\mathbb{1}_{C_1^l} \otimes \mathcal{O}_{AB})(\sigma_{C_1^l AB})$ we have $\Pr(\tilde{C}_1^l \neq C_1^l \text{ and } F = accept) \leq \epsilon$.
- *The real state produced by the commitment phase is close to the ideal state:*

$$\rho_{AB} \approx_\epsilon \sigma_{AB}.$$

The protocol is then said to be ϵ-binding.

Definition 6.5.4 (Randomized 1-out-2 (l,ϵ)-Oblivious String Transfer (OST))**.**
Let τ_R denote the maximally mixed state on register R.

A fully randomized 1-out-2 (l,ϵ)-Oblivious String Transfer scheme is a protocol between two parties, Alice and Bob, that satisfies the following three conditions.

Correctness *If both parties are honest there exists an ideal state $\sigma_{S_0 S_1 C S_C}$, where $S_1, S_1 \in \{0,1\}^l$ and $C \in \{0,1\}$, such that:*

- *The distribution over S_0, S_1 and C is uniform:*

$$\sigma_{S_0 S_1 C} = \tau_{S_0} \otimes \tau_{S_1} \otimes \tau_C \tag{6.63}$$

- *The real state ρ produced by the protocol is ϵ-close to the ideal state:*

$$\rho_{S_0 S_1 C \hat{S}_C} \approx_\epsilon \sigma_{S_0 S_1 C S_C} \tag{6.64}$$

Security for Bob *If Bob is honest, there exists an ideal state $\sigma_{A S_0 S_1 C}$ such that:*

- *Alice is ignorant about C:*

$$\sigma_{A S_0 S_1 C} = \sigma_{A S_0 S_1} \otimes \tau_C. \tag{6.65}$$

- *The real state ρ produced by the protocol is close to the ideal state:*

$$\rho_{A C \hat{S}_C} \approx_\epsilon \sigma_{A C S_C} \tag{6.66}$$

Security for Alice *If Alice is honest, there exists an ideal state $\sigma_{S_0 S_1 B C}$ such that:*

- *Bob is ignorant about S_{1-C}:*

$$\sigma_{S_0 S_1 B C} = \sigma_{S_C B C} \otimes \tau_{S_{1-C}}. \tag{6.67}$$

- *The real state ρ is close to the ideal state:*

$$\rho_{S_0 S_1 B} \approx_\epsilon \sigma_{S_0 S_1 B}. \tag{6.68}$$

REFERENCES

[1] J. Kaniewski and S. Wehner, *Device-independent two-party cryptography secure against sequential attacks,* New Journal of Physics **18**, 055004 (2016).

[2] N. Aharon, S. Massar, S. Pironio, and J. Silman, *Device-independent bit commitment based on the chsh inequality,* New Journal of Physics **18**, 025014 (2016).

[3] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, *Fully distrustful quantum bit commitment and coin flipping,* Phys. Rev. Lett. **106**, 220501 (2011).

[4] J. Ribeiro, L. P. Thinh, J. m. k. Kaniewski, J. Helsen, and S. Wehner, *Device independence for two-party cryptography and position verification with memoryless devices,* Phys. Rev. A **97**, 062307 (2018).

[5] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems,* Phys. Rev. A **74**, 022313 (2006).

[6] S. Sajeed, I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, *Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing,* Phys. Rev. A **91**, 032326 (2015).

[7] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution,* Phys. Rev. Lett. **108**, 130503 (2012).

[8] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, *Experimental measurement-device-independent quantum key distribution,* Phys. Rev. Lett. **111**, 130502 (2013).

[9] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, *High-rate measurement-device-independent quantum cryptography (article) author,* Nature Photonics **9**, 397 EP (2015).

[10] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, *Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution,* Phys. Rev. Lett. **112**, 190503 (2014).

[11] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, *Measurement-device-independent quantum key distribution over 200 km,* Phys. Rev. Lett. **113**, 190501 (2014).

[12] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, *Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits,* Phys. Rev. A **88**, 052303 (2013).

[13] R. Konig, S. Wehner, and J. Wullschleger, *Unconditional security from noisy quantum storage,* IEEE Transactions on Information Theory **58**, 1962 (2012).

[14] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner, *Experimental implementation of bit commitment in the noisy-storage model,* Nature Communications **3**, 1326 (2012), arXiv:1205.3331 [quant-ph] .

[15] H.-K. Lo, X. Ma, and K. Chen, *Decoy state quantum key distribution,* Phys. Rev. Lett. **94**, 230504 (2005).

[16] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, *Implementation of two-party protocols in the noisy-storage model,* Phys. Rev. A **81**, 052336 (2010).

[17] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, Advances in Cryptology — CRYPTO '91: Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 1992) Chap. Practical Quantum Oblivious Transfer, pp. 351–366.

[18] S. Fehr and C. Schaffner, Theory of Cryptography, edited by O. Reingold (Springer Berlin Heidelberg, Berlin, Heidelberg, 2009) pp. 350–367.

[19] R. Gallager, *Low-density parity-check codes,* IRE Transactions on Information Theory **8**, 21 (1962).

[20] J. Wullschleger, Advances in Cryptology - EUROCRYPT 2007, edited by M. Naor (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) pp. 555–572.

[21] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner, Advances in Cryptology - CRYPTO 2007, edited by A. Menezes (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) pp. 360–378.

[22] F. Dupuis, O. Fawzi, and S. Wehner, *Entanglement sampling and applications,* IEEE Transactions on Information Theory **61**, 1093 (2015).

[23] W. Hoeffding, *Probability inequalities for sums of bounded random variables,* Journal of the American Statistical Association **58**, 13 (1963), https://amstat.tandfonline.com/doi/pdf/10.1080/01621459.1963.10500830 .

[24] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, *An experimental implementation of oblivious transfer in the noisy storage model,* Nature Communications **5**, 3418 (2014), arXiv:1308.5098 [quant-ph] .

[25] R. Renner and S. Wolf, Advances in Cryptology - ASIACRYPT 2005: 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, 2005. Proceedings (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005) pp. 199–216.

[26] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information,* IEEE Transactions on Information Theory **57**, 5524 (2011).

[27] N. H. Y. Ng, M. Berta, and S. Wehner, *Min-entropy uncertainty relation for finite-size cryptography,* Phys. Rev. A **86**, 042315 (2012).

[28] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition property,* IEEE Transactions on Information Theory **55**, 5840 (2009).

[29] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, *Finite-key analysis for measurement-device-independent quantum key distribution,* Nature Communications **5**, 3732 EP (2014).

[30] R. J. Vanderbei, Linear Programming, Vol. 196 (Springer US, 2014).

7

CONCLUSION

This is a concluding chapter summarizing the scientific and technical of this thesis. We also provide an outlook of the possible future research.

7.1. SUMMARY OF RESULTS

In this thesis we have proven security in the of different protocols in various flavours of the device-independent settings, with a specific focus on two-party cryptography protocols and key distribution/agreement protocols.

- We have improved security of device independent (DI) two-party cryptography in the IID settings, by using a completely different proof techniques as compare to previously known results. In particular, our results shows that an adversary needs at least twice as quantum much memory in order to cheat as compare to what previous results showed. This statement can be reversed as follows. For the same security (against the same adversary) our proof shows that one needs to run the protocol with half as many rounds as compare to previous results.

- We have propose a new protocol for DI Conference Key Agreement and proved its security. This new protocols reduces communication complexity of protocols based on multiple use of DI Quantum Key Distribution protocols by the use of GHZ states instead of Bell pairs. We compare the key rate of the two approaches. In some network architecture our mixing the two approach can be beneficial in terms of key rate, and in terms of the quantum resources available in a network.

- We have optimized the key rate of existing DI Quantum Key Distribution protocols, and compare the key rate such a protocol can achieve when one assume the devices to be IID as compare to the full general case. We also "benchmark" different experiment platforms on which a DI Quantum Key Distribution experiment could be performed, and see how far each of these platforms is to allow the realization of such experiment.

- We have explored two-party cryptography in the Measurement-Device Independent (MDI) settings. In particular we proposed protocols for Bit Commitment and Oblivious Transfer and proved their security when the party use a perfect single photon source. Surprisingly we find that, when the single photon source is not perfect, some class of protocol for Oblivious Transfer cannot be secure in the MDI settings. One of the main interest of working in the MDI scenario compare to the full DI scenario, is that usually protocols in the former scenario are more efficient than in the latter, while providing with good security guarantees in practice.

We hope that we have contributed to close the gap between theoretical security statements and practical security for all the protocols based on the cryptographic primitives mentioned in this thesis.

7.2. OUTLOOK

In this section we will discuss some possible extension of the work performed in this thesis.

- **Can the impossibility result proven in Chapter 6 be generalized?** Answering this question would be a direct extension of the work presented in Chapter 6. If the

answer to this question is yes, then one can ask how general this impossibility can be? These questions have obvious practical implication, but they also have more fundamental implications. Indeed in the quantum realm, Bit Commitment and Oblivious Transfer are known to be equivalent [1] in opposition to classical realm in which they are not. If this impossibility result can indeed be generalized, it shows that there is something fundamentally different between the MDI setting and the trusted settings.

- **Can we improve further the lower bounds on the size of the memory required for an adversary to cheat in a DI two-party cryptography protocol?** Previous result showed (under the IID-Assumption) that there is a DI two party cryptography protocol secure against an adversary holding at most $q \leq 0.22n$ qubits of memory (where n is the number of qubits sent in the protocol). In Chapter 3 we improve this and show that the same protocol is in fact secure as long as the adversary holds at most $q \leq 0.45n$ qubits of memory. However we do not reach yet the bounds of the trusted device scenario in which it has been proven that analogous protocols are secure as long as the adversary holds at most $q \leq n - \mathcal{O}(\log(n))$ [2]. Closing the gap between the bounds proven in the DI scenario and the bounds proven in the trusted device scenario would make DI protocols more efficient.

- **Explore composability of DI two-party cryptography protocols.** The security definitions we have used in this thesis do not necessarily guarantee security in all contexts in which one may wish to use these protocols. Some work in this direction have been made [3], however these proofs only apply to the trusted device model. It is not clear how these composability results can generalize to the DI model. In particular it is known that even for QKD, usual composability results are invalid in the DI model [4] when the devices are re-used in an other protocol.

- **Use computational assumption in combination with the Noisy Quantum Storage Model in order to improve security of two-party cryptography.** Computational assumption often have the problem that, if the adversary get extra computational power after the execution of the protocol, it can then break security of this protocol. The Noisy Quantum Storage Model solves this problem. The security for two party cryptography in this model is everlasting, meaning that if the memory assumption were true during the execution of the protocol then no gain in power after the execution will ever allow the adversary to break security. However one might asks whether in the far future the Noisy Quantum Storage Model will still be valid. Indeed if in the future quantum memory becomes cheap and reliable one would expect an adversary to hold a very big and good memory. If one wants to enforce security in this scenario then the communication complexity of the protocol would make them very inefficient. One way of addressing this question might be to combine the Noisy Quantum Storage Model with computational assumptions. The computational assumption would protect the protocol for a sufficiently long time Δt, for example one or two years, after what we consider that the state stored in the adversary's memory has decohered. This would force the adversary to store a state for a long time, while the computational assumption only need to hold for this times Δt. Very few results have been established in that direction, but

we can still mention [1] in which it is proven that quantum protocol for two party cryptography can be realised under some computational assumption.

REFERENCES

[1] I. Damgård, S. Fehr, C. Lunemann, L. Salvail, and C. Schaffner, Annual International Cryptology Conference (2009) pp. 408–427.

[2] F. Dupuis, O. Fawzi, and S. Wehner, *Entanglement sampling and applications,* IEEE Transactions on Information Theory **61**, 1093 (2015).

[3] D. Unruh, Advances in Cryptology – EUROCRYPT 2011, edited by K. G. Paterson (Springer Berlin Heidelberg, Berlin, Heidelberg, 2011) pp. 467–486.

[4] J. Barrett, R. Colbeck, and A. Kent, *Memory attacks on device-independent quantum cryptography,* Phys. Rev. Lett. **110**, 010503 (2013).