Device independence for two-party cryptography and position verification with memoryless devices

Ribeiro, Jérémy; Lê, Thinh; Kaniewski, Jed; Helsen, Jonas; Wehner, Stephanie

DOI
10.1103/PhysRevA.97.062307

Publication date
2018

Document Version
Publisher's PDF, also known as Version of record

Published in
Physical Review A

Citation (APA)

Important note
To cite this publication, please use the final published version (if applicable).
Please check the document version above.

Copyright
Other than for strictly personal use, it is not permitted to download, forward or distribute the text or part of it, without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license such as Creative Commons.

Takedown policy
Please contact us and provide details if you believe this document breaches copyrights.
We will remove access to the work immediately and investigate your claim.
Device independence for two-party cryptography and position verification with memoryless devices

Jérémy Ribeiro,1 Le Phuc Thinh,1,2 Jędrzej Kaniewski,1,2,3 Jonas Helsen,1 and Stephanie Wehner1
1QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands
2Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543
3Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen, Denmark

(Received 1 May 2018; published 5 June 2018)

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 work we improve the device-independent security proofs of Kaniewski and Wehner [New J. Phys. 18, 055004 (2016)] 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 Kaniewski and Wehner [New J. Phys. 18, 055004 (2016)], security can be attained for any violation of the Clauser-Holt-Shimony-Horne inequality.

DOI: 10.1103/PhysRevA.97.062307

I. INTRODUCTION

Quantum communication has demonstrated its usefulness for quantum cryptography far beyond quantum key distribution (QKD). One domain is two-party cryptography (2PC), whose goal is to allow two parties Alice and Bob to solve joint tasks, while protecting an honest party against the actions of a malicious one. Well-known examples of such tasks are oblivious transfer [1], bit commitment, secure identification, and private information retrieval.

Another interesting application is position-based cryptography (PBC) whose goal is to use the geographical location of an entity as its (only) credential. At the heart of these is the task of position-verification (PV) where a person wants to convince the (honest) verifiers that she is located at a particular location. Quantum protocols for PV that make use of quantum communication to enhance the security have been proposed [2–6]. We will refer to such protocols as quantum position verification (PV).

Unfortunately, one cannot achieve secure 2PC and PV without making assumptions on the power of the adversary, even using quantum communication [4,7,8]. This is in stark contrast to QKD where security against an all-powerful adversary (obeying the laws of physics) is attainable. The reason can be traced back to a key difference between the two scenarios: While in QKD Alice and Bob can cooperate to check on the actions of the eavesdropper, in 2PC they do not trust each other and need to fend for themselves.

Nevertheless, due to the practical importance of 2PC one is willing to make assumptions in order to achieve security. Classically, one often relies on computational hardness assumptions such as the difficulty of factoring large numbers. However, as technology progresses the validity of such assumptions diminishes: It has been proven that factoring can be efficiently done on a quantum computer. Most significantly, an adversary can retroactively break the security of a past execution of a cryptographic protocol [9]. It turns out, however, that security of cryptographic systems can also be achieved from certain physical assumptions [10].

The advantage of these comes from the fact that physical assumptions only need to hold during the course of the protocol. That is, even if the assumption is invalidated at a later point in time, security is not compromised.

If we allow quantum communication, one possible physical assumption is the bounded quantum-storage model [11,12], and more generally, the noisy-storage model [13–15]. 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 $r \leq n - O(\log_2 n)$ [14], which is essentially optimal since no protocol can be secure if $r \geq n$ [8,16]. 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 [17,18]. It is known that the noisy-storage model allows protocols for tasks such as oblivious transfer, bit commitment, as well as position-based cryptography [2–6].

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, even if we only have limited knowledge of the quantum devices. Chiefly,
we assume that the quantum devices function as black boxes, into which we can only give a classical input, and record a classical output. The classical input indicates the choice of a measurement that we would wish to perform, although we are not guaranteed that the device actually performs this measurement. The classical output can be understood as the outcome of that measurement. The classical processing itself is assumed to be trusted. This idea of imagining black box devices is known as device-independent (DI) quantum cryptography [19–22]. There is a large body of work in DI QKD (see, e.g., [21,23,24]), but in contrast there is hardly any work in DI 2PC. A protocol has been proposed by Silman [25] 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 [26], and for one-sided DI QKD in [5].

Achieving DI security for 2PC [27] and PV presents us new 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 paper, we present a method for improving the device-independent security of two-party cryptography presented in [27] and add the device-independent analysis of position verification. We accomplish that by first reusing the device-independent model of [27] (in particular they also use the memoryless device assumption for Alice’s devices), 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 [28]. We then follow their reduction of the security of DI-WSE onto bounding the cheating probability on a “guessing game” (see Sec. IC).

In order to analyze the bound on the probability of winning the “guessing game” we developed new techniques. The previous analysis [27] permitted one to prove a bound on the cheating probability proportional to the dimension of the adversary’s quantum storage (see Table I). 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 anticommutator 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 I). We do not know if our new bound is optimal; we know, however, that the bound must satisfy $r \lesssim 1$. We would like to highlight the fact that finding an optimal bound is highly nontrivial: even in the trusted scenario, it took several years to go from the first security proof for WSE [15] to a tight bound on the adversary memory size [14], 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 I). While the adversary can be fully general during the course of the protocol, we assume in this work that the devices he prepared earlier are memoryless, 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 i.i.d. devices (which stands for independent and identically distributed).

<table>
<thead>
<tr>
<th></th>
<th>[27]</th>
<th>This paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>i.i.d. assumption on Alice’s devices</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bound on $P_{\text{guess}}$ [cf. (1)]</td>
<td>$d\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1 + \epsilon}{1 - \epsilon}}\right)^n$</td>
<td>$(1 - o(1)) \cdot \sqrt{\left(\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1 + \epsilon}{1 - \epsilon}}\right)^n}$.</td>
</tr>
<tr>
<td>Memory size $r := \log_2(d)$ (in qubits) for which security can be achieved for a maximal Bell violation</td>
<td>$r \lesssim 0.22n$</td>
<td>$r \lesssim 0.45n$</td>
</tr>
<tr>
<td>Security for PV</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Adversary memory</td>
<td>Reduction to classical adversary</td>
<td>Deals with the memory directly</td>
</tr>
<tr>
<td>Jordan’s Lemma</td>
<td>Not used</td>
<td>Reduction of dimensionality thanks to Jordan’s Lemma</td>
</tr>
<tr>
<td>Absolute effective anticommutator</td>
<td>Used</td>
<td>Used</td>
</tr>
</tbody>
</table>
A. Weak string erasure

To analyze 2PC protocols, we focus on a simpler primitive called weak string erasure (WSE) [15]. 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 \( x \in \{0,1\}^n \) and Bob holds a random substring \( x_T \) of \( x \) where \( T \) is a random subset of \( \{1,2,\ldots,n\} \). WSE is secure for honest Bob if Alice cannot guess the set \( T \) 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 \( X = \hat{X} \) is low, where \( X \) is the random variable corresponding to Alice’s output measurement and \( \hat{X} \) is the random variable corresponding to Bob’s guess, that is,

\[
\exists \alpha > 0 : \quad H_{\min}(X|\text{Bob}) \geq \alpha n
\]

\[
\Leftrightarrow \exists \alpha > 0 : \quad P_{\text{guess}}(X|\text{Bob}) = 2^{-H_{\min}(X|\text{Bob})} \leq 2^{-\alpha n}. \quad (1)
\]

For a more formal security definition of \((\alpha, \epsilon)\) WSE see [15].

One possible implementation of WSE [15] 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 [29] 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 \( \theta \), 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 measurements were done in the good basis and which were done in the wrong one. After Alice and Bob have waited for a duration \( \Delta t \), Alice sends \( \theta \) to Bob. Bob can now compare \( \theta \) with \( \theta' \) and deduce the set \( I := \{ k \in \{0,\ldots,n\} : \theta_k = \theta'_k \} \) 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 \((I, x_I)\), where \( x_I \) is the substring of \( x \) corresponding to the set \( I \).

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 2 in Sec. II A, 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 i.i.d. 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 \( \hat{\rho}_{AB} \) be the state after the execution of WSE, where \( B := (I, x_I) \) (\( X \) is the random variable for the bit string \( x \) and \( x_I \) is the random variable for the substring \( x_I \) 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 \( \rho_{AX} \) such that \( \tau_{AX} = \tau_{A'X} \otimes \tau_{T} \) and that for any given set \( I \), \( \tau_{A'X,I} = \rho_{AX,I} \). We leave open the question of whether this definition is strong enough to get any composability statement in the device-independent setting [30].

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 \( \rho_{AB} = \sigma_{AB}^n \) (i.i.d. assumption), where \( \rho_{AB} \) is an unknown but fixed state, measures the \( \rho_A \) part to get \( x \in \{0,1\}^n \) and sends the \( \rho_B \) part to Bob. Bob can proceed to any kind of operation not necessarily i.i.d. on \( \rho_B \) and stores the outcome for the duration \( \Delta t \) to get a cq state \( \rho_{KB} \). When he receives \( \theta \) from Alice he performs a general measurement on his cq state which produces the guess \( \hat{x} \). Bob’s cheating is considered successful if \( \hat{x} = x \). However, as his quantum storage is assumed to be bounded (or noisy) which imposes a restriction on the possible state Bob can hold, and permits us to show the following.

(1) 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 [27] where security was shown for \( r \lesssim 0.22n \).

To establish this result we proceeded in a similar way as in [27], 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 [27] is that we introduce new techniques to analyze this guessing game (more details about the guessing game are provided in Sec. I C). 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 round of the protocol), while [27] shows security for \( r \lesssim 0.22n \).

The detailed Weak String Erasure protocol is presented in Sec. III A (Protocol 10). The precise formal result is presented in the Corollary 12 in Sec. III A.

B. 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 one to prove whether this is true. The protocol is then secure if the probability that one or more dishonest provers impersonate a 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, we can implement the protocol as follows. \( V_1 \) prepares \( n \) EPR entangled pairs, measures half of all the pairs in some bases \( \theta \in \{0,1\}^n \) to get \( x \in \{0,1\}^n \), and sends the other half to the prover \( P \). \( V_2 \) sends \( \theta \) 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 \( \theta \) to get \( x \) and sends it back to both verifiers. The verifiers then 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 $\Delta t$, then the execution of the protocol is considered successful.

The honest execution of the device-independent version of the protocol is the same except that $V_j$ starts with a Bell test of his main device using the testing device. Then he executes the exact same steps as described above. The detailed protocol is given as Protocol 17 in Sec. III B.

In the dishonest scenario, a single prover cannot cheat because he cannot reply on time to both verifiers. More than one dishonest prover is required and, without loss of generality, 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 [4]. 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. We will work in this framework of cheating provers.

Note that to make the security reduction from PV to WSE we use a model introduced in [6] 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. 5 in Appendix C which would lead to known attacks.

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

1. 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 20, and this follows from a technical result informally presented in the next section.

C. Methods

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. 1). 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 in the bases $\theta \in \{0, 1\}^n$. The other part $\rho_B$ 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 $\rho_B$ 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 $\hat{x} = x$.

FIG. 1. Alice is in possession of two devices prepared by Bob. The “main device” permits Alice to prepare a bipartite state $\rho_{AB}$ and measure the $\rho_A$ part of it according to a list of bases $\theta \in \{0, 1\}^n$. The “testing device” measures according to a list of bases $\xi \in \{0, 1\}^n$. These two devices are assumed to be memoryless (or i.i.d.). 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 $\rho_{AB} = \sigma_{AB}^0$ (the tensor form follows the i.i.d. assumption), one part $\rho_A$ 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 $\rho_B$ 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 $\hat{x} = x$.

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 $\theta$ and then he can measure his system in those bases. As a first step towards security against fully uncharcterized devices, we assume for now that all devices used by Alice are memoryless or i.i.d., 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 $\epsilon : = \frac{1}{2}\sqrt{8 - 3S}$ on a quantity we call the effective absolute anticommutator of Alice’s measurement denoted $\epsilon_+$ [27], where $S$ is the left-hand side of the CHSH inequality. Since $\epsilon_+$ is always larger than the effective anticommutator, one can show that it gives rise to strong uncertainty relations [31].

Despite the memoryless assumption (on the 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 anticommutator $e_x$ 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 [27], the authors reduced the problem to proving security against a classical adversary (see Table I for a more detailed comparison between the papers). This reduction leads to a bound which is proportional to $\sqrt{d}$ (see Fig. 2). This improves the previous known bound by a factor $\sqrt{d}$.

The precise formal statement is given in Theorem 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 $V_i$’s outcome, and one can map the operations they used for 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 [6] (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).

II. DEVICE-INDEPENDENT GUESSING GAME

A. Preliminaries

1. Notation

We denote $\mathcal{H}_A$, the Hilbert space of the system $A$ with dimension $|A|$ and $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$ the Hilbert space of the composite system, with $\otimes$ the tensor product. By $\mathcal{L}(\mathcal{H})$, $S_0(\mathcal{H})$, $\mathcal{P}(\mathcal{H})$, and $\mathcal{S}(\mathcal{H})$ we mean the set of linear, self-adjoint, positive semidefinite, and (quantum) density operators on $\mathcal{H}$, respectively. For two operators $A, B \in S_0(\mathcal{H})$, $A \geq B$ means $(A - B) \in \mathcal{P}(\mathcal{H})$. If $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ then we denote $\rho_A := \text{tr}_B(\rho_{AB})$ and $\rho_B := \text{tr}_A(\rho_{AB})$ to be the respective reduced states. A measurement, or positive operator valued measure (POVM), of dimension $d$ is a set of positive semidefinite operators that adds up to the identity operator on dimension $d$, namely

$$\mathcal{F} = \left\{ F_x, x \in \mathcal{X} : F_x \in \mathcal{P}(\mathcal{H}) \right\}.$$  

For $M \in \mathcal{L}(\mathcal{H})$, we denote $|M| := \sqrt{M^* M}$ and the Schatten $p$ norm $\|M\|_p := \text{tr}(|M|^p)^{1/p}$ for $p \in [1, \infty]$. Norms without subscript will mean the Schatten $\infty$ norm (also known as the operator norm): $\|M\| := \|M\|_\infty$, which is the largest singular value of $M$; if $M \in \mathcal{P}(\mathcal{H})$ then $\|M\|$ is the highest eigenvalue of $M$. Some useful properties of the operator norms are $\|L\|^2 = \|L^* L\| = \|L L^*\|$ for all $L \in \mathcal{L}(\mathcal{H})$ and if $A, B \in \mathcal{P}(\mathcal{H})$ such that $A \geq B$ then $\|A\| \geq \|B\|. Moreover, whenever $A, B, L \in \mathcal{L}(\mathcal{H})$ and $A(A^* A^*) \geq B(B^* B)$ then $\|A L\| \geq \|B L\|$ [5, Lemma 1].

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

$$\|A\|_p = \sup_{x \neq 0} \frac{\|Ax\|_p}{\|x\|_p}. \quad (2)$$

In the proof of a technical lemma in the appendix, we will need the induced 1 norm and $\infty$ norm,

$$\|A\|_1 = \max_{1 \leq i \leq n} \sum_{j=1}^m |a_{ij}| \quad \text{and} \quad \|A\|_\infty = \max_{1 \leq i \leq n} \sum_{j=1}^m |a_{ij}|, \quad (3)$$

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 $\| \cdot \|^2_2 = \| \cdot \|_2$.

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

FIG. 2. Security is possible for any violation of the CHSH inequality, but depending on the violation we need to send a larger number of qubits $n$. 

\[ P \leq f(S) \]
\[ E_{C,\text{LOCC}}(\rho_{AB}) \] is the one shot entanglement cost to create a bipartite state \( \rho_{AB} \) from a maximally entangled state using only local operations and classical communication. It is formally defined as
\[
E_{C,\text{LOCC}}(\rho) := \min_{M, \Lambda} \{ \log_2(M) : \Lambda(\Psi_M^{AB}) = \rho_{AB}, \Lambda \in \text{LOCC}, M \in \mathbb{N} \},
\]
where \( \Psi_M^{AB} \) is a maximally entangled state of dimension \( M \),
\[
\Psi_M^{AB} := |\Psi_M^{AB}\rangle |\Psi_M^{AB}\rangle, \quad \Psi_M^{AB} := \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |i\rangle_A |i\rangle_B.
\]
Similarly, we have \( E_C(\mathcal{E}) \) [34, Definition 10] is the one shot entanglement cost to simulate a channel \( \mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B) \) using LOCC and preshared entanglement:
\[
E_C(\mathcal{E}) := \min_{M, \Lambda} \{ \log_2(M) : \forall \rho_A \in \mathcal{L}(\mathcal{H}_A), \lambda(\rho_A \otimes \Psi_M^{AB}) = \mathcal{E}(\rho_A) \},
\]
where \( \Lambda \) is a LOCC with \( A \to B \to 0 \) (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 \( \mathcal{E} \) so \( \Lambda \) must be independent of \( \rho_A \).

2. 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 i.i.d. constraint.

Assumptions 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 i.i.d.), 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 \( \sigma_{AB} \) may be chosen by Bob. The testing device is used in the testing Protocol 2.

Similarly dishonest Alice can prepare honest Bob’s measurement device. It is also assumed to be i.i.d.

2. When Bob receives his state \( \rho_B \) from Alice, we allow him to perform any quantum operation on it. After the operation the global state can be written as \( \rho_{ABK} \) where Alice’s part \( \rho_A \) has a tensor product form, and \( \rho_{BK} \) is an arbitrary quantum state held by Bob such that \( |B'| \leq d \) (see Assumptions 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 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 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 \( \rho_{AB} \) using her main device.

2. She sends the \( B \) subsystems in state \( \rho_B \) to her testing device and statistically estimates \( S := \text{tr}(W \rho_{AB}) \), where \( W \) is the CHSH operator defined as
\[
W := A_0 \otimes T_0 + A_0 \otimes T_1 + A_1 \otimes T_0 - A_1 \otimes T_1.
\]

The test is said to be successful if \( S \geq 2 \).

The following Lemma 4 shows that this testing procedure permits Alice to estimate the absolute effective anticommutator defined as follows.

Definition 3. Let \( \rho_{AB} \) 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 anticommutator,
\[
\epsilon_+ := \frac{1}{2} \text{tr}([\{A_0, A_1\}]\rho_A),
\]
where \( A_0 := P_0^0 - P_1^0 \) and \( A_1 := P_1^0 - P_1^1 \), and \( \rho_A := \text{tr}_{B}(\rho_{AB}) \).

Lemma 4 (Proposition 2 of [27]). Let \( \rho_{AT} \in \mathcal{S}(\mathcal{H}_{AT}) \) and let \( A_0, A_1 \) and \( T_0, T_1 \) be binary observables on subsystem \( A \) and \( T \), respectively, achieving \( \text{tr}(W \rho_{AT}) := S \) for \( S \geq 2 \) with \( W \) being the CHSH operator. The absolute effective anticommutator on Alice’s side satisfies
\[
\epsilon_+ \leq \frac{S}{4} \sqrt{8 - S^2} =: \zeta \in [0, 1].
\]

This estimation \( \zeta \) of \( \epsilon_+ \) 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 the following.

Assumptions 5. We assume that the adversarial or dishonest party cannot have access to an unlimited and perfect quantum memory or quantum entanglement. More specifically is the following.

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.

B. 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.
1. Perfect guessing game

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

**Protocol 6. (Perfect guessing game)**

Alice runs Protocol 2, if the devices pass the test successfully then she gets an estimate \( \zeta < 1 \) that upper bounds the effective anticommutator 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 \( \theta_k \) 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. Bob waits for a duration \( \Delta t \) before sending her string \( \theta \) to Bob.
3. Bob tries to guess \( x \) using \( \theta \) 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 i.i.d. Assumption 1. We will go through the (perfect) winning condition is formally at random a string \( \theta \) 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 \( \theta_k \) 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. Bob waits for a duration \( \Delta t \) before sending her string \( \theta \) to Bob.
3. Bob tries to guess \( x \) using \( \theta \) 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 i.i.d. Assumption 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 \( \rho_{AB} = \sigma_{qqc}^{\otimes n} \) and chooses the measurement setting \( \sigma_{n} \) to measure \( \rho_{A} = \sigma_{qqc}^{\otimes n} \) with the POVM \( \{ P_{x} = \bigotimes_{k} P_{x_k} \mid x \in \{0,1\}^n \} \). This measurement can be seen as a tensor product of two binary measurements \( \{ P_{0}^{(0)}, P_{0}^{(1)} \} \) and \( \{ P_{1}^{(0)}, P_{1}^{(1)} \} \) because of the i.i.d. assumption. At the same time, Alice sends to Bob a state which has i.i.d. form \( \rho_B = \sigma_{qqc}^{\otimes n} \) due to our assumption. Then, the waiting time enforces the noisy-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 the (unbounded) classical memory. Bob is allowed to perform any measurement on his system \( B' \), as advised by \( K \) and \( \theta \) 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 \( \zeta \) constrains the possible measurement devices and source Alice can have. Let \( \mathcal{P}(\zeta) \) be the set of possible main measurement devices and source Alice can have conditioned on the fact that Bob has successfully passed the testing procedure with value \( \zeta < 1 \). More formally,

\[
\mathcal{P}(\zeta) := \{ [\sigma_{AB} \cdots P_{0}^{(0)}, P_{1}^{(0)}, P_{0}^{(1)}, P_{1}^{(1)}] \in S(H_{AB}) \times \mathcal{P}(H_{A}) \times \mathcal{P}(H_{A}) : \forall i \in \{0,1\}, P_{0}^{(i)} + P_{1}^{(i)} = \mathbb{I}_{A}, \epsilon_{+} \leq \zeta \}.
\]

Then under Assumptions 1 and 5, and for devices \( \Gamma \in \mathcal{P}(\zeta) \), Bob’s guessing probability is defined as

\[
\lambda(n,d,\Gamma) := \max_{\rho_{AB} \in \mathcal{P}(\zeta)} \max_{\theta} \max_{\delta, x \in \{0,1\}^n} \left( 2^{-n} \sum_{\theta, x \in \{0,1\}^n} P_{\theta}^x \otimes F_{\theta}^{x} \rho_{AB}^{K} \right),
\]

where the first maximization is over all qqc states \( \rho_{AB,K} \), such that \( tr_{B}^{K}(\rho_{AB,K}) = tr_{B}(\rho_{AB}) = \rho_{A} \), where \( \rho_{AB} = \sigma_{qqc}^{\otimes n} \) is the initial state as defined above and \( F_{\theta}^{x} \) are the measurement operators of Alice as mentioned above. \( F_{\theta}^{x} \) are arbitrary measurement operators of Bob acting on the \( B'K \) register. Note that the state \( \rho_{B,K} := tr_{A}(\rho_{AB,K}) \) is the qc state that Bob gets after a quantum operation on the initial state \( \rho_{B} = \sigma_{qqc}^{\otimes d} \) sent to him by Alice. The second maximization is a short hand for \( 2^n \) separate maximizations: For each \( \theta \) we pick the POVM \( F_{\theta}^{x} = \{ F_{\theta}^{x} \mid x \in \{0,1\}^n \} \) which maximizes the sum over \( x \).

The following lemma, whose proof is presented in the appendix, gives a bound on the probability \( \lambda(n,d,\Gamma) \).

**Lemma 7 (Key Lemma).** In a perfect guessing game where the adversary holds a bounded quantum memory of dimension at most \( d \), we have

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

where \( t \) is defined as

\[
t = \left\lfloor - \log_2 d \left( \log_2 \left( \frac{1 + \zeta}{2} \right) \right)^{-1} \right\rfloor.
\]

which implies that,

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

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 \( r := \log_2(d) = kn \) the bound \( B(n,2',\zeta) \) decays exponentially when \( n \rightarrow \infty \) (and for constant \( \zeta < 1 \)) as long as \( k < -2 \log_2 \left( \frac{1}{2} + \frac{1 + \zeta}{2} \right) \approx 0.45 \) which is an improvement over the bound

of a factor 2 for the size of Bob's memory compared to [27].

2. Imperfect guessing game

The consideration of the 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,

\[
\lambda_{\text{ip}}(n, d, \Gamma, \gamma) := \max_{\rho_{AB} \in \mathcal{H}_{\text{qqc}}} \max_{\dim(\mathcal{H}_x) \leq d} \left( 2^{-n} \sum_{\theta, x \in [0, 1]^n} \sum_{y, z \in [0, 1]^n} P_{\theta, x}^\theta \otimes P_{y}^\theta \rho_{AB:K} \right),
\]

(13)

where \(\Gamma \in \mathcal{Q}(\xi)\) [see Eq. (10)], and \(\gamma\) 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 paper is the following.

**Theorem 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 \(\mathcal{E}\) such that \(E_{C(1)}(\mathcal{E}) \leq \log_2(d)\), the winning probability of Bob,

\[
\lambda_{\text{ip}}(n, d, \Gamma, \gamma) \leq 2^{h(\gamma)n} B(n, d, \xi) =: B'(n, d, \xi, \gamma),
\]

(14)

where \(h(\cdot)\) is the binary entropy and \(B(n, d, \xi)\) is the bound defined inLemma 7.

**Proof.** (Sketch) We first look at the imperfect guessing game in the bounded 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

\[
\text{tr} \left( \sum_{x \in [0, 1]^n} \sum_{y \in [0, 1]^n} P_{x}^\theta \otimes P_{y}^\theta \rho_{AB:K} \right) = \text{tr} \left( \sum_{x \in [0, 1]^n} \sum_{y' \in [0, 1]^n} P_{x}^\theta \otimes P_{y'}^\theta \rho_{AB:K} \right)
\]

\[
= \sum_{y' \in [0, 1]^n} \text{tr} \left( \sum_{x \in [0, 1]^n} P_{x}^\theta \otimes P_{y'}^\theta \rho_{AB:K} \right).
\]

(15)

Then combining the previous remark with (13) we have

\[
\lambda_{\text{ip}}(n, d, \Gamma, \gamma) \leq \sum_{z \in [0, 1]^n} \max_{\rho_{AB} \in \mathcal{H}_{\text{qqc}}} \max_{\dim(\mathcal{H}_z) \leq d} \left( 2^{-n} \sum_{x \in [0, 1]^n} \sum_{y \in [0, 1]^n} P_{x}^\theta \otimes P_{y}^\theta \rho_{AB:K} \right)
\]

(17)

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 7 to bound each term of the sum over \(z\) we can write

\[
\lambda_{\text{ip}}(n, d, \Gamma, \gamma) \leq B(n, d, \xi) \times \sum_{w_H(z) \leq \gamma n} 1
\]

\[
= B(n, d, \xi) \times \sum_{w_H(z) \leq \gamma n} \binom{n}{|\gamma n|}
\]

(18)

To proceed further, we assume that \(\gamma < 1/2\) so \(|\gamma n|\) is bounded by \([n/2]\) and therefore by Lemma 25 of [14] we can bound the binomial sum by the binary entropy function \(h(\cdot)\) so that

\[
\lambda_{\text{ip}}(n, d, \Gamma) \leq 2^{h(\gamma)n} B(n, d, \xi) =: B'(n, d, \xi, \gamma).
\]

(20)

It remains to extend this bound to an adversary who holds a noisy memory \(\mathcal{E}\) such that the one-shot entanglement cost satisfies \(E_{C(1)}(\mathcal{E}) \leq \log_2(d)\). Indeed, by definition of the one-shot entanglement cost [34], the above condition means that \(\mathcal{E}\)

can be simulated by the identity channel \(1_d\). Then all strategies achievable with \(\mathcal{E}\) are achievable with \(1_d\), particularly the strategy which maximizes the probability of winning in the bounded 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 9.** If the maximum QBER allowed \(\gamma\) satisfies the following conditions:

\[
h(\gamma) < - \log_2 \left( \frac{1}{2} + \frac{1}{2} \frac{1 + \xi}{2} \right). \tag{22}
\]

then \(B'(n, d, \xi, \gamma)\) decays exponentially in \(n\), when \(n \rightarrow \infty\) and \(d, \xi\) are fixed.

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

**Proof.** First note that \(B'(n, d, \xi, \gamma) = 2^{h(\gamma)n} B(n, d, \xi)\). According to Lemma 7, \(B(n, d, \xi) = \sqrt{d} \left(1 + \frac{1}{2} \frac{1 + \xi}{2} \right) - O(n^{-2-n})\). 

062307-8
It is now straightforward to see that the condition on $\gamma$ implies the exponential decay of $B'(n,d,\xi,\gamma)$. ■

III. APPLICATIONS

Following the analysis of [27] 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 [6], we also get a security proof for PV.

A. Device-independent weak string erasure

This section is divided into two subsections.

1. $(\alpha, \epsilon = 0)$-WSE in the noisy-storage model

Let the two protagonists of $(\alpha, \epsilon)$ 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 $x_I$. We can view this $x_I$ as $x$ where we have randomly erased some bits, hence the name WSE (Protocol 10). For a formal definition of $(\alpha, \epsilon)$ WSE we refer to [15].

Protocol 10 (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 2 and obtains $\xi$, an estimate of an upper bound on the effective anticommutator.
2. Alice creates $n$ identical bipartite states $\sigma_{AB}$. 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 $\theta_k$ 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 $\sigma_{AB}$ 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 $\Delta t$ before sending $\theta$ to Bob.
5. Bob determines the index set $I := \{k \in [n]: \theta'_k = \theta_k\}$, and obtains the corresponding substring $x'_I$.

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

Security for honest Bob

Let $\rho_{AB}$ be the state that dishonest Alice produces at the beginning of the protocol, $\hat{\rho}_{AB}$ the state after the execution of WSE, where $B := (I, X_I)$ ($X$ is the random variable for the bit string $x$ and $X_I$ is the random variable for the substring $x_I$ 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 $\tau_{AX_I}$ such that $\tau_{AX_I} = \hat{\rho}_{AB} \otimes \frac{1}{|I|}$ and for any given $I$, $\tau_{AX_I} = \hat{\rho}_{AB} \otimes \xi$.

Let us now take $\tau_{AX_I}$ as being the state we would obtain after Protocol 10 if Bob (in some imaginary scenario), instead of measuring the $B$ part of state $\rho_{AB}$ in his chosen bases $\theta'$, measured it in Alice’s bases $\theta$ 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 $\tau_{AX_I}$ satisfies the two properties described above, and hence that Protocol 10 implements a secure WSE for Bob.

Theorem 11. Protocol 10 realizes a secure WSE for Bob. Indeed the state $\tau_{AX_I}$ defined above satisfies the two required relations:

\[ \tau_{AX_I} = \hat{\rho}_{AB} \otimes \frac{1}{|I|}, \]

\[ \tau_{AX_I} = \tau_{AX} \otimes I. \]

where $\hat{\rho}_{AB}$ is the real state produced after the execution of WSE.

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

\[ \tau_{AX_I} = \tau_{AX} \otimes \frac{1}{|I|}. \]

Let us now compare the operations performed during the real protocol, where Bob measures in his own bases $\theta'$, with the ones performed in the hypothetical scenario where Bob chooses the bases $\theta'$ but measures in Alice’s bases $\theta$.

In both scenarios Alice produces the state $\rho_{AB}$. In both scenarios apply the map $M_{A'=A} \otimes 1_B (A' = \Theta I$ where $\Theta$ is the register for the bit string $\theta$ and $T$ is an arbitrary quantum register$)$ to $\rho_{AB}$ and send the $B$ part to Bob. In both scenarios Bob chooses uniformly at random a bit string $\theta'$. Now Bob will apply two different measurements depending on the scenario.

In the real scenario Bob applies a measurement modeled by a CPTP map $M_{\text{hyp}}$ going from $B$ to $X'I$. They correspond to the choice of basis $\theta'$.

In the hypothetical scenario Bob applies a measurement modeled by a CPTP map $M_{\text{hyp}}$ going from $B$ to $X'I$. They correspond to the choice of basis $\theta$.

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

Because the devices are memoryless and because on the rounds in $I$ the bits of $\theta$ and $\theta'$ agree, the measurements

\[ \tau_{AX_I} = \tau_{AX} \otimes I. \]
on $B_{T}$ are equal in both scenario, meaning that $\mathcal{M}_{\text{real}}^{B_{T}} = \mathcal{M}_{\text{hyp}}^{B_{T}} = \mathcal{M}_{B_{T}}$. Then we can write $\tau_{A,X,Z} = (\mathcal{M}_{A-A}\otimes\mathcal{M}_{B_{T}}\otimes\mathcal{M}_{B_{T}^{\text{hyp}}})(\rho_{AB})$. Moreover because Bob will trace out (in both scenarios) all the outcomes of the rounds in $T$, the fact that the measurements are different on these rounds does not affect the outcomes in $T$, meaning that

$$
\text{tr}_{X_{T}^{'}}\left(\left(\mathcal{M}_{A}\otimes\mathcal{M}_{B_{T}}\otimes\mathcal{M}_{B_{T}^{\text{real}}}\right)(\rho_{AB})\right) = \text{tr}_{X_{T}^{'}}\left(\left(\mathcal{M}_{A}\otimes\mathcal{M}_{B_{T}}\otimes\mathcal{M}_{B_{T}^{\text{hyp}}}\right)(\rho_{AB})\right)
$$

(23)

$$
\iff \hat{\rho}^{A}_{X_{T}^{'},Z} = \tau_{A,X_{T}^{'}Z}.
$$

(24)

\section*{Security for honest Alice}

According to [15], 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) conditioned on Bob’s register. Therefore it is sufficient to lower bound the min-entropy as follows,

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

This is equivalent to showing 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

$$
\lambda_{\text{WSE}}(n,d,\Gamma) := \max_{\rho_{ABK}} \max_{x} \text{tr}\left(2^{-n} \sum_{\theta,x} P_{x}^{\theta} \otimes F_{x}^{\theta} \rho_{ABK}\right),
$$

(25)

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.

\textbf{Corollary 12.} For $(\alpha,\epsilon = 0)$ WSE in the noisy-storage model, under Assumption 1, if Alice’s memoryless device is such that $\xi < 1$ then the cheating probability $\lambda_{\text{WSE}}(n,d,\Gamma)$ of Bob is upper bounded by $B(n,d,\xi,\gamma)$, where $B(n,d,\xi,\gamma)$ is defined in Theorem 8.

\textbf{Proof.} We can directly apply Theorem 8 in $(\alpha,\epsilon = 0)$ WSE by considering Bob’s cheating strategy as a guessing game. $\blacksquare$

\section*{2. $(\alpha,\epsilon = 0)$ 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 [6] 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 $\rho_{B_{1}B_{2}}$ such that $E_{\mathcal{E}}^{\text{B}}(\rho_{B_{1}B_{2}}) \leq \log_{2}(d)$ (which replaces Bob’s channel $\mathcal{E}$ used in the noisy storage model), and can only communicate classically from Bob1 to Bob2.

It is Bob2 who is asked to get the pair $(I,X_{2})$, while Alice sends $\rho_{B_{1}}$ to Bob1 and $\theta$ to Bob2. If the Bobs are cheats, Bob1 will try to send $\rho_{B_{1}}$ 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 $(1-\gamma)n$) 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 [6]. Again we say that WSE in the noisy-entangled model is secure if the cheating probability denoted by $\lambda_{\text{NE}}$ 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 the noisy-entanglement model.

\textbf{Definition 13.} For $(\alpha,\epsilon = 0)$ WSE in the bounded-entanglement model, the probability $\lambda_{\text{BE}}(n,d,\Gamma)$ that Bob2 perfectly guesses Alice’s output string $x \in \{0,1\}^{n}$ is the following:

$$
\lambda_{\text{BE}}(n,d,\Gamma) := \max_{\rho_{ABK}} \max_{x} \text{tr}\left(2^{-n} \sum_{\theta,x} P_{x}^{\theta} \otimes F_{x}^{\theta} \rho_{ABK}\right),
$$

(26)

where the first maximization is over all qqc states compatible with the marginal on Alice (which are constrained by the value $\xi$ measured in the testing procedure). Here the state $\rho_{B_{1}}$ is of dimension at most $d$.

In the following Lemma 14 we look at the special case where $\rho_{B_{1}B_{2}}$ 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 7.

\textbf{Lemma 14.} For WSE in the bounded-entanglement model, where the two Bobs share a perfect entangled state $\rho_{B_{1}B_{2}}$ of dimension at most $d^{2}$, the probability $\lambda_{\text{BE}}(n,d,\Gamma)$ that Bob2 perfectly guesses Alice’s output string $x \in \{0,1\}^{n}$ is

$$
\lambda_{\text{BE}}(n,d,\Gamma) \leq B(n,d,\xi),
$$

(27)

where $B(n,d,\xi)$ is defined in Lemma 7.

\textbf{Proof.} The guessing probability of Bob2 in this model is given by

$$
\lambda_{\text{BE}}(n,d,\Gamma) := \max_{\rho_{ABK}} \max_{x} \text{tr}\left(2^{-n} \sum_{\theta,x} P_{x}^{\theta} \otimes F_{x}^{\theta} \rho_{ABK}\right),
$$

(28)

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 $\rho_{ABK}$ is replaced by $\rho_{ABK}$. We can then invoke Lemma 7 since Bob2’s measurements are also acting jointly on the $d$-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 $\gamma$. 

**Definition 15.** For $(\alpha, \epsilon = 0)$ WSE in the noisy-entanglement model, the probability $\lambda_{\text{NE}}(n, d, \xi, \gamma)$ that Bob2 guesses Alice’s output string $x \in \{0, 1\}^n$ with an error rate, as defined in the paragraph before Eq. (13), at most $\gamma$ is

$$\lambda_{\text{NE}}(n, d, \Gamma, \gamma) := \max_{\rho_{AB}, k} \max_{\rho_{\text{abi}} \in \mathcal{F}(\mathcal{F})} \left( 2^{-n} \sum_{\theta, x \in \{0, 1\}^n} \sum_{y \in \{0, 1\}^n} P^\theta_x \otimes F^\theta_y \rho_{AB} \right),$$

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 $\rho_{B, B'}$ is such that $E_C^{(1)}(\rho_{B, B'}) \leq \log_2(d)$.

Now we tackle the general case where $\rho_{B, B'}$ is a noisy-entangled state such that $E_C^{(1)}(\rho_{B, B'}) \leq \log_2(d)$.

**Lemma 16.** Consider $(\alpha, \epsilon = 0)$ WSE in the noisy-entanglement model, where the two Bobs share a noisy-entangled state $\rho_{B, B'}$ such that $E_C^{(1)}(\rho_{B, B'}) \leq \log_2(d)$. If Alice’s device is such that $\xi < 1$, then the probability $\lambda_{\text{NE}}(n, d, \Gamma)$ 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:

$$\lambda_{\text{NE}}(n, d, \Gamma, \gamma) \leq B'(n, d, \xi, \gamma),$$

where $B'(n, d, \xi, \gamma)$ is defined in Theorem 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 $M \leq d$:

$$|\Psi_M^{B_1}B_2\rangle := \frac{1}{\sqrt{M}} \sum_{i=1}^M |i\rangle |i\rangle \rangle.$$

Denote $\Psi_M := |\Psi_M^{B_1}B_2\rangle |\Psi_M^{B_1}B_2\rangle \rangle$. Note that the fact that the local dimension $\Psi_M$ is at most $d$ implies that Bob2’s quantum state $\rho_{B_i}$ has a dimension bounded by $d$. Hence it is easy to see that

$$\lambda_{\text{NE}}(n, d, \Gamma, \gamma) \leq \max_{\rho_{AB}, k} \max_{\rho_{\text{abi}} \in \mathcal{F}(\mathcal{F})} \left( 2^{-n} \sum_{\theta, x \in \{0, 1\}^n} \sum_{y \in \{0, 1\}^n} P^\theta_x \otimes F^\theta_y \rho_{AB} \right) \leq \max_{\rho_{AB}, k} \sum_{z \in \{0, 1\}^n} \max_{\rho_{\text{abi}} \in \mathcal{F}(\mathcal{F})} \left( 2^{-n} \sum_{\theta, x \in \{0, 1\}^n} \sum_{y \in \{0, 1\}^n} P^\theta_x \otimes F^\theta_y \rho_{AB} \right),$$

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 Theorem 8 since the register $B_2$ has bounded dimension. We have

$$\lambda_{\text{NE}}(n, d, \Gamma, \gamma) \leq 2^{h(\gamma) \ln n} \times B(n, d, \xi) \leq B'(n, d, \xi, \gamma).$$

We can extend this bound against an adversary who holds a noisy-entangled state $\rho_{B, B'}$, such that $E_{\text{C,LOCC}}^{(1)}(\rho_{B, B'}) \leq \log_2(d)$. Indeed by definition [Eq. (4)] of the one shot entanglement cost of the state $\rho_{B, B'}$, denoted $E_{\text{C,LOCC}}^{(1)}(\rho_{B, B'})$ [35], saying that $E_{\text{C,LOCC}}^{(1)}(\rho_{B, B'}) \leq \log_2(d)$ means that $\rho_{B, B'}$ can be created from a perfectly entangled state $\Psi_M$ of dimension $M \leq d$. Thus, all strategies achievable with $\rho_{B, B'}$ are achievable with $\Psi_M$. In particular the strategy which maximizes the probability of winning with respect to $\rho_{B, B'_1}$ is achievable with $\Psi_M$ which proves the lemma.

---

**B. 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 [6, Theorem 14]. As we have proved in Lemma 16 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
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) $\rho_{V_1,\psi} = \sigma_{V_1,\psi}^{\otimes n} \rho_P$ which has a tensor product structure, and sends the part $\rho_P := \text{tr}_{V_1}(\rho_{V_1,\psi})$ to the prover.

$V_2$ sends the string $\theta$ to the prover, such that the prover receives $\theta$ and $\rho_P$ at the same time.

$V_1$ applies the measurement $\mathcal{M}_\theta = \{ P^\theta_y := \bigotimes_{j \in [n]} P^{\theta_j}_y, y \in \{0,1\}^n \}$ to his part of the state $\rho_{V_1,\psi}$ 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 $\Delta t$ then the prover passes the protocol, which means that the verifiers accept that the prover is at his claimed position.

As mentioned in the introduction, 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 $\rho_{B_1,B_2}$, 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 18.** 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

\[
\lambda_{PV}(n,d,\Gamma,\gamma) := \max_{\theta_1,M_1,M_2} \max_{\rho_{V_1,M_1,M_2}} \max_{\theta_2,M_1,M_2} \max_{\rho_{V_2,M_1,M_2}} \left( 2^{-n} \sum_{\theta,\theta_1,\theta_2 \in [0,1]^n} \sum_{y \in \{0,1\}^n} P^\theta_1 \otimes T^\theta_2 \otimes F^\theta_2 \rho_{V_1,\psi} \otimes M_1 \otimes M_2 \right),
\]

where the first maximization is over all states compatible with the marginal on $V_1$, $P_1^\theta$, $T_2^\theta$, and $F_2^\theta$ are the measurement operators for $V_1$, $M_1$, and $M_2$ respectively, and where the second and the third maximizations are short hand for $2^n$ separate maximizations: For each $\theta$, $M_1$ and $M_2$ choose the POVMs which maximize $\lambda_{PV}(n,d,\Gamma,\gamma)$.

**Definition 19.** PV is said to be $\alpha$ secure if there exists $\alpha > 0$ and an integer $N \geq 1$ such that $\Gamma n \geq N$ the probability $\lambda_{PV}(n,d,\Gamma,\gamma)$ that dishonest provers pass the protocol is such that

\[
\lambda_{PV}(n,d,\Gamma,\gamma) \leq 2^{-\alpha n}.
\]

Note that the value of $\alpha$ may depend on $d, \xi$, and $\gamma$.

In our case we limit the attack scheme by assuming that the adversaries can only share a limited amount of entanglement (Assumptions 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 1 is satisfied in our model of attack.

**Lemma 20.** In PV in the noisy-entanglement model, where Bob1 and Bob2 share a state $\rho_{B_1,B_2}$ such that $E_{LOCC}^{(3)}(\rho_{B_1,B_2}) \leq \log_2(d)$, if $V_1$’s device is such that $\xi < 1$ then the probability $\lambda_{PV}(n,d,\Gamma,\gamma)$ 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

\[
\lambda_{PV}(n,d,\Gamma,\gamma) \leq B'(n,d,\xi,\gamma),
\]

where $B'(n,d,\xi,\gamma)$ is defined in Theorem 8.
The results in the trusted device 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 the security condition stronger than in [27] for a dishonest Alice which can become useful when using WSE in other two-party cryptographic protocols. The previous result only proves the security of the two-party cryptographic protocol against the classical adversary, by proving that at the end of WSE Alice is ignorant about the set $I$.

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.

ACKNOWLEDGMENTS

J.R., J.H., and S.W. are funded by STW, NWO VIDI, and ERC Starting Grant (S.W.). L.P.T. acknowledges the support of National Research Foundation, Prime Minister’s Office, Singapore and the Ministry of Education, Singapore under the Research Centres of Excellence programme. J.K. is supported by Ministry of Education, Singapore.

APPENDIX A: 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 [36]; see also [5, Lemma 2].

**Lemma 21.** If $A_1, A_2, \ldots, A_N$ are positive semidefinite operators, then

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

(A1)

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

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

(A2)

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

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

(A3)

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;

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

(A4)

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

IV. 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 $r := \log_2(d) \lesssim 0.45nqubits$. This improves the previous known result [27] which proved security for $r \lesssim 0.22nqubits$ (see Table I). 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 analyses of optimal bound in the i.i.d. device-independent scenario. We don’t know, however, if our bound is optimal.
eigenvalue of $L$. Let $|\alpha\rangle$ be an eigenvector corresponding to the largest eigenvalue of $\tilde{K} \tilde{K}^\dagger$ and write it as 

$$|\alpha\rangle = \sum_j \alpha_j |j\rangle |e_j\rangle,$$  \hspace{1cm} (A5)

where $\alpha_j$ are real and positive and $|e_j\rangle$ are arbitrary but normalized. Then

$$\|\tilde{K} \tilde{K}^\dagger\| = \langle \alpha | \tilde{K} \tilde{K}^\dagger | \alpha \rangle = \sum_{jk} \alpha_j \alpha_k \langle e_j | \sqrt{A_j} \sqrt{A_k} | e_k \rangle.$$  \hspace{1cm} (A6)

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

$$|\alpha'\rangle = \sum_j \alpha_j |j\rangle,$$  \hspace{1cm} (A7)

which implies

$$\|K\| = \|\tilde{K} \tilde{K}^\dagger\| = \langle \alpha | \tilde{K} \tilde{K}^\dagger | \alpha \rangle \leq \langle \alpha' | L | \alpha'\rangle \leq \|L\|.$$  \hspace{1cm} (A8)

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

$$K = \sum_{jk} |j\rangle \langle k| \otimes \sqrt{A_j} \sqrt{A_k}$$  \hspace{1cm} (A9)

$$\leq \sum_{j<k} \sum_{=B_{jk}} |j\rangle \langle k| \otimes \sqrt{A_j} \sqrt{A_k} + \sum_{j} \sum_1^{|\alpha_j|} \sqrt{A_j} \langle \alpha_j | \otimes A_j.$$  \hspace{1cm} (A10)

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

$$\begin{gathered}
\langle \alpha | K | \alpha \rangle = \sum_{jk} \alpha_j \alpha_k \langle j | B_{jk} | k \rangle \langle e_k | e_k \rangle \\
+ \sum_1^{|\alpha_j|} \alpha_j^2 \langle e_j | A_j | e_j \rangle \leq \sum_{j<k} \sum_{=B_{jk}} \alpha_j \alpha_k |\langle j | B_{jk} | k \rangle | \langle e_k | e_k \rangle | + \sum_1^{|\alpha_j|} \alpha_j^2 \| A_j \|.
\end{gathered}$$  \hspace{1cm} (A12)

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 $|\beta_i\rangle$ we get

$$|\langle j | B_{jk} | k \rangle | \langle e_k | e_k \rangle | = \sum_{lm} \beta_l^j \beta_m^k \langle \beta_l | B_{jk} | \beta_m \rangle = \sum_l \beta_l^j \beta_l^k \lambda_l.$$  \hspace{1cm} (A13)

$$|\langle j | B_{jk} | k \rangle | \langle e_k | e_k \rangle | = \sum_l \beta_l^j \beta_l^k \lambda_l.$$  \hspace{1cm} (A14)

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

$$\sum_l \beta_l^j \beta_l^k \lambda_l \leq \sum_l |\beta_l^j|^2 |\beta_l^k|^2 |\lambda_l|.$$  \hspace{1cm} (A15)

It is easy to check that $\|B_{jk}\| = \|\sqrt{A_j} \sqrt{A_k}\|$. Using that and (A17) in the inequality (A12) we have

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

$$\leq \langle \alpha' | L | \alpha'\rangle \leq \|L\|.$$  \hspace{1cm} (A18)

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

Using Hölder’s inequality (Lyapunov’s inequalities) for induced $p$ norms, we have

$$\|L\| = \|L\|_1 \leq \left( \|L\|_1 \cdot \|L\|_\infty \right)^{1/2},$$  \hspace{1cm} (A19)

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

$$\|L\|_1 = \max_j \sum_i \|\sqrt{A_j} \sqrt{A_j}\|.$$  \hspace{1cm} (A20)

$$\|L\|_\infty = \max_j \sum_i \|\sqrt{A_j} \sqrt{A_j}\|.$$  \hspace{1cm} (A21)

The lemma follows since these two norms are equal for Hermitian matrices.

\section*{Appendix B: Proof of the Key Lemma}

The main content of this appendix 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 $\xi$ 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 analyze how Jordan’s Lemma permits us to conveniently express the effective absolute anticommutator 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 anticommutator. We finish the proof in Step 4 by replacing, in the previous simple bound on the overlap, the effective anticommutator by a quantity that Alice can estimate experimentally.

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

\section*{Step 1: Alice’s i.i.d. state-preparation and measurement device}

In this section we use Jordan’s Lemma to rewrite Alice’s measurement operators and the absolute effective anticommutator.

We assume that the devices used by Alice to prepare and measure satisfy the i.i.d. assumption, i.e., the state produced in $n$ rounds is of the form $\rho_{AB} = \sigma_{AB}^{(n)}$ and the measurement corresponding to input $\theta \in [0,1]^n$ can be written as $\{P_0^{\theta} = \bigotimes_k P_{\theta k}^0 : x \in [0,1]^n\}$, 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, \( \rho_A = \rho_A^\otimes^n \), 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 [32,33]. The projectors representing the first outcome \( P^0_0 \) and \( P^0_1 \) can simultaneously be 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 operator \( T \) if and only if \( TW \subseteq W \)). Moreover we only get two-dimensional blocks when the projectors have nontrivial overlap, i.e., they are neither orthogonal nor identical:

\[
P^0_0 = \sum_{j \in \mathcal{J}} P^0_{0,j}, \quad P^1_1 = \sum_{j \in \mathcal{J}} P^1_{1,j},
\]

(B1)

where \( P^a_{b,j} \) (\( a, b \in \{0,1\} \)) are such that \( \forall j, j' \mathcal{J} P^a_{0,j} P^a_{0,j'} = \delta_{jj'} P^a_{0,j} \) and are acting on a subspace of dimension one or two. Then we have

\[
P^0_0 = \sum_{j \in \mathcal{J}} (S_j - P^0_{0,j}), \quad P^1_1 = \sum_{j \in \mathcal{J}} (S_j - P^1_{1,j}),
\]

(B2)

where \( S_j \) is a projection which projects on the subspace where \( P^0_{0,j} \) and \( P^1_{1,j} \) act. Note that the number of nonzero summands in (B1) is equal to the rank of \( P^0_0 \) or \( P^1_1 \), respectively.

A convenient basis of the Hilbert space can be chosen as follows. Each index \( j \in \mathcal{J} \) corresponds to either a one- or two-dimensional subspace. For the two-dimensional subspaces indexed by \( j \) in \( \mathcal{J} \) where both \( P^0_{0,j} \) and \( P^1_{1,j} \) are nonzero, we pick the orthonormal eigenbasis of \( P^0_{0,j} \), namely \( \{ 0^0_{0,j} \} \) and \( \{ 1^0_{0,j} \} \), as the basis for these subspaces,

\[
P^0_{0,j} \{ 0^0_{0,j} \} = \{ 0^0_{0,j} \}, \quad P^0_{0,j} \{ 1^0_{0,j} \} = 0.
\]

Moreover, one can pick these basis vectors (by including a phase factor if necessary) such that the eigenstates \( \{ 0^1_{1,j} \} \) and \( \{ 1^1_{1,j} \} \) of \( P^1_{1,j} \), which satisfy

\[
P^1_{0,j} \{ 0^1_{1,j} \} = \{ 0^1_{1,j} \}, \quad P^1_{0,j} \{ 1^1_{1,j} \} = 0,
\]

are related to those of \( P^0_{0,j} \) by

\[
\begin{align*}
\{ 0^1_{1,j} \} &= \cos \beta_j \{ 0^0_{0,j} \} + \sin \beta_j \{ 1^0_{0,j} \}, \\
\{ 1^1_{1,j} \} &= \sin \beta_j \{ 0^0_{0,j} \} - \cos \beta_j \{ 1^0_{0,j} \},
\end{align*}
\]

(B5)

for some angle \( \beta_j \in [0, \pi/2] \). For the one-dimensional subspaces (also indexed by \( j \in \mathcal{J} \)) we define \( \{ 0^0_{1,j} \} \) being a unit vector, and \( \{ 1^0_{1,j} \} \) is the null vector. Then we define \( \{ 0^1_{1,j} \} \) and \( \{ 1^1_{1,j} \} \) as previously but with \( \beta_j = 0 \) or \( \beta_j = \pi/2 \). In summary, since we have defined a basis for each \( j \in \mathcal{J} \), 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 \( j \in \mathcal{J} \) 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

\[ \epsilon_+ := \frac{1}{2} \tr((A_0 A_1) |\sigma_A\rangle \langle \sigma_A|) \]

where \( A_0 := P^0_0 - P^1_0 \) and \( S_j \) being the orthogonal projections defined above, where the absolute anticommutator of a two-dimensional block \( j \) is computed using (B5) and that of a one-dimensional block follows from our definition of \( \beta_j = 0 \) in Step 1. Let \( p_j := \tr(S_j |\sigma_A\rangle \langle \sigma_A| S_j) \) be the probability of \( \sigma_A \) being projected in the \( j \)th block, then, the absolute effective anticommutator can be written as

\[ \epsilon_+ = \sum_j p_j |\cos(2\beta_j)| \]

(B7)

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

\[ \begin{align*}
P^0_x &= \bigotimes_{k=1}^n P^0_{x_k}, \\
P^1_x &= \bigotimes_{k=1}^n \sum_{b_k \in \mathcal{J}} P^b_{x_k b_k} = \bigotimes_{b \in \mathcal{J}^n} P^b_{x b},
\end{align*} \]

(B8)

where \( P^b_{x b} := \bigotimes_{k=1}^n P^b_{x_k b_k} \) and \( \mathcal{J}^n := \mathcal{J} \times \cdots \times \mathcal{J} \). We denote the set of projectors associated with this direct sum decomposition by \( \{ S_b \}_{b \in \mathcal{J}^n} \), where \( S_b := \bigotimes_{k=1}^n S_{b_k} \). For each \( k \), we have \( P^b_{x_k b_k} = \delta_{x_k b_k} P^b_{x_k b_k} \) and \( P^b_{x_k b_k} \) orthogonal to \( P^b_{x_b} \) whenever \( b_k \neq b_k' \).

The analysis of the guessing game will rest on these orthogonality relations and the set of angles \( \beta_j \) defined above.

**Step 2: From guessing probability to “operator overlaps”**

The goal of this section is to bound Bob’s winning probability in terms of the overlap \( \| \sqrt{P^1_b} \sqrt{P^0_b} \| \). To be precise we show the following.
Lemma 22. Let \( \Pi_{b}^{\theta,k} := \sum_{x} P_{x|b}^{\theta} \otimes F_{x}^{\theta,k} \), where Alice’s POVM elements \( P_{x}^{\theta} \) are defined in (B8), and where \( F_{x}^{\theta} \) are arbitrary POVM element acting on Bob’s systems [registers \( B' K' \); see Eq. (10)], and \( F_{x}^{\theta,k} \) are defined in Eq. (B13). Bob’s winning probability \( \lambda(n, d, \Gamma) \) defined in Eq. (10) is bounded as follow:

\[
\lambda(n, d, \Gamma) \leq \max_{\rho_{AB}^{K}} \max_{\{p_{x}, \rho_{x}^{\theta} \}} \left[ \sum_{k,b} p_{k} p_{b|k} \max_{\theta \in [0,1]} 2^{-n} \left[ \sqrt{\Pi_{b}^{\theta,k} \otimes \Pi_{b}^{\theta,k}} \right] \right].
\] (B9)

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 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 \( \rho_{AB,K} = \sum_{k} p_{k} \rho_{x}^{\theta,k} \otimes |k\rangle \langle k| \) whose marginal remains i.i.d. \( \rho_{A} = \text{tr}_{B,K}(\rho_{AB,K}) = \sigma_{A}^{\text{qqc}} \).

Once Alice has measured her part of the system, Bob is told the choice of her measurements represented by \( \theta \), and for convenience let us denote \( \Pi_{b}^{\theta,k} \) as the measurement operators on Alice’s side, and

\[
F_{x}^{\theta,k} := \text{tr}_{K} \left( F_{x}^{\theta} \otimes |k\rangle \langle k| \right)
\]

are \( d \)-dimensional measurement operators on Bob’s side acting on \( B' \), which depend both on his classical memory \( k \) and the basis string \( \theta \) received from Alice. The outer optimization is constrained to ensembles which yield the correct marginal on Alice’s side, i.e., \( tr_{B'}(\sum_{k} p_{k} \rho_{K}^{b|k}) = \sigma_{A}^{\text{qqc}} \). The inner maximization represents \( \theta \) 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 (B8) into (B12) we get

\[
\lambda(n, d, \Gamma) = \max_{\rho_{AB}^{K}} \max_{\{p_{x}, \rho_{x}^{\theta} \}} \left[ \sum_{k,b} p_{k} \max_{\theta \in [0,1]} 2^{-n} \left[ \sum_{b} P_{x|b}^{\theta} \otimes F_{x}^{\theta,k} \right]\right].
\] (B14)

Recall that \( S_{b} \) represents the projection operator into the blocks indexed by \( b \in J^{n} \). Define \( \rho_{b|K}^{k} := (S_{b} \otimes \mathbb{I}_{B'}) \rho_{x}^{\theta,k} (S_{b} \otimes \mathbb{I}_{B'}) / p_{b|k} \) to be the normalized projections of \( \rho_{K}^{b|k} \) into these various blocks with \( p_{b|k} := \text{tr} ((S_{b} \otimes \mathbb{I}_{B'}) \rho_{x}^{\theta,k} (S_{b} \otimes \mathbb{I}_{B'}) \) Then

\[
\lambda(n, d, \Gamma) = \max_{\rho_{AB}^{K}} \max_{\{p_{x}, \rho_{x}^{\theta} \}} \left[ \sum_{k} p_{k} \sum_{b} p_{b|k} \max_{\theta \in [0,1]} 2^{-n} \left[ \sum_{b} P_{x|b}^{\theta} \otimes F_{x}^{\theta,k} \rho_{b|K}^{k} \right]\right].
\] (B15)

and for convenience let us denote \( \Pi_{b}^{\theta,k} := \sum_{x} P_{x|b}^{\theta} \otimes F_{x}^{\theta,k} \) so that

\[
\lambda(n, d, \Gamma) = \max_{\rho_{AB}^{K}} \max_{\{p_{x}, \rho_{x}^{\theta} \}} \left[ \sum_{k,b} p_{k} p_{b|k} \max_{\theta \in [0,1]} 2^{-n} \left[ \Pi_{b}^{\theta,k} \right]\right].
\] (B16)

Bounding each of the trace terms by its operator norm yields

\[
\lambda(n, d, \Gamma) \leq \max_{\rho_{AB}^{K}} \max_{\{p_{x}, \rho_{x}^{\theta} \}} \left[ \sum_{k,b} p_{k} p_{b|k} \left\| \sum_{\theta} 2^{-n} \Pi_{b}^{\theta,k} \right\| \right].
\] (B17)

For each \( b,k \) the corresponding operator norm can be bounded using Lemma 21 as follows:

\[
\left\| \sum_{\theta} 2^{-n} \Pi_{b}^{\theta,k} \right\| \leq 2^{-n} \max_{\theta} \left\| \Pi_{b}^{\theta,k} \right\|.\] (B18)
from which (B17) becomes

$$\lambda(n,d,1) \lesssim 2^{-n} \max_{\{p_{i,j}\}^{J \times n}} \sum_{k,b} p_k p_{b,k} \max_{\theta'} \sum_{\theta} \left\| \sqrt{\Pi_b^{\theta,k}} \sqrt{\Pi_b^{\theta,k'}} \right\|.$$

(B19)

**Step 3: Bound on operator overlaps**

The goal of this section is to find a bound on $\left\| \sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta,k}} \right\|$ which holds independently 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 23.** For all $\theta', \theta \in \{0,1\}^n$ and $b \in J^n$, we have

$$\left\| \sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}} \right\| \lesssim \min \left\{ 1, \sqrt{d} \prod_{k=1}^n \left( \max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} \right)^{w_k} \right\},$$

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 $\Pi_b^{\theta}$ in Step 2 and orthogonality relations of $P_{x|y|b}^{\theta'}$ 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,

$$\begin{align*}
\sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}} &= \sum_{x,y} P_{x|y|b}^{\theta'} P_{y|b}^{\theta} \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}} \\
&= \sum_{x,y} \sum_{k \in S} P_{x|y|b}^{\theta'} P_{y|b}^{\theta} \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}} \\
&= \sum_{x,y} \sum_{k \in S} \delta_{x_k,y_k} P_{y|b}^{\theta} \otimes \sqrt{F_x^{\theta'}} \sqrt{F_y^{\theta}}.
\end{align*}$$

(B21)

(B22)

where $|y_k^{\theta}|$ are the eigenvectors defined in Step 1. The notation $|y_k^{\theta}|_{b_k}$ 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 $b_k \in J$.

The sum over $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \{0,1\}^n$ can be split into a sum of variables with indices in $S$ which we will denote by $x, y$ and indices in $T$ denoted $x', y'$. The definition of $S$ implies that $x \equiv y$. Let

$$M_x := \sum_{x',y' \in \{0,1\}^n} \sum_{k \in T} \left| x_k^{\theta} \right|_{b_k} \left| y_k^{\theta} \right|_{b_k} \otimes \sqrt{F_{x'}^{\theta'}} \sqrt{F_{y'}^{\theta}},$$

(B24)

where the two strings $x'$ and $x$ together form a bit string of length $n$ and give meaning to the notation $F_{x'}^{\theta'}$ (same for $F_{x'y'}^{\theta}$). Since the register labeled as (•) consists of orthogonal projectors, the desired operator norm is achieved by a maximization over $\bar{x} \in \{0,1\}^S$. That is

$$\left\| \sqrt{\Pi_b^{\theta'}} \sqrt{\Pi_b^{\theta}} \right\| = \max_{\bar{x} \in \{0,1\}^S} \| M_\bar{x} \|. $$

(B25)

In the following we derive an upper bound which does not depend on $\bar{x}$. Since for $k \in T$ we have $\theta_k \neq \theta'_k$, we use Eq. (B5) to evaluate the inner product,

$$\left| x_k^{\theta} \right|_{b_k} \left| y_k^{\theta} \right|_{b_k} = (-1)^{x_k y_k} \cos(\beta_{b_k})^{x_k \oplus y_k} \sin(\beta_{b_k})^{x_k \oplus y_k},$$

(B26)

where $x_k \oplus y_k = 1 - x_k \oplus y_k$. Therefore,

$$M_\bar{x} = \sum_{x',y'} (-1)^{x' y'} \sum_{k \in T} \cos(\beta_{b_k})^{x_k \oplus y_k} \sin(\beta_{b_k})^{x_k \oplus y_k} \left| x_k^{\theta} \right|_{b_k} \left| y_k^{\theta} \right|_{b_k} \otimes \sqrt{F_{x'}^{\theta'}} \sqrt{F_{y'}^{\theta}},$$

(B27)

where $\forall x, y \in \{0,1\}^n, x.y := \sum_k x_k y_k$. 

062307-17
From $\|M_i\| = \sqrt{\|M_i^\dagger M_i\|}$ and the definition,

$$f(\beta_b, x', y', z') := (-1)^{x' \otimes z'} \prod_{k \in T} \cos(\beta_{bk}) \frac{\cos x_k + \cos z_k}{\sin x_k + \sin z_k},$$  \hspace{1cm} (B28)

where $\beta_b$ is a vector of angles, we simplify $M_i M_i^\dagger$ and get

$$\|M_i\| = \left\| \sum_{x', z'} \bigotimes_{k \in T} \left| \frac{\alpha_k'}{x'_k \otimes z'_k \otimes \beta_k} \right| \otimes \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \left( \sum_{y'} f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right) \sqrt{F_{y'_k z'_k}} \right\|^{1/2}. \hspace{1cm} (B29)$$

Bounding the register labeled as $(\ast)$ by its operator norm does not decrease the norm as mentioned in Lemma 21. Hence we have

$$\|M_i\| \leq \sum_{x', z'} \bigotimes_{k \in T} \left| \frac{\alpha_k'}{x'_k \otimes z'_k \otimes \beta_k} \right| \cdot \left\| \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \left( \sum_{y'} f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right) \sqrt{F_{y'_k z'_k}} \right\|^{1/2}. \hspace{1cm} (B30)$$

Bounding the outer operator norm with the Schatten two norm ($\| \cdot \| \leq \| \cdot \|_2$) gives

$$\|M_i\| \leq \sum_{x', z'} \bigotimes_{k \in T} \left| \frac{\alpha_k'}{x'_k \otimes z'_k \otimes \beta_k} \right| \cdot \left\| \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \left( \sum_{y'} f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right) \sqrt{F_{y'_k z'_k}} \right\|^{1/2} \hspace{1cm} (B31)$$

$$= \left( \sum_{x', z'} \left\| \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \left( \sum_{y'} f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right) \sqrt{F_{y'_k z'_k}} \right\|^2 \right)^{1/4}. \hspace{1cm} (B32)$$

Using submultiplicativity of the operator norm we have

$$\|M_i\| \leq \left( \sum_{x', z'} \left\| \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \right\|^2 \sum_{y'} \left\| f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right\|^2 \left\| \sqrt{\frac{F_{y'_k z'_k}}{F_{y_k z_k}}} \right\|^2 \right)^{1/4} \hspace{1cm} (B33)$$

$$= \left( \sum_{x', z'} \left\| \sqrt{\frac{F_{x'_k z'_k}}{F_{x_k z_k}}} \right\|^2 \sum_{y'} \left\| f(\beta_b, x', y', z') F_{y'_k}^{\beta} \right\|^2 \left\| \sqrt{\frac{F_{y'_k z'_k}}{F_{y_k z_k}}} \right\|^2 \right)^{1/4}. \hspace{1cm} (B34)$$

From the definition of $f(\beta_b, x', y', z')$ in (B28) it is easy to see that

$$|f(\beta_b, x, y, z)| \leq \prod_{k \in T} \max \left\{ \cos^2 \beta_{bk}, \sin^2 \beta_{bk} \right\}. \hspace{1cm} (B35)$$

Since this bound does not depend on $y'$ we can take it out of the sum,

$$(\ast) \leq \prod_{k \in T} \max \left\{ \cos^4 \beta_{bk}, \sin^4 \beta_{bk} \right\} \sum_y \left\| F_{y'_k}^{\beta} \right\|^2 \hspace{1cm} (B36)$$

$$\leq \prod_{k \in T} \max \left\{ \cos^4 \beta_{bk}, \sin^4 \beta_{bk} \right\}. \hspace{1cm} (B37)$$
The latter inequality holds because \(\sum_j F_{ij}^\theta \leq 1\). Using this bound in (B34) gives us

\[
\| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq \prod_{k \in T} \max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} \left[ \sum_{x \leq z} \| F_{ix}^\theta \| \| F_{ix}^{0,\theta} \| \right]^{1/4}
\]

(0.0438)

\[
= \prod_{k \in T} \max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} \left[ \sum_{x \leq z} \| F_{ix}^\theta \| \right]^{1/2}
\]

(0.0439)

\[
\leq \sqrt{d} \prod_{k \in T} \max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \},
\]

(0.0440)

where in the last inequality we use the observation that for all \(\tilde{x} \in \{0,1\}^{n-1}\),

\[
\sum_{x \leq z} \| F_{ix}^\theta \| \leq \sum_{x \leq z} \text{tr} \left( F_{ix}^{0,\theta} \right) = \text{tr} \left( \sum_{x \leq z} F_{ix}^{0,\theta} \right) \leq \text{tr}(\mathbb{I}_d) = d,
\]

(B41)

since Bob’s quantum memory is of dimension at most \(d\). Combining this bound with the trivial bound \(\| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq 1\) completes the proof.

Lemma 24. For all \(\theta', \theta \in \{0,1\}^n\) and \(b \in \mathcal{J}_n\), we have

\[
\| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq \min \left\{ 1, \sqrt{d} \prod_{k=1}^n \left( \frac{1 + \epsilon_{b_k}}{2} \right)^{w_k/2} \right\},
\]

(B42)

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 \(b \in \mathcal{J}_n\),

\[
\epsilon_{b_k} := |\cos 2 \beta_{b_k}| = \begin{cases} 
\cos 2 \beta_{b_k} & \text{if } \beta_{b_k} \in [0,\pi/4] \\
-\cos 2 \beta_{b_k} & \text{if } \beta_{b_k} \in [\pi/4,\pi/2]
\end{cases}.
\]

(0.0443)

If \(\beta_{b_k} \in [0,\pi/4]\) then \(\cos \beta_{b_k} \geq \sin \beta_{b_k}\) and

\[
\max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} = \cos \beta_{b_k} = \sqrt{\frac{1 + \cos 2 \beta_{b_k}}{2}} = \sqrt{\frac{1 + \epsilon_{b_k}}{2}}.
\]

(B44)

Similarly, if \(\beta_{b_k} \in [\pi/4,\pi/2]\) then \(\sin \beta_{b_k} \geq \cos \beta_{b_k}\) and

\[
\max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} = \sin \beta_{b_k} = \sqrt{\frac{1 - \cos 2 \beta_{b_k}}{2}} = \sqrt{\frac{1 + \epsilon_{b_k}}{2}}.
\]

(B45)

Plugging

\[
\max \{ \cos \beta_{b_k}, \sin \beta_{b_k} \} = \sqrt{\frac{1 + \epsilon_{b_k}}{2}}.
\]

(B46)

into Lemma 23 completes the proof.

---

**Step 4: Completing the proof**

In this section we first we bound Bob’s winning probability in terms of the absolute anticommutator \(\epsilon_+\), 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 \(\epsilon_+\). That’s to say we show that

Lemma 25. In (B19) we bounded the winning probability in terms of \(\Lambda\), which can be further bounded as follows:

\[
\Lambda = 2^{-n} \sum_{k,b} p_k p_{b_k} \max_{\theta'} \sum_{\theta} \| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq 2^{-n} \sum_w \min(1, g(\tilde{\epsilon}_+, w)).
\]

(B47)

where \(w := \theta' \oplus \theta \in \{0,1\}^n\), \(\epsilon_+ = \sum_{j \in \mathcal{J}} p_j \epsilon_j\), \(\tilde{\epsilon}_+ \) is the vector \((\epsilon_+, \epsilon_+, \ldots, \epsilon_+)\), and

\[
g(\tilde{a}, w) := \sqrt{d} \prod_{k=1}^n \left( \frac{1 + a_k}{2} \right)^{w_k/2},
\]

where \(\tilde{a}\) is a vector \((a_1, \ldots, a_k, \ldots, a_n)\).

Proof. Define

\[
g(\epsilon_b, w) = \sqrt{d} \prod_{k=1}^n \left( \frac{1 + \epsilon_{b_k}}{2} \right)^{w_k/2}, \quad w := \theta' \oplus \theta \in \{0,1\}^n.
\]

(B48)

When we apply Lemma 24 we get the bound,

\[
\max_{\theta'} \sum_{\theta} \| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq 2^{-n} \max_{\theta'} \sum_w \min(1, g(\epsilon_b, w)).
\]

(B49)

From (B48), we observe that

\[
\max_{\theta'} \sum_{\theta} \min(1, g(\epsilon_b, w)) = \sum_w \min(1, g(\epsilon_b, w)),
\]

(B50)

because the objective function to be maximized is independent of \(\theta'\). The objective function in the optimization of (B19) can be bounded as

\[
\sum_{k,b} p_k p_{b_k} \max_{\theta'} \sum_{\theta} 2^{-n} \| \sqrt{\prod_b \sqrt{\prod_b}} \| \leq \sum_{k,b} p_k p_{b_k} 2^{-n} \sum_w \min(1, g(\epsilon_b, w)),
\]

(B51)
where the inner expression is independent of $k$. This is the uniform bound we mentioned. Performing the sum over $k$ first gives

$$
\sum_k p_k p_{b_k} = \sum_k p_k \text{tr} \left( S_b \otimes 1_B \rho_{AB}^{k} S_b \otimes 1_B \right)
$$

which is the uniform bound we mentioned. Performing the sum over $k$ first gives

$$
\sum_k p_k \text{tr} \left( S_b \otimes 1_B \rho_{AB}^{k} S_b \otimes 1_B \right)
$$

where $p_b$ for $b \in J$ has been defined before (B7).

Hence we see explicitly that while the attack of Bob may induce $p_b$ non-i.i.d. for some $k$, on average he cannot influence Alice’s local i.i.d. state and therefore $p_b$ remains i.i.d.

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,

$$
2^{-n} \sum_{b,w} p_b \min(1,g(\epsilon_b,w)) \leq 2^{-n} \sum_w \min \left( 1, \sum_b p_b g(\epsilon_b,w) \right).
$$

The sum inside the minimum,

$$
\sum_b p_b g(\epsilon_b,w) = \sum_b p_b \sqrt{d} \prod_{k=1}^n \left( 1 + \frac{\epsilon_{b_k}^2}{2} \right)^{w_k/2}
$$

is a product of sums because $p_b$ is a product [see Eq. (B55)]:

$$
\sum_b p_b g(\epsilon_b,w) = \sqrt{d} \prod_{k=1}^n \sum_{j \in J} p_j \left( 1 + \frac{\epsilon_j}{2} \right)^{w_k/2}.
$$

FIG. 5. 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-qubit 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.
Now each sum in the product can be bounded because of the concavity of the square root we get

$$\sum_b p_b g(\epsilon_b, w) \leq \sqrt{d} \prod_{k=1}^{n} \left( \frac{1 + \epsilon_k - \frac{1}{2}}{2} \right)^{w_k/2} = g(\bar{\epsilon}_+, w), \quad (B60)$$

hence we have

$$2^{-n} \sum_{b, w} p_b \min(1, g(\epsilon_b, w)) \leq 2^{-n} \sum_{w} \min(1, g(\bar{\epsilon}_+, w)),$$  \quad (B61)

where $\epsilon_+ = \sum_{j \in J} p_j \epsilon_j$ and $\bar{\epsilon}_+$ 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 $\xi$.

Lemma 26. In the perfect guessing game where Alice’s devices behave i.i.d. and Bob has a quantum memory of dimension $d$, his winning probability is bounded by

$$\lambda(n,d,\Gamma') \leq 2^{-n} \left[ \sum_{k=0}^{t} \binom{n}{k} + \sqrt{d} \sum_{k=t+1}^{n} \binom{n}{k} \left( \frac{1 + \frac{\xi}{2}}{2} \right)^{k/2} \right],$$  \quad (B63)

where $t$ is the threshold defined as

$$t := \left\lfloor -\log_2 d \cdot \left\lfloor \log_2 \left( \frac{1 + \frac{\xi}{2}}{2} \right) \right\rfloor \right\rfloor^{-1}, \quad (B64)$$

and $\xi := \frac{S}{\sqrt{8} - S^2}$ with $S$ being the CHSH violation as defined in Lemma 4.

**Proof.** Combine (B62) with (B48) and (B19) 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

$$\lambda(n,d,\Gamma') \leq 2^{-n} \sum_{w} \min \left\{ 1, \sqrt{d} \prod_{k=1}^{n} \left( \frac{1 + \epsilon_+ - \frac{1}{2}}{2} \right)^{w_k/2} \right\}.$$  \quad (B65)

Using Lemma 4 we have $\epsilon_+ \leq \xi$ and then

$$\lambda(n,d,\Gamma') \leq 2^{-n} \sum_{w} \min \left\{ 1, \sqrt{d} \prod_{k=1}^{n} \left( \frac{1 + \xi}{2} \right)^{w_k/2} \right\}. \quad (B66)$$

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

$$\lambda(n,d,\Gamma') \leq 2^{-n} \left[ \sum_{k=0}^{t} \binom{n}{k} + \sqrt{d} \sum_{k=t+1}^{n} \binom{n}{k} \left( \frac{1 + \frac{\xi}{2}}{2} \right)^{k/2} \right],$$  \quad (B67)

where $t$ is the threshold defined in the lemma.

**APPENDIX C: CHEATING STRATEGY USING UNLIMITED QUANTUM CHANNELS**

Figure 5 shows how using unbounded quantum channels one can store (left) and create (right) an arbitrary amount of entanglement without having access to more than four-qubit 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.


[33] O. Regev, Witness-preserving QMA amplification, in Quantum Computation Lecture Notes, Spring 2006 (Tel Aviv University, Tel Aviv, 2006).

