Key rates for quantum key distribution protocols with asymmetric noise

Murta, Gláucia; Rozpdek, Filip; Ribeiro, Jérémy; Elkouss, David; Wehner, Stephanie

DOI
10.1103/PhysRevA.101.062321

Publication date
2020

Document Version
Final published version

Published in
Physical Review A

Key rates for quantum key distribution protocols with asymmetric noise

Gláucia Murta,[1,2] Filip Rozpędek,[1,3] Jérémy Ribeiro,[1,3] David Elkouss,[1] and Stephanie Wehner[1,3]
[1]*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2]*Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, D-40225 Düsseldorf, Germany*
[3]*Kavli Institute of Nanoscience, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*

(Received 29 February 2020; accepted 8 May 2020; published 11 June 2020)

We consider the asymptotic key rates achieved in the simplest quantum key distribution protocols, namely, the BB84 and the six-state protocols when nonuniform noise is present in the system. We first observe that higher qubit error rates do not necessarily imply lower key rates. Second, we consider protocols with advantage distillation and show that it can be advantageous to use the basis with higher quantum bit error rate for the key generation. We then discuss the relation between advantage distillation and entanglement distillation protocols. We show that applying advantage distillation to a string of bits formed by the outcomes of measurements in the basis with a higher quantum bit error rate is closely connected to the two-to-one entanglement distillation protocol of Deutsch-Ekert-Jozsa-Macchiavello-Popescu-Sanpera [Phys. Rev. Lett. **77**, 2818 (1996)]. Finally, we discuss the implications of these results for implementations of quantum key distribution.

DOI: 10.1103/PhysRevA.101.062321

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is one of the most remarkable examples of the power of quantum mechanics. Many classical cryptosystems used for secure communication nowadays are based on computational assumptions. Computational assumptions make these systems vulnerable to retroactive attacks in case more powerful quantum computers become available in the future. In contrast, quantum mechanics allows two parties to distribute a key achieving information-theoretic security. This means that security is guaranteed even against an eavesdropper that has unlimited classical and quantum resources. Secure communication can then be achieved if this key is used in a one-time pad scheme [3,4] (for a discussion about the assumptions present in a QKD implementation, see Ref. [5]).

Near-term quantum technologies suffer from imperfections. Therefore, even in the absence of an active eavesdropper, a QKD implementation will be subjected to a finite amount of noise. In order to guarantee security, one is interested in designing protocols that can tolerate levels of noise compatible with current technology and, at the same time, achieve the highest possible key rates.

The simplest proposed QKD protocol, BB84 [1], is based on the conjugate coding ideas developed by Wiesner in Ref. [6]. In the BB84, Alice prepares a single qubit state in one of the eigenstates of the Z-basis $\{|0\rangle, |1\rangle\}$ or one of the eigenstates of the X-basis $\{|+\rangle, |-\rangle\}$. An extension of the BB84, exploring three conjugate bases, was proposed in Ref. [7] and is called the six-state protocol. In the six-state protocol, Alice can also prepare the qubit in one of the eigenstates of the Y-basis $\{|+_Y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), |-_Y\rangle \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$. The six-state protocol was proven to be more robust to noise [7]. Intuitively, this is due to the fact that more parameters are characterized during the protocol, therefore, restricting the possible actions of a potential eavesdropper.

In this article, we consider the asymptotic key rates that can be obtained in the BB84 and six-state protocols as a function of the quantum bit error rates (QBERs). We first consider instances of these protocols in which information reconciliation and privacy amplification are applied directly to the raw keys formed by the outcomes of Alice's and Bob's measurements. Then, we consider the case when, additionally, a subroutine that allows Alice and Bob to select more correlated parts of their string, namely, advantage distillation, is applied to the raw keys before information reconciliation. We discuss observed counterintuitive behaviors of the asymptotic key rates with the QBER. As our main result, we show that, in the presence of asymmetric noise, higher key rates may be obtained if the basis with a higher QBER is used for the key generation in protocols with advantage distillation. This can have a direct impact for implementations that make use of advantage distillation [8]. Finally, we show that implementing the six-state protocol with advantage distillation and measurements in the basis with a higher QBER is closely connected to the two-to-one entanglement distillation protocol of Deutsch-Ekert-Jozsa-Macchiavello-Popescu-Sanpera (DEJMPS) [9].

The paper is organized as follows: In the remainder of this section, we detail the general structure of the QKD protocols under consideration. In Sec. II, we first consider the asymptotic key rates of the BB84 and the six-state protocols without advantage distillation. We then proceed to analyze the effect of advantage distillation and show interesting behaviors of the key rates as a function of the QBERs. In Sec. III, we discuss the relation of QKD and entanglement distillation protocols. Finally, in Sec. IV, we discuss the implications of our results to experimental implementations.

Quantum key distribution protocols

For an implementation of the BB84 or six-state protocols, the only required resources are the preparation, transmission,

and measurement of single-qubit states. That is, these protocols can be implemented in a prepare-and-measure setup without the need of entanglement. However, both protocols have an equivalent entanglement-based implementation [2,10] in which a source (that may be in Alice's laboratory) produces a state that is distributed to Alice and Bob (ideally the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$). Then, upon receiving their systems, Alice and Bob perform measurements in randomly chosen bases (having two choices of basis for the BB84, and three for the six-state protocol). As long as the measurement devices are well characterized and controlled, an entanglement-based implementation allows one to relax the need for a precise characterization of the state preparation. The entanglement-based version of the BB84 and six-state protocols played a key role to formalize their security proofs [11–13]. From now on, for the purpose of our analyses, we focus on the entanglement-based version of these protocols. However, we remark that, for all our results, there is an equivalent implementation that requires only single-qubit states preparation.

The BB84 and the six-state protocols can be described by four main steps:

(1) *Distribution and measurements*. Alice uses the source to produce a two-qubit state. She keeps one qubit and sends the other to Bob using a quantum channel. Upon receiving the systems, Alice and Bob, each randomly chooses a basis and performs the corresponding measurement. They repeat this procedure N times. With the outcomes of their measurements, they establish a string of N bits each.

(2) *Sifting and parameter estimation*. Alice and Bob communicate the measurement bases and discard the rounds in which different bases were used. Moreover, they sacrifice m bits in order to estimate their average correlation and decide whether to abort or proceed with the protocol. If the protocol does not abort, the remaining n bits constitute the raw key.

(3) *Advantage distillation (optional)*. The goal is to classically postprocess the raw key in order to increase the correlation between Alice and Bob and get an advantage over the eavesdropper.

(4) *Information reconciliation and privacy amplification*. In this step, Alice and Bob first implement an information reconciliation protocol that allows Bob to correct his bit string for errors. Finally, they apply a privacy amplification protocol to transform a partially secure key of n bits into a secure key of $l < n$ bits.

The parameters estimated in Step 2 are determined by the particular protocol. In an implementation of the BB84 protocol, Alice and Bob can estimate the values of the QBERs in the X and Z bases Q_X and Q_Z. For the six-state protocol, they will also have an estimate of the QBER in the Y-basis Q_Y. The QBER in the $Z(X)$-basis $Q_Z(Q_X)$ is the probability that Alice and Bob get different outcomes when they both measure their systems in the basis $Z(X)$. The QBER in the Y basis is defined in a similar way, however, since the target state $|\Phi^+\rangle$ exhibits anticorrelation in the Y basis, Bob flips his outcomes whenever he chooses to measure in the Y basis.

In the originally proposed BB84 and six-state protocols, all the bases were chosen with equal probability among the set of bases specified by the protocols. However, as shown in Ref. [14], the efficiency of these protocols can be increased without compromising security if one of the bases is chosen with a higher probability. Then, in the asymptotic limit, the preferred basis is used almost all the time. The remaining bases are used only occasionally in order to test for the eavesdropper. This significantly increases the key rates as only a small fraction of the rounds are discarded in the sifting process. In these protocols, the raw key is usually created from the rounds in which the preferred basis is used. The remaining rounds in which other bases were chosen are used for parameter estimation. For this reason, we denote the basis chosen with higher probability as the *key generation basis*.

Advantage distillation in Step 3 is an optional step. It consists of Alice and Bob using two-way classical communication to select parts of the raw key that exhibit stronger correlation. This method was introduced in the context of classical protocols [15] and was proven to be useful for quantum protocols as well [16,17]. Usually, advantage distillation leads to significant drops in the key rate for the low noise regime, but it can considerably increase the noise tolerance of a protocol. For example, a BB84 implementation subjected to depolarizing noise (in which $Q_X = Q_Z$) without advantage distillation can tolerate up to 11% QBER. If some advantage distillation is performed, the noise tolerance can be increased to 20% QBER [16]. Advantage distillation protocols that have better performance in the low noise regime were also proposed [18].

Information reconciliation in Step 4 aims at correcting Bob's string in order to make it equal to Alice's string. Information reconciliation can be implemented using only one-way communication from Alice to Bob. Interactive protocols [19], which are efficient to implement, are broadly used in QKD implementations [20]. These protocols require two-way communication, however, they should not be confused with advantage distillation performed in Step 3. In advantage distillation, two-way communication is essential and, moreover, both Alice's and Bob's strings are modified during the protocol.

II. RESULTS

A. Key rates for protocols without advantage distillation

We first consider the BB84 and the six-state protocols when Alice and Bob skip Step 3. After measuring their quantum systems, Alice and Bob proceed to perform information reconciliation and privacy amplification. Information reconciliation protocols based on two-universal hashing functions leak the minimum amount of information necessary to correct for errors in Bob's string [19]. In Ref. [21], it was proven that the minimum leakage of a one-way information reconciliation protocol is given by $nH(A|B) + O(\sqrt{n})$, where $H(A|B)$ is the entropy of Alice's output conditioned on Bob's output, defined as $H(A|B) = -\sum_{a,b} p(A = a,\ B = b) \log_2 p(A = a|B = b)$ with $p(A = a,\ B = b)$ being the probability that Alice and Bob obtain outcomes a and b, respectively, for the measurement in consideration, $p(A = a|B = b) = \frac{p(A=a,\ B=b)}{p(B=b)}$ is the conditional probability, and the logarithms are taken in basis 2.

In order to analyze the key rate of the BB84 and the six-state protocol, we can assume without loss of generality that the state distributed by the source is a Bell-diagonal state [13],

$$\rho = \lambda_{00}\Phi_{00} + \lambda_{01}\Phi_{01} + \lambda_{10}\Phi_{10} + \lambda_{11}\Phi_{11}, \tag{1}$$

where $\Phi_{ij} = |\Phi_{ij}\rangle\langle\Phi_{ij}|$ and $|\Phi_{ij}\rangle = X^i Z^j \otimes I|\Phi^+\rangle$. Restricting the analysis to Bell-diagonal states is sufficiently general because, for all states ρ' such that $\lambda_{ij} = \langle\Phi_{ij}|\rho'|\Phi_{ij}\rangle$, the corresponding Bell-diagonal state exhibits the same QBERs as the original state and leads to the lowest key rate [13].

For the security analysis, it is also assumed that the measurements are perfect, and all the noise can be mapped into the distributed state. In this case, the Bell coefficients $\{\lambda_{ij}\}$ relate to the QBERs Q_X, Q_Y, and Q_Z by the following:

$$\begin{aligned}
\lambda_{00} &= 1 - \frac{(Q_X + Q_Y + Q_Z)}{2}, \\
\lambda_{01} &= \frac{Q_X + Q_Y - Q_Z}{2}, \\
\lambda_{10} &= \frac{-Q_X + Q_Y + Q_Z}{2}, \\
\lambda_{11} &= \frac{Q_X - Q_Y + Q_Z}{2}.
\end{aligned} \tag{2}$$

Note that a Bell-diagonal state is completely characterized by the three QBERs (Q_X, Q_Y, Q_Z).

The key rates for the BB84 and the six-state protocols can be determined as a function of the coefficients of the estimated Bell-diagonal state and, therefore, as a function of the QBERs. In a real implementation in which a finite number of rounds is considered, statistical effects play a role in the value of the key rate. However, for a sufficiently large number of rounds, the key rate of the six-state protocol with Z being the key generation basis approaches the asymptotic value given by [12,13,22]

$$R_{\text{six-state}} = 1 - H(\{\lambda_{ij}\}), \tag{3}$$

where $H(\{\lambda_{ij}\}) = \sum_{ij} -\lambda_{ij}\log_2\lambda_{ij}$, and the logarithms are taken in basis 2.

For BB84, since information about Q_Y is not available, the key rate is given by the minimum over all possible values of Q_Y. This results in [11,13,22]

$$R_{\text{BB84}} = 1 - h(Q_X) - h(Q_Z), \tag{4}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy.

If one of the other available bases is used for the key generation, the corresponding key rate can be obtained by simply permuting the QBERs in expressions (3) and (4). Note that choosing the basis for key generation implies a choice of protocol. Once the key generation basis is fixed, Alice and Bob can run the protocol using this basis for almost all the rounds. The key rate now depends on the information available to the eavesdropper when the estimated state, given in Eq. (1), is measured in the chosen key generation basis. A measurement in the X basis, or the Y basis, performed on the estimated state, Eq. (1), can be seen as a Z-basis measurement performed on a rotated state. The corresponding rotated state for when the X basis, or the Y basis, is used for the key generation measurement relates to Eq. (1) by a permutation of the coefficients $\{\lambda_{ij}\}$. Equations (3) and (4) are invariant under permutation of the QBERs. Therefore, the resulting key rate for protocols that use information reconciliation with minimum leakage is the same regardless of which of the available bases is chosen for the key generation rounds. This is stated in Proposition 1.

Proposition 1. In an implementation of the BB84 or the six-state protocol in which an information reconciliation protocol with minimum leakage is used, the asymptotic key rate does not depend on which of the available bases is chosen as the key generation basis.

Remark. It is important to remark that Proposition 1 takes into account that information reconciliation is performed using a protocol with minimum leakage. The minimum leakage is asymptotically given by $h(Q_M)$, where M is the basis used for the key generation rounds, $M \in \{X, Z\}$ for BB84 and $M \in \{X, Y, Z\}$ for the six-state protocol. Information reconciliation protocols with minimum leakage cannot be implemented in practice, and protocols that have higher leakage are used instead. There exist efficient information reconciliation protocols with asymptotic leakage given by $fh(Q_M)$, where $f \leqslant 1.2$ [23–25]. The use of a suboptimal information reconciliation protocol creates an asymmetry of the QBERs in the key rate, and in this case, in order to maximize the key, it is advantageous to choose the basis with the lowest QBER for the key generation rounds.

Now, we state an interesting fact regarding the key rates of the six-states protocol when an information reconciliation protocol with minimum leakage is used.

Observation 1. For fixed values of Q_X and Q_Z, the key rate is *not* a monotonically decreasing function of Q_Y.

Proof. If we fix the values of Q_X and Q_Z in order to ensure positivity of the corresponding Bell-diagonal state, the possible values of Q_Y are in the range,

$$|Q_X - Q_Z| \leqslant Q_Y \leqslant Q_X + Q_Z. \tag{5}$$

Additionally, we require that $Q_X + Q_Y + Q_Z < 1$ in order to have an entangled state. One can see this by inspecting Eq. (2).

Now, evaluating the derivative of the key rate, Eq. (3), with respect to Q_Y, we conclude that the minimum occurs for

$$Q_Y^* = Q_X + Q_Z - 2Q_X Q_Z, \tag{6}$$

which can be strictly smaller than the maximum attainable value for Q_Y. ■

Observation 1 is illustrated in Fig. 1 for the family of Bell-diagonal states $(Q_X = 0.1,\ Q_Y, Q_Z = 0.1)$.

Note that the minimum of the curve in Fig. 1 gives the key rate for the BB84 protocol when $Q_X = Q_Z = 0.1$.

Observation 1 together with the continuity of the key rate for the six-state protocol implies the following corollary.

Corollary 1. There exists a state $\rho^{(1)}$ with QBERs $(Q_X^{(1)}, Q_Y^{(1)}, Q_Z^{(1)})$ and a state $\rho^{(2)}$ with QBERs $(Q_X^{(2)}, Q_Y^{(2)}, Q_Z^{(2)})$ such that

$$Q_X^{(1)} > Q_X^{(2)}, \quad Q_Y^{(1)} > Q_Y^{(2)}, \quad Q_Z^{(1)} > Q_Z^{(2)},$$

and

$$R_{\text{six-state}}(\rho^{(1)}) > R_{\text{six-state}}(\rho^{(2)}).$$

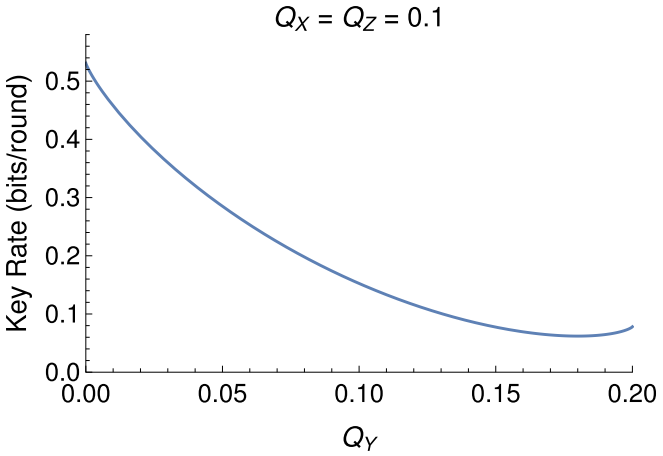

FIG. 1. Asymptotic key rate of the six-state protocol with minimum leakage information reconciliation as a function of the QBER in the Y basis Q_Y for the family of Bell-diagonal states with $Q_X = Q_Z = 0.1$.

As an example of Corollary 1, take $\rho^{(1)}$ to be the state with QBERs $Q_X^{(1)} = Q_Z^{(1)} = 10\%$ and $Q_Y^{(1)} = 20\%$, and $\rho^{(2)}$ to be the state with $Q_X^{(2)} = Q_Z^{(2)} = 9.8\%$ and $Q_Y^{(2)} = 18\%$. It holds that $R_{\text{six-state}}(\rho^{(1)}) > R_{\text{six-state}}(\rho^{(2)})$.

We, now, investigate the behavior of the singlet fidelity and the entanglement of formation [26] for the family of states considered in Fig. 1.

For an entangled Bell-diagonal state ρ, Eq. (1), with $\lambda_{00} > \frac{1}{2}$, the entanglement of formation [26] (EoF) is given by

$$\text{EoF}(\rho) = h\left(\tfrac{1}{2} + \sqrt{\lambda_{00}(1-\lambda_{00})}\right), \tag{7}$$

and the singlet fidelity F is

$$F(\rho) = \lambda_{00}. \tag{8}$$

Figure 2 illustrates that both quantities are monotonically decreasing functions of Q_Y. This supports the intuition that a state with higher QBER is less close to the ideal state. However, as stated in Observation 1 (see also Fig. 1), this monotonic behavior is not always observed in the key rates of the six-state protocol.

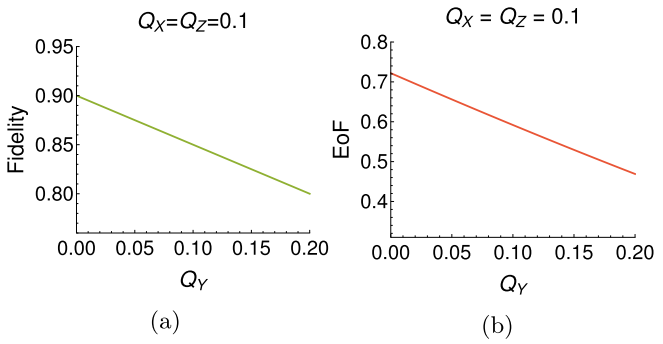

FIG. 2. (a) Singlet fidelity and (b) entanglement of formation for the family of Bell-diagonal states specified by QBERs $(0.1, Q_Y, 0.1)$. Both quantities decrease monotonically as Q_Y increases in the range of possible values of Q_Y, $0 \leqslant Q_Y \leqslant 0.2$.

B. Key rates for protocols with advantage distillation

We now consider the BB84 and the six-state protocols when advantage distillation is employed in Step 3. In particular, we consider the advantage distillation protocol [13,17,27] described in Protocol I.

The key rates for the BB84 and six-state protocols with advantage distillation, Protocol I, were derived in Refs. [13,17]. For the six-state protocol, the key rate is given by

$$R^{AD}_{\text{six-state}} = \tfrac{1}{2} p^{AD}_{\text{succ}} [1 - H(\{\tilde{\lambda}_{ij}\})], \tag{9}$$

where p^{AD}_{succ} is the probability that Protocol I succeeds, i.e., that Alice and Bob do not discard a block. This occurs if either the two bits of Alice and Bob are equal or if both bits in the block are flipped. Note that steps 3 and 4 of Protocol I check whether the pair of bits of Alice and the pair of bits of Bob have the same parity. If the raw key is generated by measurements in the Z basis, then

$$\begin{aligned} p^{AD}_{\text{succ}} &= (\lambda_{00} + \lambda_{01})^2 + (\lambda_{10} + \lambda_{11})^2 \\ &= Q_Z^2 + (1 - Q_Z)^2. \end{aligned} \tag{10}$$

And the coefficients $\{\tilde{\lambda}_{ij}\}$ are given by

$$\begin{aligned} \tilde{\lambda}_{00} &= \frac{(\lambda_{00} + \lambda_{01})^2 + (\lambda_{00} - \lambda_{01})^2}{2 p^{AD}_{\text{succ}}}, \\ \tilde{\lambda}_{01} &= \frac{(\lambda_{00} + \lambda_{01})^2 - (\lambda_{00} - \lambda_{01})^2}{2 p^{AD}_{\text{succ}}}, \\ \tilde{\lambda}_{10} &= \frac{(\lambda_{10} + \lambda_{11})^2 + (\lambda_{10} - \lambda_{11})^2}{2 p^{AD}_{\text{succ}}}, \\ \tilde{\lambda}_{11} &= \frac{(\lambda_{10} + \lambda_{11})^2 - (\lambda_{10} - \lambda_{11})^2}{2 p^{AD}_{\text{succ}}}, \end{aligned} \tag{11}$$

where $\{\lambda_{ij}\}$'s relate to the QBERs by Eq. (2).

In Refs. [13,17], it was shown that applying advantage distillation, Protocol I, has the same effect as if Alice and Bob would apply a quantum operation that brings two copies of a Bell-diagonal state with coefficients $\{\lambda_{ij}\}$ into one copy of a Bell-diagonal state with coefficients $\{\tilde{\lambda}_{ij}\}$ and then perform the measurement in this final state. This operation succeeds with probability p^{AD}_{succ}. We will see, in Sec. III, that the corresponding quantum operation is the application of bilocal CNOT gates (i.e., Alice applies a CNOT to her two subsystems, and Bob does the same to his subsystems), followed by measurements of the target qubits and postselection of the results.

The key rate for the BB84 protocol is obtained by taking the minimum of Eq. (9) over all possible values of Q_Y.

Note that, for protocols with advantage distillation, the key rate, Eq. (9), is not symmetric over permutation of the QBERs. Therefore, choosing a different basis (among the set of available bases) for key generation may lead to different key rates. We now state a curious observation about QKD protocols in which advantage distillation, given by Protocol I, is performed.

Observation 2. In an implementation of the BB84 or the six-state protocol in which advantage distillation, given by Protocol I, is performed, higher key rates may be obtained if

Protocol I: Advantage distillation.

Let $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ be strings of bits held by Alice and Bob, respectively.
1: Alice and Bob divide their strings in blocks of two consecutive bits.
2: **for** each block j of size 2 **do**
3: Alice chooses a random bit $r \in \{0, 1\}$ and publicly communicates $(c_{j_1}, c_{j_2}) := (a_{j_1} \oplus r, a_{j_2} \oplus r)$ to Bob.
4: Bob checks whether $(b_{j_1} \oplus c_{j_1}, b_{j_2} \oplus c_{j_2}) \in \{\vec{0}, \vec{1}\}$. If that is the case he accepts, $acc = 1$, else he sets $acc = 0$.
5: Bob communicates acc to Alice.
6: If $acc = 1$, Alice keeps a_{j_1}, and Bob keeps b_{j_1} for their raw key. Else they discard the two bits of the block.
7: **end for**

the basis with the higher QBER is used for the key generation rounds.

Figure 3 illustrates Observation 2 for the family of states $Q_X = Q_Z = 0.1$ considered in the previous section. In comparison with Fig. 1, we note that, for lower values of Q_Y, higher rates are obtained when no advantage distillation is performed. However, as Q_Y increases, an advantage is obtained with the use of advantage distillation and, especially, if the basis with higher QBER is used for the key generation rounds. Note also that, similar to Observation 1, an increase in the key rate with Q_Y for high values of Q_Y is also observed for the key generated with measurements in the Y basis.

In order to explore Observation 2 in more detail, we have performed an extensive numerical check over the range of possible values of QBERs (Q_X, Q_Y, Q_Z). For the BB84 protocol, Fig. 4 illustrates that, for almost all the values of Q_X and Q_Z that lead to positive key, the highest asymptotic key rate is obtained when the key generation basis is the one with a higher QBER. This behavior inverts only for a small range of parameters, next to the limiting region where positive key can no longer be obtained. It is interesting to note that the success probability of the advantage distillation protocol, given in Eq. (10), is a monotonically decreasing function of the QBER of the key generation basis. However, even with the contribution of this factor to the key rate, see Eq. (9), Fig. 4 shows that it is typically advantageous to use the basis with a higher QBER for the key generation rounds.

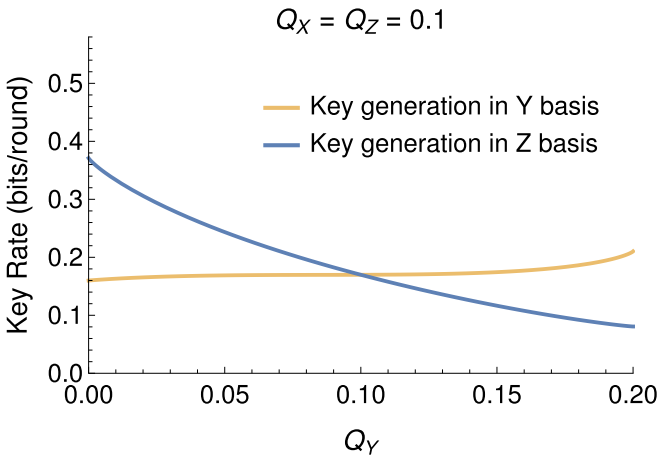

FIG. 3. Key rates for the six-state protocol with advantage distillation, given by Protocol I, for the family of states $Q_X = Q_Z = 0.1$. Blue (dark gray) curve shows the key rate when the Z basis is used for key generation, and the yellow (light gray) curve when the Y basis is used for key generation.

For the six-state protocol, we numerically compared, for the range of allowed parameters, the rates achieved when each of the three bases is used for key generation. Similar to the BB84 case, we observed that higher key rates are obtained for key generation in the basis with higher QBER except for a small range of parameters. We found that it is not advantageous to use the basis with higher QBER for key generation only for some range of QBERs (Q_X, Q_Y, Q_Z) next to the region where no key can be obtained. As an example, for a state with QBERs $(Q_X = 0.39,\ Q_Y = 0.39,\ Q_Z = 0.01)$, one can obtain a secret key only if the Z basis is used for key generation in the six-state protocol with advantage distillation given by Protocol I.

It is interesting to remark that the advantage of using the basis with higher QBERs for protocols with advantage distillation can also occur in practical implementations where information reconciliation is performed using an one-way

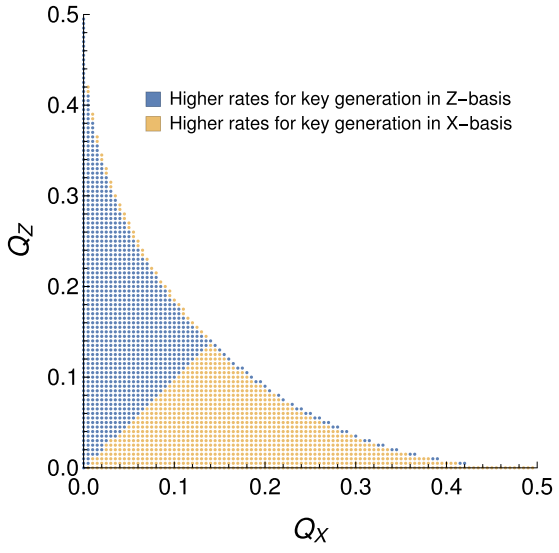

FIG. 4. Comparison of the key rates for the BB84 protocol with advantage distillation given by Protocol I when the X and the Z bases are used for the key generation. The blue (dark gray) dots represent the parameters for which higher key rates are achieved when Z is the key generation basis. The yellow (light gray) dots represent the case when higher rates are achieved if X is used for key generation. One can observe that, for almost all ranges of parameters, higher rates are obtained when the basis with higher QBER is used for key generation. This behavior only inverts for a small range of parameters, near the limiting region where positive key can no longer be extracted.

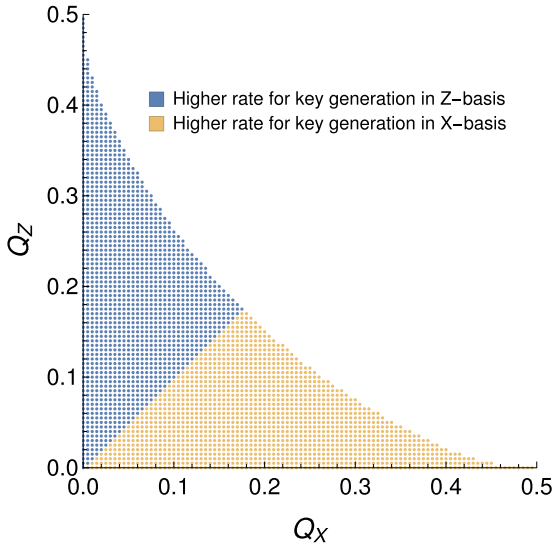

FIG. 5. Comparison of the key rates for the BB84 protocol with an advantage distillation protocol that uses blocks of size 7. The blue (dark gray) dots represent the parameters for which higher key rates are achieved when the Z basis is used for key generation. The yellow (light gray) dots represent the case when higher key rates are achieved with measurements in the X basis. For this case, it is advantageous to always use the basis with higher QBER for key generation.

protocol [23–25] with nonoptimal asymptotic leakage $fh(Q_M)$ for $f \leqslant 1.2$. Indeed, the advantage obtained by the use of a basis with higher QBER can be sufficiently large to compensate for the penalty of using an efficient information reconciliation protocol with higher leakage.

Protocol I can be generalized to blocks of arbitrary size b [15]. Even though this leads to a significant decrease in the key rate in the low noise regime, higher noise tolerance can be achieved [16,17,27]. Figure 5 illustrates the behavior of the key rates for the BB84 with advantage distillation using blocks of size 7. We now find that it is advantageous to use the basis with the higher QBER for key generation in all the ranges of parameters that lead to a positive key rate.

In Ref. [18], Watanabe *et al.* introduced an advantage distillation protocol that does not suffer from a big drop of the key rate in the low noise regime. The protocol introduced in Ref. [18] contains Protocol I as a subroutine, and, in the high noise regime, the key rate coincides with the one obtained using Protocol I. Therefore, we expected that Observation 2 may also have an impact in this protocol. Indeed, in Fig. 6, we illustrate that choosing the basis with the higher QBER for key generation leads to higher rates for the family of states $Q_X = Q_Z = 0.1$ when the advantage distillation protocol of Ref. [18] is performed. This effect played a role on the key rates estimated in Ref. [8] for near-term implementations based on nitrogen-vacancy platforms and quantum repeaters.

III. QKD AND ENTANGLEMENT DISTILLATION PROTOCOLS

In this section, we show that the DEJMPS entanglement distillation protocol [9] is related to advantage distillation,

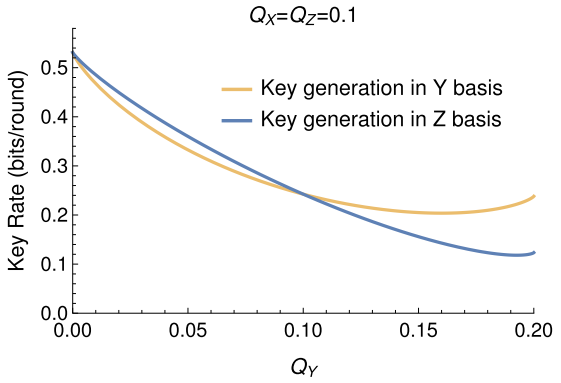

FIG. 6. Key rates for the six-state protocol with the advantage distillation protocol introduced in Ref. [18] for the family of states $Q_X = Q_Z = 0.1$. Blue (dark gray) curve illustrates the key rates when the Z basis is used for the key generation rounds, and the yellow (light gray) curve when the Y basis is used for the key generation rounds.

Protocol I, when it is applied to a string of bits generated by measurements in the basis with the higher QBER.

A maximally entangled state provides a perfectly secure bit of key. Therefore, quantum key distribution and entanglement distillation are closely related [2,11]. In fact, if the states shared by Alice and Bob have distillable entanglement, Alice and Bob could first distill maximally entangled states out of their noisy shared states and then proceed to extract a perfectly secure key by measuring the distilled states. Interestingly, some entanglement distillation protocols can be completely mapped into a classical postprocessing of the string of bits obtained after measurements on the initial states [16]. In that case, the entanglement distillation protocol has a corresponding QKD protocol that can be implemented in a prepare-and-measure setup. In a prepare-and-measure protocol, measurements of the quantum states are performed as soon as the states are received by Alice and Bob. This is of great interest for practical implementations as no quantum memory is required to implement these protocols. In Ref. [16], Gottesman and Lo characterized the properties that an entanglement distillation protocol needs to satisfy in order to be turned into a prepare-and-measure QKD protocol. The main idea is that some quantum operations (as CNOT gates) can be translated into classical operations (as XOR of the bits) on the string of bits generated by measurements in the initial state.

One-way information reconciliation based on hashing functions followed by privacy amplification is closely related to one-way entanglement distillation protocols based on Calderbank-Shor-Steane codes that can correct for the corresponding amount of bit flip and phase flip errors [11,12]. Similarly, the advantage distillation protocol, given by Protocol I, can be related to a two-to-one entanglement distillation protocol that takes two copies of a two-qubit state and maps it into one two-qubit state, hopefully more entangled than the original ones. Under the assumption that the eavesdropper is restricted to individual attacks, it has been shown [28,29] that a positive key can be extracted from any entangled state if advantage distillation with blocks of arbitrarily

Protocol II: DEJMPS entanglement distillation.

Consider that Alice and Bob share n copies of a Bell-diagonal state.

1: Alice and Bob apply local unitary operations to each copy of their states in order to bring them to the form

$$\rho = \lambda_{00}\Phi_{00} + \lambda_{10}\Phi_{10} + \lambda_{11}\Phi_{11} + \lambda_{01}\Phi_{01},$$
$$\text{such that } \lambda_{00} > \frac{1}{2} \quad \text{and} \quad \lambda_{00} > \lambda_{10} \geqslant \lambda_{11} \geqslant \lambda_{01}. \quad (12)$$

2: **for** every 2 systems **do**
3: Apply bilocal CNOT gates between the two copies.
4: Measure the target qubits, and communicate the results.
5: If the measured flags are 00 or 11, keep the first system. Else discard both pairs.
6: **end for**

large size is applied. This shows that prepare-and-measure implementation is as powerful as entanglement distillation if the eavesdropper is restricted to individual attacks. This result was also generalized to high-dimensional QKD [30,31]. However, this equivalence does not hold true under general attacks [27].

In the following, we will focus on a two-to-one entanglement distillation protocol. We will prove an interesting relation between the two-to-one entanglement distillation protocol introduced in Ref. [9], the DEJMPS protocol described in Protocol II, and advantage distillation with blocks of size two, given by Protocol I.

Protocol II includes a rotation of the initial states, step 1, before the application of the CNOT gates. Any entangled two-qubit Bell-diagonal state can be brought to the form (12) by local unitaries (e.g., applying a Hadamard to each qubit leads to a permutation of the Bell states Φ_{01} and Φ_{10}). The originally proposed DEJMPS protocol [9] includes specific rotations that are independent of the input state. In Ref. [32], it was proven that bringing the state to the form (12), before applying the CNOT gates, maximizes the fidelity of the output state. Here, we include, in the DEJMPS protocol, as a first step, the rotations that optimize the output fidelity. Moreover, note that the DEJMPS protocol can also be applied to non-Bell-diagonal states as any two-qubit entangled state that has singlet fidelity higher than $\frac{1}{2}$ can be brought to the form (12) by local operations and classical communication [26, Appendix A].

The following theorem states that the DEJMPS protocol is actually related to the six-state protocol with advantage distillation, given by Protocol I when the basis with the higher QBER is chosen for the key generation.

Theorem 1. The following two procedures result in the same key rates:

(i) Alice and Bob implement the six-state protocol with advantage distillation, given by Protocol I, using the basis with the higher QBER for key generation.

(ii) Alice and Bob apply the DEJMPS protocol to every two copies of their states and, subsequently, implement the six-state protocol without advantage distillation by measuring the distilled states.

Proof. In order to prove the equivalence of procedures (i) and (ii), we show that generating a string of bits by performing measurements in the basis with the higher QBER followed by advantage distillation is equivalent to performing the DEJMPS entanglement distillation protocol and measuring the resulting state in the Z basis.

We first note that steps 2–6 of Protocol II, followed by the measurement of the remaining qubits, can be, equivalently, implemented in a prepare-and-measure scenario. This is due to the following observations: (a) The CNOT gate commutes with measurements in the Z basis; (b) the final measurements performed on the remaining control qubits also commute with the postselection operation applied in step 5. This is due to the fact that, in step 5, a pair of qubits is discarded according to the outputs of the target qubits only, therefore, this operation acts as the identity on the control qubits of the remaining systems. Observations (a) and (b) imply that in an implementation of steps 2–6 of Protocol II followed by measurement of the remaining qubits, one can first measure all the subsystems and then proceed to apply the CNOT gate, step 3, and postselection of results, step 5. In this equivalent description in which all the systems are measured first, the CNOT gate and the postselection act on classical strings. Their action, then, corresponds to Alice and Bob locally computing the XOR of their respective two bits and comparing if they have the same parity. And this is exactly the action of the advantage distillation described in Protocol I (note that, in Protocol I, $acc = 1$ iff $a_{j_1} \oplus a_{j_2} = b_{j_1} \oplus b_{j_2}$).

Protocol II includes a local rotation of the quantum states in step 1. Instead of rotating the state, we could equivalently rotate the operations. From the previous paragraphs, we have seen that procedure (ii) of the theorem can be implemented by performing measurements in the Z basis on all the subsystems before applying the CNOT gates and postselection of the results. The first step of measurements is described as

$$\left(\sum_i |i\rangle\langle i|_A \otimes \sum_i |i\rangle\langle i|_B\right)\rho_{AB}\left(\sum_i |i\rangle\langle i|_A \otimes \sum_i |i\rangle\langle i|_B\right). \quad (13)$$

If the initial states are rotated before the measurements $\rho_{AB} \mapsto U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger$, then, we have

$$\left(\sum_i |i\rangle\langle i|_A \otimes \sum_i |i\rangle\langle i|_B\right)(U_A \otimes U_B \rho_{AB} U_A^\dagger \otimes U_B^\dagger)\left(\sum_i |i\rangle\langle i|_A \otimes \sum_i |i\rangle\langle i|_B\right)$$
$$= \left(\sum_i |i\rangle\langle i|U_A \otimes \sum_i |i\rangle\langle i|U_B\right)\rho_{AB}\left(\sum_i U_A^\dagger|i\rangle\langle i| \otimes \sum_i U_B^\dagger|i\rangle\langle i|\right). \quad (14)$$

Since the rotations are local, they can be mapped into the measurements, and the last expression of (14) describes measurements in the rotated bases $\{U_A^\dagger|i\rangle\}$ and $\{U_B^\dagger|i\rangle\}$ on the original state ρ_{AB}. By the equivalence established in the

previous paragraph, Protocol II, followed by measurement of the remaining qubits, corresponds to applying the advantage distillation, Protocol I, to a string of outcomes obtained from measurements performed in the corresponding rotated basis.

Finally, let us evaluate the effect of the rotation performed in step 1 of Protocol II. The QBERs of a Bell-diagonal state are given by

$$\begin{aligned} Q_X &= \lambda_{01} + \lambda_{11}, \\ Q_Y &= \lambda_{01} + \lambda_{10}, \\ Q_Z &= \lambda_{10} + \lambda_{11}. \end{aligned} \tag{15}$$

Given the relations satisfied by the coefficients after the rotation in step 1, Eq. (12), we have that $Q_Z \geqslant Q_X$ and $Q_Z \geqslant Q_Y$. Therefore, after the initial rotation, Z is the basis with the highest QBER. In the alternative picture in which all the measurements are performed first, and the rotation of the state is mapped into a rotation of the measurements, see Eq. (14), we have that the rotated bases $\{U_A^\dagger|i\rangle\}$ and $\{U_B^\dagger|i\rangle\}$ correspond to measurements in the basis with the highest QBER.

So the DEJMPS protocol followed by a measurement in the Z basis corresponds to advantage distillation, given by Protocol I, applied to the outcomes of measurements in the basis with highest QBER. This proves the equivalence of procedures (i) and (ii) of Theorem 1. ■

Theorem 1 establishes that the DEJMPS protocol falls into the category of entanglement distillation protocols that have a corresponding prepare-and-measure QKD as characterized by Gottesman and Lo [16]. Moreover, it shows that the particular rotation introduced in step 1 of Protocol II can be implemented in the prepare-and-measure scenario by choosing the basis with the higher QBER for key generation.

In Ref. [32], it was shown that the DEJMPS protocol, Protocol II, is the two-to-one entanglement distillation protocol that achieves the highest fidelity among all possible protocols that involve Pauli rotations. In Ref. [33], it was proven that the DEJMPS is the optimal two-to-one entanglement distillation protocol for rank 3 Bell-diagonal states. I.e., the highest possible fidelity is achieved with the highest possible probability of success, considering all possible protocols that take two copies into one. We now state analogous results for the key rates of the corresponding QKD protocol.

A Bell-diagonal state of rank up to 3 satisfies that one of the QBERs is equal to the sum of the other two. Without loss of generality, we can consider $Q_Y = Q_X + Q_Z$. The corresponding Bell-diagonal state is then,

$$\rho = (1 - Q_X - Q_Z)\Phi_{00} + Q_Z\Phi_{10} + Q_X\Phi_{11}. \tag{16}$$

We numerically compared the key rates achieved by the state given in Eq. (16) for the six-state protocol with advantage distillation given by Protocol I and key generation in all of the three bases. In the region of positive key rate, we observed that, over all the ranges of values of Q_X and Q_Z, the higher rate is achieved when Y is the key generation basis.

For rank-4 states, using the basis with the highest QBER is not always advantageous. As mentioned in Sec. II, a counterexample is given by the state with QBERs ($Q_X = 0.39$, $Q_Y = 0.39$, $Q_Z = 0.01$). For a Bell-diagonal state with the specified QBERs, a positive key rate can only be obtained by performing measurements in the Z basis in an implementation of the six-state protocol with advantage distillation given by Protocol I. We remark, however, that this does not contradict the fact that the corresponding state, after an application of the DEJMPS procedure, has higher fidelity. Indeed, as we have seen from Observation 1, higher fidelity does not necessarily imply higher key rates in the six-state protocol. Analyzing this example in detail, we find that the fidelity of the initial state is 0.605 and no key can be extracted by directly applying information reconciliation and privacy amplification. If entanglement distillation is performed without the previous rotations, i.e., by applying only steps 4–6 of Protocol II, the final fidelity is 0.525 and a positive key can be extracted from the corresponding final state using a six-state protocol with an optimal one-way hashing information reconciliation. Applying the DEJMPS protocol in which the initial rotations are performed, we obtain a state with higher fidelity, equal to 0.698, yet this state does not lead to positive key rate in the six-state protocol.

IV. IMPLICATIONS TO EXPERIMENTAL IMPLEMENTATIONS

We now discuss the implications of our results to fiber-based implementations of quantum key distribution over long distances.

The most common way of transmitting qubits over long distances is by using photons sent through optical fibers. One of the challenges of a fiber-based implementation is that the transmissivity of the channel decays exponentially with the distance. It has been shown that this also leads to an exponential decay of the achievable secret-key rate over such a channel [34,35], thus, making practical QKD over direct fiber connections impossible for longer distances. Significant amounts of both theoretical and experimental efforts are being invested into overcoming this problem using the so-called quantum repeaters [36], which have the capability of beating the exponential scaling of secret-key rate with distance. One of the fundamental building blocks of such quantum repeater schemes is a memory node that can store quantum information over time. By dividing the channel into elementary links, entanglement generation can be attempted independently over those segments, thanks to the quantum memories at the intermediate repeater stations. Unfortunately, quantum states stored in such memories decohere with time.

Decoherence is often a complex process that could be modeled by a composition of different noise channels depending on the physical implementation of the quantum memory. However, often, the dominant type of noise corresponds to the dephasing channel. This has been observed for many physical platforms which are promising candidates for long-lived quantum memories, such as nitrogen-vacancy centers [37–39], trapped ions [40], and neutral atoms [41]. Therefore, the dephasing channel is frequently used to model memory decoherence in quantum repeater literature, thus, leading to expected nonuniform QBERs over the three bases [8,42–45]. Hence, the results of this paper will be highly relevant for choosing the key generation basis for entanglement-based QKD schemes implemented across a future quantum repeater network. In fact, some of the authors of this paper have

already applied the results of this paper into their model of near-term proof-of-principle quantum repeaters based on nitrogen-vacancy centers [8].

Regarding prepare-and-measure QKD schemes, the method of decoy states was introduced to overcome vulnerabilities due to imperfections in the source [46,47]. In a decoy state protocol, the asymptotic key rates (3) and (4) are modified to account for the information leakage from the rounds in which multiple photons are generated. The modified key rates have a much more intricate dependence on the QBERs and, therefore, a detailed analysis is required to determine the effects of asymmetric noise in decoy state implementations. We leave it as an interesting open question for future investigation.

ACKNOWLEDGMENTS

We thank K. Goodenough, J. Kaniewski, S. de Bone, and T. Coopmans for helpful discussions. This work was supported by the European Research Council through a Starting Grant, and the Netherlands Organisation for Scientific Research (NWO) through a VIDI grant, and a Zwaartekracht grant. G.M. was also funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy-Cluster of Excellence Matter and Light for Quantum Computing (ML4Q) Grant No. EXC 2004/1-390534769. D.E. was also supported by the Netherlands Organization for Scientific Research (NWO/OCW), as part of the Quantum Software Consortium program (Project No. 024.003.037/3368).

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, Piscataway, NJ, 1984), pp. 175–179.

[2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).

[3] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, Trans. Am. Inst. Electr. Eng. **XLV**, 295 (1926).

[4] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. **28**, 656 (1949).

[5] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[6] S. Wiesner, Conjugate coding, SIGACT News **15**, 78 (1983).

[7] D. Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett. **81**, 3018 (1998).

[8] F. Rozpędek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission, Phys. Rev. A **99**, 052330 (2019).

[9] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum Privacy Amplification and the Security of Quantum Cryptography Over Noisy Channels, Phys. Rev. Lett. **77**, 2818 (1996).

[10] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum Cryptography without Bell's Theorem, Phys. Rev. Lett. **68**, 557 (1992).

[11] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[12] H.-K. Lo, Proof of unconditional security of six-state quantum key distribution scheme, Quantum Inf. Comput. **1**, 81 (2001).

[13] R. Renner, Security of quantum key distribution, Int. J. Quantum Inf. **6**, 1 (2008).

[14] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptology **18**, 133 (2005).

[15] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[16] D. Gottesman and H.-K. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Trans. Inf. Theory **49**, 457 (2003).

[17] B. Kraus, C. Branciard, and R. Renner, Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, Phys. Rev. A **75**, 012316 (2007).

[18] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, Key rate of quantum key distribution with hashed two-way classical communication, Phys. Rev. A **76**, 032312 (2007).

[19] G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, in *Advances in Cryptology—EUROCRYPT '93*, edited by T. Helleseth (Springer, Berlin, Heidelberg, 1994), pp. 410–423.

[20] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, Demystifying the information reconciliation protocol cascade, Quantum Inf. Comput. **15**, 453 (2015).

[21] R. Renner and S. Wolf, Simple and tight bounds for information reconciliation and privacy amplification, in *Advances in Cryptology-ASIACRYPT 2005*, edited by B. Roy (Springer, Berlin, Heidelberg, 2005), pp. 199–216.

[22] B. Kraus, N. Gisin, and R. Renner, Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication, Phys. Rev. Lett. **95**, 080501 (2005).

[23] M. van Dijk and A. Koppelaar, High rate reconciliation, *Proceedings of IEEE International Symposium on Information Theory, Ulm, Germany, 1997* (IEEE, Piscataway, NJ, 1997), p. 92.

[24] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, Efficient reconciliation protocol for discrete-variable quantum key distribution, *2009 IEEE International Symposium on Information Theory, Seoul, South Korea* (IEEE, Piscataway, NJ, 2009), pp. 1879–1883.

[25] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, Fundamental finite key limits for one-way information reconciliation in quantum key distribution, Quant. Inf. Proc. **16**, 280 (2017).

[26] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).

[27] J. Bae and A. Acín, Key distillation from quantum channels using two-way communication protocols, Phys. Rev. A **75**, 012334 (2007).

[28] N. Gisin and S. Wolf, Quantum Cryptography on Noisy Channels: Quantum Versus Classical Key-Agreement Protocols, Phys. Rev. Lett. **83**, 4200 (1999).

[29] A. Acín, L. Masanes, and N. Gisin, Equivalence Between Two-Qubit Entanglement and Secure Key Distribution, Phys. Rev. Lett. **91**, 167901 (2003).

[30] A. Acin, N. Gisin, and V. Scarani, Security bounds in quantum cryptography using d-level systems, Quantum Inf. Comput. **3**, 563 (2003).

[31] D. Bruß, M. Christandl, A. Ekert, Berthold-Georg Englert, D. Kaszlikowski, and C. Macchiavello, Tomographic Quantum Cryptography: Equivalence of Quantum and Classical Key Distillation, Phys. Rev. Lett. **91**, 097901 (2003).

[32] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Local permutations of products of Bell states and entanglement distillation, Phys. Rev. A **67**, 022310 (2003).

[33] F. Rozpędek, T. Schiet, Le Phuc Thinh, D. Elkouss, Andrew C. Doherty, and S. Wehner, Optimizing practical entanglement distillation, Phys. Rev. A **97**, 062333 (2018).

[34] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[35] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[36] H-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. **81**, 5932 (1998).

[37] A. Reiserer, N. Kalb, M. S. Blok, K. J. M. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, Robust Quantum-Network Memory Using Decoherence-Protected Subspaces of Nuclear Spins, Phys. Rev. X **6**, 021040 (2016).

[38] N. Kalb, P. C. Humphreys, J. J. Slim, and R. Hanson, Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks, Phys. Rev. A **97**, 062330 (2018).

[39] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham *et al.*, Room-temperature quantum bit memory exceeding one second, Science **336**, 1283 (2012).

[40] D. Kielpinski, Entanglement and decoherence in a trapped-ion quantum register, Ph.D. thesis, University of Colorado at Boulder, 2001.

[41] D. Schrader, I. Dotsenko, M. Khudaverdyan, Y. Miroshnychenko, A. Rauschenbeutel, and D. Meschede, Neutral Atom Quantum Register, Phys. Rev. Lett. **93**, 150501 (2004).

[42] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, Overcoming lossy channel bounds using a single quantum repeater node, Appl. Phys. B: Lasers Opt. **122**, 1 (2016).

[43] F. Rozpędek, K. D. Goodenough, J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, Parameter regimes for a single sequential quantum repeater, Quantum Sci. Technol. **3**, 034002 (2018).

[44] M. Razavi, M. Piani, and N. Lütkenhaus, Quantum repeaters with imperfect memories: Cost and scalability, Phys. Rev. A **80**, 032301 (2009).

[45] K. Nemoto, M. Trupke, S. J. Devitt, B. Scharfenberger, K. Buczak, J. Schmiedmayer, and W. J. Munro, Photonic quantum networks formed from NV-centers, Sci. Rep. **6**, 26284 (2016).

[46] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[47] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).