Security of quantum key distribution protocols using two-way classical communication or weak coherent pulses

Barbara Kraus¹, Cyril Branciard², and Renato Renner³

¹ Institute for Theoretical Physics, University of Innsbruck, Austria
² Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland
³ Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 OWA, United Kingdom

(Dated: April 1, 2022)

We apply the techniques introduced in [Kraus et. al., Phys. Rev. Lett., 95, 080501, 2005] to prove security of quantum key distribution (QKD) schemes using two-way classical post-processing as well as QKD schemes based on weak coherent pulses instead of single-photon pulses. As a result, we obtain improved bounds on the secret-key rate of these schemes.

PACS numbers: 03.67.Dd,03.67.-a

I. INTRODUCTION

A fundamental problem in cryptography is to enable two distant parties, traditionally called Alice and Bob, to communicate in absolute privacy, even in presence of an eavesdropper, Eve. It is a well known fact that a secret key, i.e., a randomly chosen bit string held by both Alice and Bob, but unknown to Eve, is sufficient to perform this task (one-time pad encryption). Thus, the problem of secret communication reduces to the problem of distributing a secret key.

Classical key distribution protocols are typically based on unproven computational assumptions, e.g., the task of decomposing a large number into its prime factors is intractable. In contrast to that, the security of quantum key distribution (QKD) protocols merely relies on the laws of physics, or, more specifically, quantum mechanics. This ultimate security is certainly one of the main reasons why so much theoretical and experimental effort is undertaken towards the implementation of secure QKD protocols [1, 2].

Typically [3, 2], in the first step of a QKD protocol, Alice chooses a random bit string and encodes each bit into the state of a quantum system, which she then sends to Bob (using a quantum channel). Bob applies a certain measurement on the received quantum system to decode the bit value. In a second step, called sifting, Alice and Bob publicly exchange some information about the encoding and decoding of each of the bits which allows them to discard bit pairs which are not (or only weakly) correlated.

After this sifting process, Alice and Bob hold a pair of classical correlated bitstrings, in the following called raw key pair. Alice and Bob can determine the quality of the raw key pair by comparing the values of some randomly chosen bit pairs (using an authenticated classical communication channel). This so-called parameter estimation gives an estimate for the quantum bit error rate (QBER), i.e., the ratio of positions for which the values of the bits held by Alice and Bob do not coincide. A fundamental principle of QKD is that this error rate also imposes a bound on the amount of information an adversary can have on the raw key: The smaller the QBER, the more secret key bits can be extracted from the raw key. If the QBER is above a certain threshold, then no secret key can be generated at all, and Alice and Bob have to abort the protocol [3].

The purpose of the remaining part of the protocol, called classical post-processing, is to transform the raw key pair into a pair of identical and secret keys. In this article, we consider classical post-processing which consists of the following three subprotocols: (i) local randomization (also called pre-processing), where Alice randomly flips each of her bits with some given probability q, (ii) error correction, where Alice and Bob equalize their strings, and (iii) privacy amplification, where Alice and Bob apply some compression function to their bitstring with the aim to reduce Eve’s information on the outcome. Steps (i)–(iii) described above only require (classical) one-way communication from Alice to Bob. However, in practical implementations, the error correction is sometimes done with two-way protocols (e.g., the cascade protocol [4]).

In [4, 5], an information-theoretic technique to analyze QKD protocols of the type described above has been presented. In contrast to most previously known methods (e.g., [6]), the technique does not require a transformation of the key distillation protocol into an entanglement purification scheme, which makes it very general. It has been applied to prove the security of various schemes such as the BB84, the six-state, the B92, and the SARG protocol [7] (see [6] for an analysis of the first three protocols and [8] for an analysis of the latter). In particular, it has been shown that the local randomization, i.e., step (i) described above, increases the bounds on the maximum tolerated QBER by roughly 10–15%.

In this paper, we extend the technique of [4, 5] (Section III) and apply it to two classes of QKD protocols which have not been covered in [4, 5]. The first (Section III) is the class of so-called two-way protocols. These use an additional subprotocol, called advantage distillation, which is invoked between the parameter estimation and the classical post-processing step described above. In contrast to the classical post-processing considered in
II. INFORMATION-THEORETIC ANALYSIS OF QKD SCHEMES

In this section we first review the results presented in [4, 5] and then show how they can be generalized. Throughout this paper we use subscripts to indicate the subsystems on which a state is defined. Alice and Bob’s quantum systems are labelled by A and B, respectively. Similarly, the classical values obtained by measuring their quantum systems are denoted by X and Y, respectively. Typically, we write \( \rho_{AB} \) or \( \rho_n \), to denote the state of all the qubits held by Alice and Bob, whereas \( \sigma_{AB} \) is a two-qubit state. We will often consider two-qubit Bell-diagonal states, i.e., states that are diagonal in the Bell basis, \( |\Phi_j\rangle = (|00\rangle + e^{|i\pi/4}|11\rangle)/\sqrt{2} \). \( P_{\Phi} \) denotes the projector onto the state \( |\Phi\rangle \). Furthermore, we denote by \( h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x) \) the binary entropy function.

A. Review of the technique

The information-theoretic technique proposed in [4, 5] directly applies to a general class of quantum key distribution protocols using one-way classical communication. However, it is required that the protocol can be represented as a so-called entanglement-based scheme, as described below.

Generally, a QKD protocol uses a set of so-called encoding bases. We consider the special case where each basis \( j \) is defined by two states \( |\phi^0_j\rangle \) and \( |\phi^1_j\rangle \), which are used to encode the bit values 0 and 1, respectively. In a prepare-and-measure scheme, Alice repeatedly chooses at random a bit \( i \) and a basis \( j \), prepares the state \( |\phi^i_j\rangle \), and sends the state to Bob. Bob then measures the state in a randomly chosen basis \( k \). This measuring process can be seen as some filtering operator \( B_k = |0\rangle\langle 0| + |1\rangle\langle 1| \), where \( |\phi^i_{j,k}\rangle \) is some state orthogonal to \( |\phi^i_j\rangle \), followed by a measurement in the computational basis.

In an entanglement-based view, the above can equivalently be described as follows: Alice prepares the two-qubit states \( A_j|\Phi_00\rangle \), where \( |\Phi_00\rangle \) denotes the Bell state \( 1/\sqrt{2}(|00\rangle + |11\rangle) \) and \( A_j \) is an encoding operator (for details see [4]) such that \( \langle i|A_j|\Phi_00\rangle = |\phi^i_j\rangle \). She then sends the second qubit to Bob and prepares Bob’s system at a distance by measuring her system in the computational basis. Bob’s measurement is described in the same way as in the prepare-and-measure scheme.

Note that, in an experimental realization of a QKD protocol, one might prefer to implement a prepare-and-measure scheme. However, when analyzing the security of a protocol, it is usually more convenient to consider its entanglement-based version.

As an illustration, consider the BB84 protocol, which uses the \( z \)-basis and the \( x \)-basis are used for the encoding. Using the above notation, we have \( |\phi^0_i\rangle = |i_z\rangle \) and \( |\phi^1_i\rangle = |i_x\rangle \), for \( i = 0, 1 \). Hence, the operators applied by Alice are \( A_0 = 1 \) and \( A_1 = H \), where \( H \) denotes the Hadamard transformation. Because the bases are orthonormal, the same operators describe Bob’s measurement as well.

For the following, we assume that Alice and Bob apply a randomly chosen permutation to rearrange the order of their qubit pairs, in the following denoted by \( P_S \), and, additionally, apply to each of the qubit pairs at random either the identity or the operation \( \sigma_x \) or \( \sigma_z \). (Note that the symmetrization operations commute with the measurement and can therefore be applied to the classical bit strings). Then, as shown in [4], the state \( \rho_{AB} \) describing the \( N \) qubit pairs shared by Alice and Bob can generally (after the most general attack by Eve, a so-called coherent attack) be considered to be of a simple form, namely

\[
\rho_{AB} = \sum_{n_1,\ldots,n_4} \lambda_{n_1,n_2,n_3,n_4} P_S(P^{\otimes n_1}_{00} \otimes P^{\otimes n_2}_{01} \otimes P^{\otimes n_3}_{10} \otimes P^{\otimes n_4}_{11}) .
\]

(1)

The sum runs over all nonnegative \( n_1,\ldots,n_4 \) such that \( n_1 + n_2 + n_3 + n_4 = N \). The set of possible values of the coefficients \( \lambda_{n_1,n_2,n_3,n_4} \) depends on the specific protocol and the parameters estimated by Alice and Bob (e.g., the QBER of the raw key). Furthermore, one can assume without loss of generality that Eve has a purification of this state, i.e., the situation is fully described by a pure state \( |\Psi\rangle_{ABE} \) such that \( \rho_{AB} = \text{tr}_E(P|\Psi\rangle_{ABE}) \). (However, as we shall see, dropping this assumption might lead to better estimates of the key rate.) After this distribution of quantum information Alice and Bob measure their systems. Thus they are left with classical bit-strings.

Consider now any situation where Alice and Bob have a classical pair of raw keys \( X^n \) and \( Y^n \) consisting of \( n \) bits whereas Eve controls a quantum system \( E \). The secret-key rate, i.e., the rate at which secret key bits can be generated per bit of the raw key, for any one-way protocol (with communication from Alice to Bob), is given by

\[
r = \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \sup_{U \leftarrow X} S(U^n|E^n) - S_\alpha(E^n) - H_\alpha(U^n|Y^n) .
\]

(2)

Here, \( S_\alpha, H_\alpha \) denote the smooth Rényi entropies (also called min-entropy if \( \alpha = \infty \) and max-entropy if \( \alpha = 0 \)) [21]. Moreover, the supremum runs over all classical values \( U^n \) that can be computed from (the classical value) \( X^n \).

For a QKD protocol as described above (where the distributed state is of the form of Eq. (1)), formula (2) can be lower bounded by an expression which only involves two-qubit systems. More precisely [7],

\[
r \geq \inf_{U \leftarrow X} \sup_{\sigma_{AB} \in \Gamma_Q} S(U|E) - H(U|Y) ,
\]

(3)
where $\Gamma_Q$ is the set of all two-qubit states $\sigma_{AB}$ (after the filtering operation) which can result from a collective attack $\mathcal{E}$ and which are compatible with the parameters estimated by Alice and Bob (in particular, the QBER). Here, $S$ and $H$ denote the von Neumann entropy and its classical counterpart, the Shannon entropy, respectively. Moreover, $X$ and $Y$ denote the classical outcomes of measurements of $\sigma_{AB}$ (on $A$ and $B$, respectively) in the computational basis, and $E$ is any system that purifies $\sigma_{AB}$. Similarly to the above formula, the supremum runs over all mappings from $X$ to $U$.

B. Local randomization

The local randomization step described above has first been considered in [6, 7] and later been improved in [16]. In [17], the local randomization is nicely explained in the context of entanglement purification.

To get an intuition why the local randomization can help to increase the secret-key rate, it is useful to describe the process as a quantum operation (as in [17]). Let $\sigma_{AB}$ be the state of a qubit pair held by Alice and Bob and let $|\Psi\rangle_{ABE}$ be a purification of $\sigma_{AB}$. The state after Alice randomly flips her bit value $A$ with probability $q$, can be described by $|\Psi\rangle_{AA'BE} = \sqrt{1-q}|\Psi\rangle_{ABE}|0\rangle_{A'} + \sqrt{q}\sigma_{A'}|\Psi\rangle_{ABE}|1\rangle_{A'}$, where $A'$ is an auxiliary system on Alice’s side. The measurement of system $A$ gives the raw key. Note that $|\Psi\rangle_{AA'BE}$ results from the application of a controlled-not operation on system $AA'$, where system $A'$ is prepared in the state $\sqrt{1-q}|0\rangle_{A'} + \sqrt{q}|1\rangle_{A'}$. The randomization of Alice thus entangles her system to some auxiliary system (which is not under Eve’s control). This, in turn, reduces the entanglement between Alice’s relevant system ($A$) and Eve’s systems (monogamy of entanglement), as Eve does not have a purification of the state on the systems $A$ and $B$, since now she only has the purification of the state $\rho_{AA'B}$. Note that Bob’s information on $A$ is also reduced by the randomization process, but—for certain values of the parameter $q$—he is less penalized than Eve. From this point of view, it can be easily understood that the local randomization can help to increase the secret-key rate.

C. Comparison to known bounds

For protocols based on qubit pairs, where the raw key pair is obtained by orthogonal measurements of Alice and Bob on some Bell-diagonal state $\sigma_{AB} = \sum_{i,j} \lambda_{ij} |\Phi_{ij}\rangle\langle\Phi_{ij}|$ (e.g., the BB84 or the six-state protocol), it follows from [8] that the secret-key rate $r$ (even without the local randomization) is bounded by

$$r \geq 1 - S(\sigma_{AB}) \geq 1 - h(e_b) - h(e_p).$$

Here, $e_b = \lambda_{10} + \lambda_{11}$ is the QBER and $e_p = \lambda_{01} + \lambda_{11}$ the phase error rate, i.e., the probability that Alice and Bob get different bits when measuring in the $z$ and the $x$-basis, respectively. Because the QBER and the phase error rate are not changed by applying at random $\sigma_x$ or $\sigma_z$, which make any state Bell diagonal, the bound $1 - h(e_b) - h(e_p)$ holds for arbitrary states $\sigma_{AB}$. Note that the above bound implies any of the lower bounds on the one-way secret-key rate derived in previous works [3, 11].

D. Generalization of the lower bound

Because we assume above that Eve controls a system that purifies the state $\rho_{AB}$ held by Alice and Bob, the bound [3] is fully determined by $\rho_{AB}$. However, this assumption on Eve might overestimate her possibilities, in which case the bound is not optimal. In the following we drop this assumption to derive better lower bounds on the secret-key rate.

Suppose that the state distributed in an entanglement-based scheme is of the form $\mathcal{P}_S((\mathcal{D}_{AB} \otimes 1)^{\otimes n}(\rho^{ABE}_{FE}))$, where $\mathcal{P}_S$ again denotes the map that randomly permutes the order of the qubit pairs, $\mathcal{D}_{AB}$ is some completely positive map on two-qubit states, and $\rho^{ABE}_{FE}$ is some tripartite state. Then, it is an immediate consequence of Lemma A.4 in [7] that the bound [3] on the secret-key rate can be generalized to

$$r \geq \sup_{U \in X} \inf_{\sigma_{ABE} \in \Gamma_Q} S(U|E) - H(U|Y).$$

Here, the infimum ranges over the set $\Gamma_Q$ of all states $\sigma_{ABE}$ which can result from a collective attack and are compatible with the parameters estimated by Alice and Bob (e.g., the QBER).

We refer to Appendix C for an application of this result to improve the analysis of the one-way SARG protocol for single-photon pulses.

Consider now the general situation where the state describing Alice, Bob, and Eve’s system is the reduced density operator of a state $|\Psi\rangle_{ABE} = \sum_n \alpha_n |\Psi_n\rangle_{ABE}|n\rangle_R$, where $\{ |n\rangle \}$ forms an orthonormal basis of the Hilbert space of an auxiliary system $R$, i.e., none of the three parties has the auxiliary system at their disposal. Starting from [3] and using the concavity of the entropy, we find that the secret-key rate is bounded by

$$r \geq \sup_{U \in X} \inf_{\sigma_{ABE} \in \Gamma_Q} \left( \sum_{n=0}^{\infty} |\alpha_n|^2 S(U|E,n) \right) - H(U|Y),$$

where $S(U|E,n) = S(U|E) - S(E|n)$, is the entropy of $U$ conditioned on $E$ and the event that the measurement of the auxiliary system $R$ in the basis $\{|n\rangle\}$ yields $n$.

One might also improve the bound using the following observation which has also been used to derive the bound given in Eq. [3]. Let us consider the situation where some auxiliary system is at Alice’ and/or Bob’s disposal, but not at Eve’s (this could be for instance some additional qubits). Suppose that the state shared by $ABE$ and some auxiliary system $R$ (which is not under Eve’s
control) is given by $|\Psi\rangle_{ABER} = \sum_n \alpha_n |\Psi_n\rangle_{ABE}|n\rangle_R$, where $\{|n\rangle\}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$. The state $|\Psi\rangle_{ABER}$ is an orthonormal basis of $\mathcal{H}_R$, the Hilbert space corresponding to system $R$.

III. QKD PROTOCOLS WITH TWO-WAY POST-PROCESSING

In the following, we will consider QKD protocols where, before the post-processing of the raw key as described above, Alice and Bob additionally invoke a so-called advantage-distillation subprotocol, which requires two-way communication between Alice and Bob. The notion of advantage distillation has first been investigated in the context of classical key agreement \[12,18\] and later been generalized to QKD \[19,20\].

The advantage distillation protocol we consider here has the following form: Alice publicly announces to Bob the position of a block of $m$ bits which have all the same value (of course, she does not tell him which value). Then Bob tells Alice whether for the given position, his corresponding bits are all identical as well. If this is the case, they both continue using the first bit of the block as a new raw-key bit, otherwise they discard the whole block.

We emphasize here that our analysis below works for any fixed value of the block size $m$ (not only asymptotically for large $m$). This is important for realistic protocols, where $m$ is usually small (e.g., $m = 3$).

To simplify the study of such protocols, we first show that it suffices to analyze the action of the advantage distillation process on two-qubit Bell-diagonal states. More precisely, Lemma 1 below implies that the state $\rho_n$ obtained by applying a block-wise operation $\mathcal{E}$ (for blocks of size $m$) to a symmetric state $\rho_n$ (see Eq. (1)) has virtually the same statistics as if $\mathcal{E}$ was applied to a state $\sigma^{\otimes m}$.

**Lemma 1.** Let $\rho_n$ be a state on $n$ particle pairs of the form $\rho_n = \mathcal{P}_S(P_{\theta_{n1}} \otimes P_{\theta_{n2}} \otimes P_{\theta_{n3}} \otimes P_{\theta_{n4}})$ and let $\sigma$ be a two-qubit Bell-diagonal state with eigenvalues $\lambda_{11}, \ldots, \lambda_{1m}$. Moreover, let $\mathcal{E}$ be an operation which maps Bell states of blocks of $m$ particle pairs to Bell states of one single particle pair. Finally, let $\rho_n = \sum_{\bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4} \mu_{\bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4} P_{\mathcal{S}}(P_{\theta_{n1}} \otimes P_{\theta_{n2}} \otimes P_{\theta_{n3}} \otimes P_{\theta_{n4}})$ be the state describing $\tilde{n} = \frac{\mu_{\bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4}}{m}$ particle pairs defined by $\tilde{n} := \mathcal{E}(\rho_n)$ and let $\lambda_1, \ldots, \lambda_4$ be the eigenvalues of $\sigma := \mathcal{E}(\sigma^{\otimes m})$. Then, for any $\varepsilon \geq 0$,

$$\sum_{\bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4} \mu_{\bar{n}_1, \bar{n}_2, \bar{n}_3, \bar{n}_4} \geq 1 - 2^{-\Theta(\bar{n} \varepsilon^2) + O(\log n)},$$

where $B^\delta(\lambda_1, \ldots, \lambda_4)$ denotes the set of all tuples $\bar{n}_1, \bar{n}_4$ such that $(\bar{n}_1, \bar{n}_4)$ is $\varepsilon$-close to $(\lambda_1, \lambda_4)$ and $\Theta(\bar{n} \varepsilon^2)$ is asymptotically the same as $\bar{n} \varepsilon^2$, up to a constant factor.

The lemma is a direct consequence of the exponential quantum de Finetti Theorem \[21\]. It states that, for any $n$-partite quantum state $\rho_n$ which is invariant under permutations of the subsystems, any part $\rho_m = tr_{m-1}(\rho_n)$ consisting of $m$ subsystems is exponentially (in $n-m$) close to a convex combination of states that virtually are of the form $\sigma^{\otimes m}$. For completeness, we give a direct proof of Lemma 1 (without referring to de Finetti’s theorem) in Appendix A.

In order to analyze protocols with advantage distillation using Lemma 1 we use the following quantum mechanical description of the advantage distillation subprotocol: Alice and Bob both apply the operation $X_{ij}^m = |0\rangle \langle 0|^m + |1\rangle \langle 1|^m$ on $m$ qubits. It is straightforward to check that

$$X_{ij}^m \otimes \mathcal{F}_i |\Phi_{i,j}\rangle = \frac{1}{\sqrt{2}} (\delta_{i,k} |\Phi_{i,j+i}\rangle),$$

where the sum $j + l$ of indices is understood to be modulo 2. Hence, applying advantage distillation to $m$ identical Bell-diagonal qubit-pairs with eigenvalues $\lambda$ leads to a Bell-diagonal state with eigenvalues $\lambda'$ given by

$$\lambda'_{ij} = \frac{1}{T} [(\lambda_{i1} + \lambda_{i2})^m + (-1)^j (\lambda_{i0} - \lambda_{i1})^m]$$

where $T = 2[(1 - Q)^m + Q^m]$ and where $Q = \lambda_{10} + \lambda_{11}$ is the QBER before the advantage distillation. The QBER $Q'$ after the advantage distillation is thus given by $Q' = \lambda'_{10} + \lambda'_{11} = \frac{Q^m}{1 - Q^m + Q^m}$ and $(1 - Q)^m + Q^m$ is the probability that the advantage distillation is successful (i.e., Alice and Bob end up with a new raw key bit). If Alice and Bob apply, after the advantage distillation the one-way classical post-processing described above, the lower bound on the secret-key rate is given by
Eq. 3, where the eigenvalues of $\sigma$ are given by the $\lambda_i$'s in \(7\) \[37\]. For instance for the six-state protocol one obtains a positive key rate for any $\text{QBER} < 0.276$ (for $n \rightarrow \infty$). Note that for the six-state protocol it has been shown that the tolerable QBER cannot be larger than 0.276, if the first step in the post-processing is advantage distillation \[22\]. As mentioned before, the bound still tolerates a QBER of up to 0.

In \[20\], Chau considered the secret-key rate obtained when applying the above described advantage distillation followed by the XOR transformation, where Alice and Bob locally compute new raw key bits by taking the XOR of a block of given bits. (For the sake of completeness we demonstrate in Appendix \[12\] how the XOR protocol can be included in our analysis.) Both procedures were analyzed in the asymptotic limit for infinitely large block sizes. The result found there is that the six-state protocol tolerates a QBER of up to 0.276. Surprisingly, the same threshold for the QBER can be obtained, as shown above, by a simpler protocol where the XOR transformation is replaced by a local randomization on single bits on Alice's side. Moreover, the rate of this modified protocol is much larger than that of Chau's protocol, as local randomization consumes less bits than the XOR transformation. Note that, as shown recently by Bae and Acin \[23\], if one omits the local randomization completely, the protocol still tolerates a QBER of up to 0.276, but the secret-key rate for large values of the QBER might be smaller.

IV. PROTOCOLS USING WEAK COHERENT PULSES

A. Preliminaries

We now consider protocols where Alice does not send single photons to Bob, but uses weak coherent pulses instead. This scenario is practically motivated by the fact that, with current technologies, it is difficult to create single-photons pulses. In fact, many of today's implementations of QKD rely on weak coherent pulses.

We start with a description of a prepare-and-measure scheme and then translate it to an equivalent entanglement-based scheme, for which we will prove security.

In the prepare-and-measure scheme, Alice encodes the bit values into phase randomized coherent states \[32\]. More precisely, she randomly chooses a basis $j$ and encodes the bit value $k$ into the state $\rho_j^k = \sum_{n \geq 0} p_n |\phi_j^k\rangle \langle \phi_j^k| ^\otimes n$, where $|\phi_j^k\rangle \langle \phi_j^k| ^\otimes 0$, denotes the vacuum for any value of $j$ and $k$ and $p_n = e^{-\mu} \mu^n / n!$, with $\mu$ the mean photon number (for a Poissonian source \[32\]).

The description of Bob's measurement depends on the experimental setup. We focus on the situation where Bob's detectors do not distinguish between the cases where they receive one or more than one photons, since with current technology, it is difficult to count the number of photons. The POVM describing the photon detector is thus given by the operators \( \{D_0, D_1\} \), with

\[
D_0 = \sum_{n \geq 0} \sqrt{p_{n.d.}(n)} P_{|n\rangle} \quad \text{and} \quad D_1 = \sum_{n \geq 0} \sqrt{1 - p_{n.d.}(n)} P_{|n\rangle},
\]

where $p_{n.d.}(n)$ is the probability of not detecting any photon in case $n$ photons arrived at the detector. This probability is given by $p_{n.d.}(n) = (1 - p_d)^n (1 - \eta)^n$, where $p_d$ is the probability of a dark count, and $\eta$ is the detection efficiency, i.e. overall transmission factor. The POVM element $D_0$ corresponds to the case where no photon is detected, whereas $D_1$ corresponds to the detection of one or more photons. In the prepare-and-measure scheme Bob would randomly choose a basis $j$ and measure the arriving photons in that basis.

In the following, we consider the so-called untrusted-device scenario, where it is assumed that Eve exchanges Bob's detectors with perfect ones (having perfect efficiency and no dark counts) and introduces all errors herself \[10\]. Clearly, security under this assumption implies security in a situation where Eve might not be able to corrupt Bob's detectors. Additionally, we assume that Bob's detector is constructed in such a way that, whenever a pulse consisting of more than one photon arrives, then the detector output corresponds to the measurement of one of the photons in the pulse chosen at random \[41\].

In the described scenario, we can without loss of generality assume that Eve only sends single photons to Bob. This follows directly from the fact that the situation obtained by sending a multi-photon pulse is the same as if Eve randomly selected one photon from the pulse and sent this single photon to Bob. Bob's measurement can therefore simply be described by the operators $B_j = |0\rangle \langle 1_j | + |1\rangle \langle 0_j |$ as defined previously.

Alice and Bob can estimate the following parameters related to their raw key: (i) the total sifting rate $R_s := \sum_{n} R_n$, for $R_n := p_n Y_n$, where $Y_n$ is the probability for Bob to find a conclusive result in case Alice sent $n$ photons; (ii) the average QBER $Q_n := \sum_{n} \frac{p_n}{n} Q_{n}$, where $Q_{n}$ denotes the QBER for the pairs where Alice sent an $n$-photon pulse. These two parameters will determine the amount of key that can be extracted from the particular raw key.

We use similar techniques as in \[8\] \[9\] to describe the same protocol in the entanglement-based scheme. The states prepared by Alice are

\[
|\Psi_j\rangle_{ABR_1} = \sum_{n \geq 0} \sqrt{p_{n.d.}(n)} |\Psi^{n}_{j}\rangle_{AB} |n\rangle_{R_1},
\]

where $|\Psi^{n}_{j}\rangle_{AB} = 1/\sqrt{2} (|0\rangle_A |\phi_j^{0}\rangle_B ^\otimes n + |1\rangle_A |\phi_j^{1}\rangle_B ^\otimes n)$. Here, we have introduced an auxiliary system $R_1$ containing the photon number (which is neither controlled by Alice nor Bob). If Alice measures her qubit in the computational basis and receives outcome $k$, the state Bob is left with in the noiseless case (without interaction of Eve) is $\rho_B = 2 \text{tr}_{R_1} (P_k |\Psi_{j}\rangle_{ABR_1} \langle \Psi_{j}|) = \sum_{n \geq 0} p_{n.d.} P_{|n\rangle}$, which corresponds to the coherent state (with randomized phase) sent by Alice in the prepare-and-measure scheme \[12\].
The operation on Bob’s side is given by the operators $B_j$, as described above.

The state describing the situation after Bob’s operation is given by

$$|\chi\rangle_{ABER_1R_2} = \sum_j B_j U_{EB}(|\Psi_j\rangle_{ABER_1}|j\rangle_{R_2}),$$

where $j$ corresponds to the basis chosen by Alice and $U_{EB}$ is a unitary describing the attack of Eve. Note that this state is not necessarily normalized, but its weight $\text{tr}(|\chi\rangle\langle\chi|)$ corresponds to the sifting rate.

Restricted to Alice and Bob’s systems, $|\chi\rangle_{ABER_1R_2}$ is a two-qubit state. We can thus apply the techniques presented in Section III to analyze the security of the protocol. More precisely, we need to evaluate the r.h.s. of (9) to get a lower bound on the secret-key rate. First we do not take the local randomization into account, i.e., we choose $U = X$. The case including local randomization will be treated in the next subsection. We thus obtain, for the key rate

$$r \geq \inf_{\sigma \in \Gamma_{R_\mu,Q_\mu}} \sum_{n=0}^{\infty} R_n S(U|E,n) - R_\mu S(U|Y).$$

The set $\Gamma_{R_\mu,Q_\mu}$ contains all states which can result from a collective attack by Eve and are compatible with the average sifting rate $R_\mu$ and the QBER $Q_\mu$, as estimated by Alice and Bob.

Because the (conditional) entropy of a classical variable cannot be negative, the r.h.s. of (9) can be lower bounded by restricting to any of the terms in the sum over $n$. Note that, in (9), the average over $n$ is only taken over the term for the entropy conditioned on Eve’s system, but not on the term for the entropy conditioned on Bob’s system. This is because Eve might be able to measure the photon number, whereas this is not the case for Bob.

B. Protocols with local randomization

So far we did not consider the possibility for Alice to apply some local randomization on her classical bits. The randomization can easily be included in the analysis: if the randomization is acting on single bits, $U \leftarrow X$ (bit flip with probability $q$). Simply writes

$$r \geq \inf_{\sigma \in \Gamma_{R_\mu,Q_\mu}} \sum_{n=0}^{\infty} R_n S(U|E,n) - R_\mu S(U|Y).$$

Bob’s uncertainty is now given by $S(U|Y) = h(Q_\mu^q)$, where $Q_\mu^q = (1-q)Q_\mu + q(1-Q_\mu)$. Since $R_\mu = \sum_n R_n$, (10) can also be written as

$$r \geq \inf_{\sigma \in \Gamma_{R_\mu,Q_\mu}} \sum_{n=0}^{\infty} R_n \left[ S(U|E,n) - h(q) \right] - R_\mu \left[ h(Q_\mu^q) - h(q) \right].$$

Note that, for any $n \geq 0$, the term $S(U|E,n)$ on the r.h.s. of this inequality can be bounded by $S(U|E,n) \geq S(U|X) = h(q)$ (since $U$ is only computed from $X$), and therefore the r.h.s. of (11) can again be lower bounded by restricting the sum to any of its terms.

As we will see, the local randomization allows us to get better lower bounds for the secret-key rate as well as better lower bounds for the maximum distance for which the rate is positive.

C. Examples: the BB84 and the SARG protocols

Using the results above, in particular (9), we now compute the lower bound on the secret-key rate of the BB84 as well as the SARG protocols. In Section IV E we compare the results we derive here with previous results, in particular with the ones presented in [24] and [25].

In contrast to the single-photon case, where the lower bound on the secret-key rate was a function of the QBER, we are aiming here for a lower bound that depends on the only two measurable quantities $R_\mu$ (the total sifting rate) and $Q_\mu$ (the total QBER). For simplicity, we will in the following not explicitly include the local randomization, except in the final results (see Figures 1 and 2).

Our computation of the bound given by (9) is subdivided into two steps: First, for any $n \geq 0$ and for any $Q_\mu$, we compute $S\mu(Q_n) := \inf_{\sigma_n \in \Gamma_{Q_n}} S(X|E,n)$, where $\Gamma_{Q_n}$ is the set of all states $\sigma_n$ which can result from a collective attack on a $n$-photon pulse causing a QBER of $Q_n$. In a second step, we compute the infimum

$$\inf_{\{R_n,Q_n\} \in \Gamma_{R_\mu,Q_\mu}} \sum_{n=0}^{\infty} R_n S_n(Q_n)$$

where $\Gamma_{R_\mu,Q_\mu}$ denotes the set of all parameters $\{R_n,Q_n\}$ which are compatible with $R_\mu$ and $Q_\mu$. All the technical details can be found in Appendix D.

1. BB84

For the BB84 protocol, it is easy to verify that for any pulse consisting of $n \geq 2$ photons, Eve has full information on Alice’s measurement outcome $X$, i.e., $\inf_{\sigma_n \in \Gamma_{Q_n}} S(X|E,n) = 0 \forall n \geq 2$. The lower bound is thus given by (13)

$$r \geq \inf_{\{R_1,Q_1\} \in \Gamma_{R_\mu,Q_\mu}} R_1 S_{BB84}^1(Q_1) - R_\mu h(Q_\mu)$$

where $S_{BB84}^1(Q_1) := 1 - h(Q_1)$ (see Appendix D or [6, 7]).

As shown in Appendix D, the conditions in the untrusted-device scenario for $R_1$ and $Q_1$ to be compatible
with $R_\mu$ and $Q_\mu$ are the following:

$$
R_1 \leq \frac{1}{2} p_1
$$

$$
R_1 \geq R_\mu - \frac{1}{2} \sum_{n \geq 2} p_n
$$

$$
R_1 Q_1 \leq R_\mu Q_\mu.
$$

(14)

Let $R_1^{\text{min}} = R_\mu - \frac{1}{2} \sum_{n \geq 2} p_n$. If $R_1^{\text{min}} \leq 0$, then $R_1$ can be set equal to zero, and the lower bound on $r$ is negative, i.e., Alice and Bob have to abort the protocol. If $R_1^{\text{min}} > 0$, let $Q_1^{\text{max}} = \min(R_\mu Q_\mu/R_1^{\text{min}}, 1/2)$. Due to the decreasing of $S_1^{\text{BB84}}(Q_1)$ for $Q_1 \leq 1/2$, we then get

$$
r \geq R_1^{\text{min}} (1 - h(Q_1^{\text{max}})) - R_\mu h(Q_\mu).
$$

(15)

Note that this bound has first been derived in [27] using a different technique. This bound can be interpreted as follows: For an optimal attack, Eve should make $R_1$ as small as possible (i.e., block as many single-photon pulses as possible) and, at the same time, make $Q_1$ as large as possible (i.e., introduce as many errors as possible on the single-photon pulses that she forwards, which reduces her uncertainty on Alice’s system as much as possible).

To get an idea of how good this bound is, we evaluate the rate for the situation where there is no Eve present, instead, the errors are introduced due to a realistic channel. The channel we consider is a lossy depolarizing channel with visibility $V$ (or fidelity $F = 1 - V$) and disturbance $D = 1 - \frac{1}{2} V$), and a transmission factor $t = 10^{-3} \cdot \alpha$ at distance $\ell$ ($\alpha$ is the attenuation coefficient). Furthermore, we consider the situation where Bob’s detectors have an efficiency $\eta_{\text{det}}$ and a probability of dark counts $p_d$. An explicit calculation (see Appendix D) shows that under these assumptions, the rates that Alice and Bob would get are

$$
R_\mu = \frac{1}{4} \left[ 1 - \bar{p}_d e^{-\mu \eta} \right],
$$

$$
R_\mu Q_\mu = \frac{1}{4} \left[ \bar{p}_d e^{-\mu D - \mu \eta} - \bar{p}_d^2 e^{-\mu \eta} \right],
$$

where $\eta = t \eta_{\text{det}}$, $\bar{p}_d = 1 - p_d$. When we insert these values in (15) for experimentally reasonable values of $\alpha$, $p_d$ and $\eta_{\text{det}}$, and optimize for different distances over the mean photon number $\mu$ (which Alice is free to choose), we get the results illustrated in Fig. 1 (for $V = 1$) and Fig. 2 (for $V = 0.95$). We find that the optimal $\mu$ is proportional to the transmission factor $t$, and our bound on the secret-key rate is proportional to $t^2$ (at least for short distances, i.e., in the regime where dark counts are not dominant); this was already observed in [26, 27].

2. SARG

A major difference between the SARG protocol and the BB84 protocols is that Eve cannot get full information on Alice’s value even if the pulse contains two photons.

FIG. 1: Lower bound on the secret-key rate per pulse and optimal $\mu$ for Poissonian sources as a function of the distance, for the BB84 and SARG protocols, when Alice and Bob share a quantum channel with perfect visibility $V \geq 1$. The other experimental parameters are $\alpha = 0.25 \text{ dB/km}$, $\eta_{\text{det}} = 0.1$ and $p_d = 10^{-5}$. The thick lines are the results we obtain when Alice performs an optimal bit-wise local randomization; the thin lines are the same, without randomization ($q = 0$).

FIG. 2: Same plot as in Fig. 1 (top), but for a quantum channel with non-perfect visibility, $V = 0.95$. 

In order to take this into account, we include the contribution of the two-photon components in our formula for the secret-key rate, i.e. we compute (11):

\[ r \geq \inf_{\{R_1, Q_1, R_2, Q_2\}} R_1 S_{\text{SARG}}(Q_1) + R_2 S_{\text{SARG}}(Q_2) - R_\mu h(Q_\mu). \]

In Appendix D we describe how to compute \( S_{\text{SARG}}(Q_1) \) and \( S_{\text{SARG}}(Q_2) \) (see also Appendix C and (22)), and we derive the following conditions for \( R_1, Q_1, R_2 \) and \( Q_2 \) to be compatible with \( R_\mu \) and \( Q_\mu \):

\[
\begin{align*}
R_1(1 - Q_1) &\leq \frac{1}{2} p_1 \\
R_2(1 - Q_2) &\leq \frac{1}{2} p_2 \\
R_1(1 - Q_1) + R_2(1 - Q_2) &\geq R_\mu(1 - Q_\mu) \tag{17} \\
R_1Q_1 + R_2Q_2 &\leq R_\mu Q_\mu.
\end{align*}
\]

If \( R_\mu(1 - Q_\mu) - \frac{1}{2} \sum_{n \geq 3} p_n > 0 \), one can see in (10) that Eve’s optimal choice is to set \( R_1 \) and \( R_2 \) as small as possible, and \( Q_1 \) and \( Q_2 \) as large as possible (\( S_{\text{SARG}}(Q_1) \) and \( S_{\text{SARG}}(Q_2) \) are decreasing): she should therefore set the equality in the third constraint.

However, contrary to BB84, we have not been able to give a simpler analytical expression for the infimum in (10); we therefore resort to numerical computations.

Again, in order to estimate the previous bound in a practical implementation of the protocol, we compute the typical values of the parameters \( R_\mu \) and \( Q_\mu \) when Alice and Bob use a Poisson source and a lossy depolarizing channel (see Appendix D):

\[
R_\mu = \frac{1}{2} \left[ 1 - \bar{p}_d^2 e^{-\mu} + \bar{p}_d e^{-\mu} \sigma_F n - \bar{p}_d e^{-\mu} \sigma_D n \right].
\]

\[
Q_\mu = \frac{1}{2} \left[ 1 - \bar{p}_d^2 e^{-\mu} + \bar{p}_d e^{-\mu} \sigma_F n - \bar{p}_d e^{-\mu} \sigma_D n \right].
\]

Similarly to the BB84 protocol, inserting these values in Eq. (16), and optimizing for different distances over the mean photon number \( \mu \), provides the results illustrated in Figures 1 and 2.

For \( V = 1 \), we find an optimal \( \mu \) proportional to \( t^{1/2} \), and therefore our bound on the secret-key rate scales like \( t^{3/2} \) (see also (31)), which is more efficient than for BB84 (where we had \( r \propto t^2 \)).

For \( V = 0.95 \) however, we find that the SARG protocol is less efficient than the BB84, and our lower bound for the secret-key rate of SARG also scales like \( t^2 \), the same as for BB84. However, it should be noted that we determine here only lower bounds on the rates.

### D. Decoy states

The relevant set \( \Gamma_{R_\mu,Q_\mu} \) in (12) over which the infimum has to be taken to obtain the lower bound on the secret-key rate is quite big, since Alice and Bob can only estimate the total sifting and total error rate. They do neither have a good estimation of the error rates, \( Q_n \) nor of the corresponding yields, \( Y_n \). Hwang and Lo et. al. pointed out a method to improve the lower bound on the secret-key rate by making some additional measurements (24, 28; see also (29)). The idea of the so-called decoy states is to change the intensity of the pulses sent by Alice in order to be able to estimate more quantities. This allows them to deduce more information about the possible attack of an eavesdropper (like the estimate of the QBER does). For practical purpose one assumes that Alice is always sending weak coherent pulses, varying only the mean photon number. We will show here how this particular idea can be included in our analysis.

Let us first of all consider the case where Alice uses two different intensities, i.e., one with mean photon number \( \mu_0 \) (we call it signal pulse in the following) and the other (decoy pulse) with mean photon number \( \mu_1 \). Using more decoy states is a straightforward generalization of this case. We describe the states sent by Alice by \( |\psi\rangle_{\text{ABR}} = |\psi_\mu\rangle_{\text{ABR}} |0\rangle_r + |\psi_2\rangle_{\text{ABR}} |1\rangle_r \), where \( |\psi_\mu\rangle_{\text{ABR}}, |\psi_2\rangle_{\text{ABR}} \) denotes the (unnormalized) signal (decoy) pulse (see Eq. (5)). System \( R_2 \) is again some auxiliary system, introduced to keep track of the signal and decoy pulses. In this case this system is in Alice’s hands, as she chooses the intensity of the signals. Since Alice is going to measure the auxiliary system \( R_2 \) in the computational basis, we can consider the state \( \sigma = p_\sigma |0\rangle_r \otimes |0\rangle_{\text{ABR}} + (1-p_\sigma) |1\rangle_r \otimes |1\rangle_{\text{ABR}} \), where \( |\sigma_\langle \rangle, |\sigma_c\rangle \rangle \) are Alice and Bob’s signal (decoy) states after Eve’s intervention, respectively. Bob’s measurement is described in the same way as before. Again, Alice and Bob can only measure the total sifting rate \( R_\mu = \sum_n p_n Y_n \) and estimate the total error rate \( Q_\mu = \sum_n p_n Q_n / R_n \), with \( Y_n = \sum_n p_n Y_n \rangle / R_n \), however, now they are in the position to obtain more information about their qubit pairs, as they are capable of measuring these quantities for different values of \( \mu \) (recall \( p_n = e^{-\mu} n^\mu / n! \)), i.e., they can measure the values \( R_\mu, Q_\mu \) and \( R_{\mu_1}, Q_{\mu_1} \). We can again use (30) to compute a lower bound on the secret-key rate. In this case, the infimum is taken over the set \( \Gamma_{(R_\mu,Q_\mu)} \), of all Bell-diagonal two-qubit states of the form \( p_\sigma |\sigma\rangle\langle \sigma| + p_c |\sigma_c\rangle\langle \sigma_c| \), with \( |\sigma\rangle \rangle, |\sigma_c\rangle \rangle \) denoting the Bell-diagonal states corresponding to the signal (decoy) bits, which are compatible with all estimated total sifting rates \( R_\mu \), and total error rates \( Q_\mu \).

Let us now consider the case where Alice uses many different intensities for her decoy states. Due to the definition of \( R_\mu \) it is clear that, by varying \( \mu \), one can obtain information about the quantities \( Y_n \). Knowing \( Y_n \) and \( Q_\mu \) one can then determine \( Q_\mu \). Note that in order to determine \( Y_n \) and \( Q_\mu \) one needs infinitely many decoy intensities; however, already a small number of such decoy intensities suffices to restrict the values of \( Y_n \) and \( Q_\mu \) (see for instance (29)). The results of the analysis above are illustrated in Fig. 3 and 4. In order to evaluate the lower bounds we consider the situation where Alice and Bob share a lossy depolarizing channel with visibilities \( V = 1, V = 0.95 \) respectively.
FIG. 3: Lower bound on the secret-key rate per pulse and optimal $\mu$ for Poissonian sources as a function of the distance, for the BB84 and SARG protocols using decoy states, when Alice and Bob share a quantum channel with perfect visibility $V = 1$. The other parameters are the same as in Fig. 1. The thick lines are the results we obtain when Alice performs an optimal bit-wise local randomization; the thin lines correspond to the protocol without randomization ($q = 0$).

FIG. 4: Same plots as in Fig. 3 but for a quantum channel with non-perfect visibility, $V = 0.95$.

E. Related work

In [25], a similar comparison between the BB84 and SARG protocols has been done, and lower bounds on the secret-key rates were computed. For BB84, our results are very similar to those of [22] (see also [27]), but we could slightly increase the rates and the limiting distances with using the local randomization process [45].

For the SARG protocol, taking into account the two-photon contribution in the lower bound allows to increase the lower bound. In the case of SARG without decoy states, we could thus improve significantly the bound of [27]. Our conclusion is therefore different: we find that the SARG protocol performs better than BB84 for high visibility $V \approx 1$ (see Fig. 1). However, the SARG is more sensitive to the loss of the channel, and for $V = 0.95$ for instance, BB84 is more efficient (Fig. 2).

In the case of SARG with decoy states, the two-photon contribution had already been taken into account in [27], and we again get similar results. However, we could slightly improve the rate with the improved calculation of $S^r_{SARG}(Q_1)$ (see Appendix C), and with the local randomization process. Nevertheless, our conclusion is the same as in [25], namely that when decoy states are used, the SARG is outperformed by the BB84 protocol.

V. FURTHER APPLICATIONS, AND OPEN PROBLEMS

There are still several possibilities to improve the lower bounds on the secret-key rate of QKD protocols. One way to look at this problem is to analyze the properties of the set $\Gamma$ over which one has to optimize in order to obtain the lower bound (see e.g. Eq. 3). Concerning the single photon QKD protocols, one might try to find the conditions on the encoding (and decoding) operations which would lead to a properly restricted set $\Gamma_Q$, such that a high QBER can be tolerated.

In a protocol based on weak coherent pulses, it might be advantageous to take the detected double clicks into account. As mentioned above, this would (most likely) impose further restrictions on the set of possible attacks and thus result in an improvement of the secret-key rate. In addition, it would be interesting to generalize the ideas developed in this article to a scenario, where not only the intensity of light is used but where also the coherence of the light is checked (similar to the decoy states). One protocol taking this into account has for instance been proposed in [3]. Another possibility is to consider protocols based on weak coherent pulses that use two-way
post-processing, as studied by Lo [30]. We also note here that the techniques presented here can also be applied to protocols based on squeezed states.

In this work, we considered the so-called untrusted-device scenario, where the adversary might arbitrarily modify the efficiency of Bob’s detector. If one considers the reasonable situation, where Eve cannot influence Bob’s device, one might obtain larger values for the key rate.

VI. ACKNOWLEDGEMENTS

The authors would like to thank Nicolas Gisin, Antonio Acín, and Valerio Scarani for helpful discussions. This project is partly supported by SECOQC and by the FWF. RR acknowledges support by HP Labs, Bristol and BK by the FWF through the Elise-Richter project.

APPENDIX A: PROOF OF LEMMA

In this appendix we prove the Lemma presented in Section III. The operator \( \sigma^{(n)} \) is symmetric and can thus be written as

\[
\sigma^{(n)} = \sum_{n_1^\prime,...,n_4^\prime} \lambda_{n_1, n_2, n_3, n_4} (P_{|\Phi_{000}\rangle} \otimes P_{|\Phi_{101}\rangle} \otimes P_{|\Phi_{010}\rangle} \otimes P_{|\Phi_{111}\rangle}),
\]

for appropriate coefficients \( \lambda_{n_1, n_2, n_3, n_4} \). Hence, with the definition \( p := \lambda_{n_1, n_2, n_3, n_4} \), we have

\[
\sigma^{(n)} = p \rho_n + (1 - p) \tilde{\rho}_n,
\]

where \( \tilde{\rho}_n \) is a symmetric quantum state on \( n \) subsystems. Moreover, it is easy to see that the coefficient \( p \) cannot be smaller than \( \frac{1}{n} \).

By linearity, we get the following expression for the state after the operation \( \mathcal{E}^{(n)} \) has been applied to \( \sigma^{(n)} \):

\[
\mathcal{E}^{(n)}(\sigma^{(n)}) = p \mathcal{E}^{(n)}(\rho_n) + (1 - p) \mathcal{E}^{(n)}(\tilde{\rho}_n). \tag{A1}
\]

Because \( \mathcal{E}^{(n)} \) is symmetric, it can be written as

\[
\mathcal{E}^{(n)} = \sum_{n_1^\prime,...,n_4^\prime} \tilde{\mu}_{n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime} \mathcal{P}_{|\Phi_{000}\rangle} \otimes \mathcal{P}_{|\Phi_{101}\rangle} \otimes \mathcal{P}_{|\Phi_{010}\rangle} \otimes \mathcal{P}_{|\Phi_{111}\rangle},
\]

for some coefficients \( \tilde{\mu}_{n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime} \). Furthermore, by the law of large numbers, the sum of the coefficients \( \tilde{\mu}_{n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime} \) for tuples \( n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime \) which are not contained in \( B^\prime(\lambda_1, ..., \lambda_4) \) is exponentially small, i.e.,

\[
\sum_{(n_1^\prime,...,n_4^\prime) \notin B^\prime(\lambda_1, ..., \lambda_4)} \tilde{\mu}_{n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime} \leq e^{-\Theta(n \pi^2)}. \tag{A2}
\]

Finally, because of (A1),

\[
\tilde{\mu}_{n_1, n_2, n_3, n_4} \geq p \cdot \tilde{\mu}_{n_1^\prime, n_2^\prime, n_3^\prime, n_4^\prime},
\]

where \( \tilde{\mu}_{n_1, n_2, n_3, n_4} \) are the coefficients of \( \tilde{\rho}_n \). Since \( p \geq \frac{1}{n} \),

\[
\tilde{\mu}_{n_1, n_2, n_3, n_4} \leq n \cdot \tilde{\mu}_{n_1, n_2, n_3, n_4},
\]

Combining this with (A2), we conclude

\[
\sum_{(n_1,...,n_4) \notin \mathcal{B}^\prime(\lambda_1, ..., \lambda_4)} \tilde{\mu}_{n_1, n_2, n_3, n_4} \leq n e^{-\Theta(n \pi^2)}. \tag{A3}
\]

APPENDIX B: ADVANTAGE DISTILLATION USING THE XOR PROCESS

In this appendix we explain how the XOR process applied to many qubit pairs can be easily included within this formalism. Alice selects randomly a set of bits and informs Bob about this set. Then, Alice and Bob compute both the XOR of those bits and keep only the result, discarding all the others. Our goal is to find a simple description of the remaining logical bits, Eve’s system, and the classical information sent form Alice to Bob (note that Eve knows the randomly chosen set which is used by Alice and Bob). We demonstrate here how this can be achieved with the example of three qubit pairs. The idea can be easily generalized to any number of pairs.

Quantum mechanically the XOR operation can be described by a controlled-not operation, denoted by \( \text{U}_{\text{C}} \). Three copies of the state \( |\Psi\rangle_{ABE} = \sum_{i,j} \sqrt{\lambda_{i,j}} |\Phi_{i,j}\rangle_{ABE} |\Phi_{j,i}\rangle_{E} \) transform, under the transformation \( U_{\text{C}}^3 \otimes U_{\text{C}}^2 \otimes U_{\text{C}} \) to the state

\[
\sum_{i,j,k,l,m,n} \sqrt{\lambda_{i,j} \lambda_{k,l} \lambda_{m,n}} |\Phi_{i,j+k+m+n}\rangle_{A_1 B_1 E} |\Phi_{k,l}\rangle_{A_2 B_2 E} |\Phi_{m,n}\rangle_{A_3 B_3 E}, \tag{B1}
\]

where \( |\Phi_{i,j+k+m+n}\rangle_E = |\Phi_{i,j}\rangle |\Phi_{k,l}\rangle |\Phi_{m,n}\rangle \). Since Alice and Bob are not going to use the systems 2 and 3 anymore, we want to consider a state that describes only Alice’s and Bob’s first systems. More importantly, we want to give Eve a purification of this state. If we would assume that Eve has a purification of the state describing systems \( A_1 \) and \( B_1 \), this would be equivalent to assume that Eve has Alice’s and Bob’s second and third pair after this transformation. It is evident that we assume then that she has more power than she actually has. In order to avoid to give her too much power we use the idea mentioned in Section III (see also [10]), by considering the systems \( A_2, B_2, A_3, B_3 \) as auxiliary system \( R \). For the unitary transformations, \( U_{k,l,m,n} \) we choose \( U_{i,j+k+l+m,n} = \omega^{A_1} \) for \( l + j = n + j = 1 \) and the identity otherwise. It can be easily verified that the state describing Alice’s and Bob’s first system is then the partial trace over \( E, R \) of the state \( |\Psi\rangle_{A_1 B_1 R E} = \sum_{i,j+k+l+m,n} \sqrt{\lambda_{i,j} \lambda_{k,l} \lambda_{m,n}} |\Phi_{i+k+m+j+n}\rangle_{A_1 B_1 E} |\Phi_{j,k,l,m,n}\rangle_{R} \) where \( |\Phi_{j,k,l,m,n}\rangle_R \) denotes the state \( |\Phi_{k,l,j,m,n}\rangle_{A_2 B_2 E} |\Phi_{m,n}\rangle_{A_3 B_3 E} \). As explained in Section III providing Eve with a purification of the state that describe the systems \( A_1, B_1 \) never underestimates her power. The eigenvalues of the
two-qubit Bell-diagonal state describing Alice’s and Bob’s remaining systems, denoted by $\tilde{\lambda}_{i,j}$ are

$$
\tilde{\lambda}_{i,j} = \lambda_{i,j}^2 + 3\lambda_{i,j+1}^2 + 3\lambda_{i+1,j}^2 + 6\lambda_{i,j}\lambda_{i+1,j}\lambda_{i+1,j+1}.
$$

The intuition for this choice of unitary transformations is the following. The state $|\Psi\rangle_{ABE}$ under consideration is supposed to lead to a secret-bit. Thus, the coefficients $\lambda_{i,j}$ are such that it is very likely that if both, $t + j = 1$ and $n + j = 1$ then $j = 1$, which means that within the remaining qubit-pair there is a phase-flip error. The unitaries are chosen such that this error is corrected.

Using the new eigenvalues of the state describing Alice’ and Bob’s remaining bits, it is straightforward to compute the lower bound on the secret-key rate (Eq. (3)).

**APPENDIX C: AN IMPROVED ANALYSIS OF THE SARG PROTOCOL WITH SINGLE PHOTONS**

In the SARG protocol the bit value 0 (1) is encoded in the $z$-basis ($x$-basis) respectively. During the sifted phase Alice announces a set containing two states, the one which she sent and one in the other basis. There are 4 different encoding and decoding operators. For instance $A_1 = |0\rangle\langle 0, 0\rangle + |1\rangle\langle 1, 0\rangle$ and $B_1 = |0\rangle\langle 0, 1\rangle + |1\rangle\langle 1, 1\rangle$ describe the situation where Alice sends on of the two states $\{|0\rangle, |1\rangle\}$ and tells Bob that the sent state is within this set. Let us for the moment consider a single qubit sent by Alice (for more details see [12]).

The state shared by Alice, Bob, and Eve after the sift is given by $|\chi\rangle_{ABER} = \sum_j A_j \otimes B_j |\Psi\rangle_{ABE}|j\rangle_{R_1}$, where $|\Psi\rangle_{ABE}$ is the state shared by Alice, Bob, and Eve after Eve’s intervention. Now, we apply some symmetrization to the state, which does not change any security consideration, as explained in Section II. Let us consider the state $|\chi\rangle_{ABER} = |\chi\rangle_{ABER}|0\rangle_{R_1} + \sigma^x \otimes \sigma^y |\chi\rangle_{ABER}|1\rangle_{R_2}$. It is straightforward to show that the reduced state describing Alice’ and Bob’s system is equal to $D_2 D_1 [D_2 (\rho_0)]$, with $\rho_0 = \text{tr}_E (P_0)$. Here, $D_2 (\rho) = 1/2(\rho + \sigma_2 \otimes \sigma_2 \rho \sigma_2 \otimes \sigma_2, D_1 (\rho) = \sum_j A_j \otimes B_j A_j^\dagger \otimes B_j^\dagger$ is given by the protocol and $D_2$ denotes the depolarizing map, i.e. $D_2 (\rho) = 1/4(\rho + \sigma_2 \otimes \sigma_2 \rho \sigma_2 \otimes \sigma_2 + \sigma_y \otimes \sigma_y \rho \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z \rho \sigma_z \otimes \sigma_z)$. Furthermore, the action of $D_1$ on a Bell-diagonal state is the same as $A_1 \otimes B_1$ on that state. Thus, we only need to consider the situation where Eve has a purification of the state $D_2 (\rho_0)$, i.e. the state before the action of $D_1$ and $D_2$. Using the results of [13] this implies that the state we have to use in order to compute the lower bound on the secret-key rate is $\rho_{ABE} = D_2 ^{AB} (P_{AB \otimes B_1} |\Psi\rangle_{ABE})$, where $|\Phi\rangle_{ABE} = \sqrt{\lambda_{00}} |\Phi_{00}\rangle_{AB} |\Phi_{00}\rangle_{E} + \sqrt{\lambda_{11}} |\Phi_{11}\rangle_{AB} |\Phi_{11}\rangle_{E} + \sqrt{\lambda_{01}} |\Phi_{01}\rangle_{AB} |\Phi_{10}\rangle_{E} + \sqrt{\lambda_{10}} |\Phi_{10}\rangle_{AB} |\Phi_{01}\rangle_{E}$, i.e. a purification of the Bell-diagonal state $D_2 (\rho_0)$.

Using this description it is straightforward to compute the state describing Alice’ and Bob’s system, which is, in contrast to former considerations, no longer Bell-diagonal. In the following we consider the situation where Bob accepts only if the probability for him to obtain the bit values 0 is the same as detecting 1. This is a first step in the parameter estimation. Note that this condition imposes $\lambda_{01} = \lambda_{10}$. The QBER, $Q$, can be easily determined and one finds $Q = (\lambda_{01} + \lambda_{11})/(1/2 + \lambda_{01} + \lambda_{11})$. Using the normalization condition we find that the coefficients in the state $|\Phi\rangle_{ABE}$ are given by: $\lambda_{00} = 1 - Q/(1 - Q) + \lambda_{11}, \lambda_{01} = Q/(2(1 - Q)) - \lambda_{11}, \lambda_{10} = \lambda_{01}$. Thus, for a fixed QBER there is only one parameter, $\lambda_{11} \in [0, Q/(2(1 - Q))]$, over which one needs to minimize to obtain the lower bound on the secret-key rate given in formula Eq. (4). Without the local randomization one finds that the lower bound on the secret-key rate is positive as long as $Q \leq 0.1167$. Including the local randomization allows to increase the tolerable QBER to 0.1308 compared to the previously known bounds of 0.0968 without and 0.1095 with local randomization, respectively [12].

**APPENDIX D: CALCULATIONS RELATED TO THE ANALYSIS OF PROTOCOLS BASED ON COHERENT PULSES**

This appendix contains some calculations related to the evaluation of the lower bound (9) on the secret-key rate for the BB84 and SARG protocols with weak coherent pulses (see Section IV).

For this purpose, we first compute the infimum $S_n (Q_n) := \inf_{x_n \in \Gamma_{Q_n}} S (X | E, n)$ for any given $Q_n$, and then optimize (from Eve’s point of view) over the parameters $R_n, Q_n$. These parameters must be compatible with the measurable quantities $R_n, Q_n$: in the case of protocols which do not use decoy states, this leads to particular constraints for each protocol, which we derive here. (Note that for protocols with decoy states, Alice and Bob can estimate all rates $R_n, Q_n$: Eve can no longer optimize over these parameters.)

Recall that we work in the untrusted device scenario, where Eve has full control over Bob’s detectors. Dark counts do not occur, and therefore $R_0 = 0$, as Eve should obviously not send any photon to Bob when she receives an empty pulse from Alice. Moreover, we consider protocols where Bob treats all double clicks as if only one randomly chosen detector clicked.

In a second step, in order to give estimations of our bounds, we compute the typical values of the yields and error rates if no adversary is present, i.e., if the channel between Alice and Bob is a depolarizing channel with fidelity $F$ (or disturbance $D = 1 - F$) and with a transmission factor $t$. In addition, we suppose in that case that Bob’s detectors have an efficiency $\eta_{det}$ and a probability of dark counts $p_d$. We will use the notations $\eta = \eta_{det}$ for the overall transmission factor and $p_d = 1 - p_d$. 


1. BB84 protocol

a. Eve’s uncertainty on the one-photon pulses

For BB84, the set $\Gamma_{Q_1}$ contains all states with diagonal entries (in the Bell basis) $\lambda_{00} = 1 - 2Q_1 + \lambda_{11}$ and $\lambda_{01} = \lambda_{10} = Q_1 - \lambda_{11}$, for any $\lambda_{11} \in [0, Q_1]$.

One can easily prove that $S(X|E, n = 1)$ takes its minimum when $\lambda_{11} = Q_1^2$. Then, a straightforward calculation shows that $S_{BB84}^{BB}(Q_1) = \inf_{\sigma_1 \in \Gamma_{Q_1}} S(X|E, n = 1) = 1 - h(Q_1)$. Note that $S_{BB84}^{BB}(Q_1)$ is decreasing for $0 \leq Q_1 \leq 1/2$: as expected, the higher the error Eve introduces, the more she reduces her uncertainty.

b. Constraints on the yields and error rates

In the BB84 protocol, the probability that Alice and Bob choose the same basis for their preparation and measurement respectively is $1/2$ (this is the sifting factor). Therefore we have $Y_n \leq \frac{1}{2}$ for all $n$, which implies the following bounds:

$$R_1 = p_1 Y_1 \leq \frac{1}{2} p_1 \tag{D1}$$
$$R_1 = R_\mu - \sum_{n \geq 2} p_n Y_n \geq R_\mu - \frac{1}{2} \sum_{n \geq 2} p_n \tag{D2}$$

These are the first two constraints announced in $\text{[14]}$. The third constraint follows from the definition of $Q_\mu$, $R_\mu Q_\mu = \sum_n R_n Q_n$.

c. Yields and error rates for depolarizing channels

When implementing the BB84 protocol, Alice and Bob would estimate the quantities $Q_\mu$, $R_\mu$, and then compute the rate as explained above. In order to get an idea how good the obtained bounds on the rate are we evaluate here these quantities for the situation where there is no Eve present and Alice and Bob share a lossy depolarizing channel.

In BB84, when Alice sends $n$ photons, the probability that Bob chooses the same basis as Alice and gets a single or a double click is:

$$Y_n = \frac{1}{2} \left[1 - \bar{\rho}_d^2 (1 - \eta)^n\right]$$

Bob gets a wrong bit if only the wrong detector clicks, or if the two detectors click, but he randomly chooses a wrong bit. This happens with probability:

$$Y_n Q_n = \frac{1}{2} \sum_{k=0}^{n} C_n^k \rho_d^k D^{n-k} \left[\bar{\rho}_d (1 - \eta)^k \left[1 - \bar{\rho}_d (1 - \eta)^n - k\right] + \frac{1}{2} \left[1 - \bar{\rho}_d (1 - \eta)^k \left[1 - \bar{\rho}_d (1 - \eta)^n - k\right]\right] \right]$$
$$= \frac{1}{4} \left[1 + \bar{\rho}_d (1 - F \eta)^n - \bar{\rho}_d (1 - D \eta)^n - \bar{\rho}_d^2 (1 - \eta)^n\right]$$

When Alice uses a Poissonian source (i.e. $p_n = \frac{n^n}{n!} e^{-\mu}$), the overall yield and error rate are then

$$R_\mu = \frac{1}{2} \left[1 - \bar{\rho}_d^2 (1 - \eta)^n\right]$$
$$R_\mu Q_\mu = \frac{1}{4} \left[1 + \bar{\rho}_d e^{-\mu F \eta} - \bar{\rho}_d e^{-\mu D \eta} - \bar{\rho}_d^2 e^{-\eta}\right].$$

2. SARG protocol

a. Eve’s uncertainty on the one-photon pulses

In order to compute Eve’s uncertainty on the one-photon pulses, we use the method presented in Appendix C. We don’t have an analytical expression for $S_{SARG}^{SARG}(Q_1) = \inf_{\sigma_1 \in \Gamma_{Q_1}} S(X|E, n = 1)$, but we compute it numerically. Note that we find $S_{SARG}^{SARG}(Q_1)$ is decreasing only for $0 \leq Q_1 \leq 0.338$, and does not reach zero.

b. Eve’s uncertainty on the two-photon pulses

We follow the calculations of $\text{[25]}$ to compute Eve’s uncertainty on the two-photon pulses. The set $\Gamma_{Q_2}$ contains all states with the following diagonal entries (in the Bell basis)

$$\begin{align*}
\lambda_{00} &= 1 - Q_2 - \lambda_{11} \\
\lambda_{10} &= Q_2 - \lambda_{11} \\
\lambda_{01} + \lambda_{11} &= x Q_2 + g(x), \forall x
\end{align*}$$

where $g(x) = \frac{1}{2} (3 - 2x + \sqrt{6 - 6\sqrt{2} x + 4x^2})$. When minimizing $x Q_2 + g(x)$ over $x$, we get

$$\begin{align*}
\lambda_{00} &= 1 - Q_2 - \lambda_{11} \\
\lambda_{10} &= Q_2 - \lambda_{11} \\
\lambda_{01} + \lambda_{11} &\leq B(Q_2)
\end{align*}$$

where $B(Q_2) = \frac{1}{2} + \frac{1}{\sqrt{3}} (2Q_2 - 1)$. We then have $B(Q_2) < \frac{1}{2}$ and the optimal choice of the parameters $\lambda_{ij}$ for Eve is $\lambda_{00} = 1 - Q_2 - \lambda_{11}$, $\lambda_{10} = Q_2 - \lambda_{11}$, $\lambda_{01} + \lambda_{11} = B(Q_2)$ (i.e. Eve should make the phase error as high as possible, up to $\frac{1}{2}$, and $\lambda_{11} = Q_2 B(Q_2)$).

Then, a straightforward calculation gives $S_{SARG}^{SARG}(Q_2) = \inf_{\sigma_2 \in \Gamma_{Q_2}} S(X|E, n = 2) = 1 - h(B(Q_2))$. Note that $S_{SARG}^{SARG}(Q_2)$ is decreasing for $0 \leq Q_2 \leq \frac{1}{3}$, and $S_{SARG}^{SARG}(\frac{1}{3}) = 0$.

c. Constraints on the yields and error rates

In the case of SARG, because of the non orthogonality of the quantum states that are used to encode the classical bit values, it is a little bit more tricky to find the constraints that the yields and error rates must satisfy. Here, we will derive a constraint on the yields without
errors (or probability that Bob gets a right conclusive result), i.e., on $p_{\text{right}} = Y_n(1 - Q_n)$ (for any $n \in \mathbb{N}$).

To this aim, let’s suppose in a first step that Alice sends photons in the state $|+\rangle$, that Eve attacks the pulse and decides either to forward one photon to Bob in the state $\rho_B$, or to block the pulse. In this case, Bob gets a right conclusive result if (i) Alice announces the set $\{|+\rangle, |+\rangle\}$ (which she does with probability $1/2$), Bob chooses to measure $\sigma_z$ (probability $1/2$) and (only) the detector corresponding to $|+\rangle$ clicks; or (ii) Alice announces the set $\{|+\rangle, |-\rangle\}$, Bob chooses to measure $\sigma_x$, and the detector corresponding to $|+\rangle$ clicks. Therefore, Bob’s probability to get a right conclusive result when Alice sends $|+\rangle$ is bounded by:

$$p_{\text{right} | +} \leq \frac{1}{4} \langle -x | \rho_B | -x \rangle + \frac{1}{4} \langle +x | \rho_B | +x \rangle$$  \hspace{1cm} (D5)

This result actually does not depend on the state sent by Alice, and we therefore have

$$p_{\text{right}} = Y_n(1 - Q_n) \leq \frac{1}{4}.$$  \hspace{1cm} (D7)

The first three constraints announced in [14] then follow:

$$R_1(1 - Q_1) \leq \frac{1}{4} p_1$$  \hspace{1cm} (D8)

$$R_2(1 - Q_2) \leq \frac{1}{2} p_2$$  \hspace{1cm} (D9)

$$R_1(1 - Q_1) + R_2(1 - Q_2) \geq R_n(1 - Q_n) - \frac{1}{4} \sum_{n \geq 3} p_n$$  \hspace{1cm} (D10)

As before, the last constraint follows from the definition of $Q_n$.

$$d. \quad \text{Yields and error rates for depolarizing channels}$$

As for the BB84–protocol, we evaluate here the lower bound on the secret key rate for the situation where there is no Eve present and Alice and Bob share a lossy depolarizing channel, in order to get an idea of how good the obtained bounds on the rate are.

In order to calculate the yields and error rates for the SARG protocol, let’s suppose that Alice sends $n$ photons in the state $|+\rangle$, and announces $\{|+\rangle, |+\rangle\}$. By symmetry, the following still holds for any state sent by Alice, and any announcement. Similar calculations can be found in [14].

If Bob measures $\sigma_z$, he gets a (wrong) conclusive click on the detector corresponding to $|-\rangle$, or a double click with probabilities:

$$p_{|z|z} = \sum_{k=0}^{n} C_n^k F^k D^{n-k} |\bar{p}_d(1 - \eta)^k| |1 - \bar{p}_d(1 - \eta)^{n-k}|$$

$$p_{\text{2 clicks} | z} = 1 - 2\bar{p}_d(1 - \frac{\eta}{2})^n + \bar{p}_d^2(1 - \eta)^n$$

Similarly, if Bob now measures $\sigma_x$, he gets a (right) conclusive click on the detector corresponding to $|-\rangle$, or a double click with probabilities:

$$p_{|z|z} = \sum_{k=0}^{n} C_n^k F^k D^{n-k} |\bar{p}_d(1 - \eta)^k| |1 - \bar{p}_d(1 - \eta)^{n-k}|$$

$$p_{\text{2 clicks} | z} = 1 - 2\bar{p}_d(1 - \frac{\eta}{2})^n + \bar{p}_d^2(1 - \eta)^n$$

Since Bob randomly chooses the basis he measures, with equal probabilities, and since he randomly chooses one outcome in the case of double clicks (conclusive or not), the probability that Bob’s result is conclusive when Alice sends $n$ photons is $Y_n = \frac{1}{2}(p_{|z|z} + \frac{1}{4}p_{\text{2 clicks} | z}) + \frac{1}{2}(p_{|z|z} + \frac{1}{4}p_{\text{2 clicks} | z})$, and the error rate on these pulses is $Q_n = \frac{1}{2}(p_{|z|z} + \frac{1}{4}p_{\text{2 clicks} | z})$. We find:

$$Y_n = \frac{1}{2} \left[ 1 + \frac{\bar{p}_d}{2}(1 - F\eta)^n - \frac{\bar{p}_d}{2}(1 - D\eta)^n - \bar{p}_d^2(1 - \eta)^n \right]$$

$$Q_n = \frac{1}{2} \left[ 1 + \frac{\bar{p}_d}{2}(1 - F\eta)^n - \frac{\bar{p}_d}{2}(1 - D\eta)^n - \bar{p}_d^2(1 - \eta)^n \right]$$

For a Poissonian source, the overall yield and error rate are then

$$R_n = \frac{1}{4} \left[ 1 + \frac{\bar{p}_d}{2}e^{-\mu F\eta} - \frac{\bar{p}_d}{2}e^{-\mu D\eta} - \bar{p}_d^2 e^{-\mu \eta} \right]$$

$$Q_n = \frac{1}{4} \left[ 1 + \frac{\bar{p}_d}{2}e^{-\mu F\eta} - \frac{\bar{p}_d}{2}e^{-\mu D\eta} - \bar{p}_d^2 e^{-\mu \eta} \right]$$

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics, 74, 145 (2002).
[2] http://www.idquantique.com  http://www.magiqtech.com
[3] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, quant-ph/0411022 (2004); D. Stucki, N. Brunner, N. Gisin, V. Scarani, H. Zbinden, Appl. Phys. Lett. 87, 194108 (2005).
[4] K. Inoue, E. Waks, Y. Yamamoto, Phys. Rev. A 68, 022317 (2003).
[5] G. Brassard and L. Salvail, Workshop on the theory and application of cryptographic techniques on Advances in Cryptology, pp. 410–423 (1994).
[6] B. Kraus, N. Gisin, and R. Renner Phys. Rev. Lett. 95, 080501 (2005).
[7] R. Renner, N. Gisin, and B. Kraus Phys. Rev. A 72, 012332 (2005).
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441,
[14] H.-K. Lo, Quant. Info. Comp., 66 (2006).
[15] R. Renner, Security of Quantum Key Distribution, PhD thesis, ETH (2005), available at: http://arxiv.org/abs/quant-ph/0512258.
[16] A. Acin, J. Bae, E. Bagan, M. Baig, Ll. Masanes, R. Munoz-Tapia, Phys. Rev. A 73, 012327 (2006).
[17] J. Bae and A. Acin, quant-ph/0610048 (2006).
[18] H.-K. Lo, X. Ma, K. Chen, Phys. Rev. A 74, 032330 (2006).
[19] M. Koashi, quant-ph/0507154 (2005).
[20] This description applies to a large class of QKD protocols. There are, however, certain proposals of QKD schemes where the encoding is different [14, 15].
[21] In addition to the QBER, further parameters estimated by Alice and Bob (e.g., the sifting rate) might be used to bound the adversary’s information.
[22] A collective attack is an attack where the adversary treats each signal sent over the channel identically and independently of the other signals.
[23] An even tighter lower bound is given by $r \geq \sup_{U \rightarrow X,Y \leftrightarrow U} \inf_{\rho_{AB} \in \mathcal{E}} S(U|V) - H(U|Y)$. This includes the possibility that Alice sends some additional information, $V$ to Bob. However, we are not aware of any protocol where this additional step helps (at least not after the sifting phase).
[24] $\lambda$ is a vector of eigenvalues $\lambda_{ij}$ corresponding to the Bell states $|\Phi_{ij}\rangle$.
[25] Note that assuming that Eve has a purification of the state describing Alice’ and Bob’s system takes into account the fact that Eve knows the classical information, about the bits which are grouped in the different blocks.
[26] We do not consider the situation where Alice also sends a strong reference pulse to Bob. In this case, the state Alice would send is of the form $|\psi\rangle = \sum_{n \geq 0} \sqrt{\epsilon^{n}} \mu^{n} / n! |n\rangle |N-n\rangle$, where $|n\rangle$ denotes the state of $n$ photons in a certain mode. Here we consider the situation where she sends only the first of these two systems to Bob.
[27] Similarly, one could consider any other distribution instead of the Poissonian distribution.
[28] We still make the so-called fair-sampling assumption, which means that the errors are independent of the measurement bases chosen by Bob.
[29] This means that, whenever Bob measures a double-click, he has to replace it by a random single click.
[30] The factor 2 after the first equality sign is due to the renormalization (each of Alice’s outcome $k$ has probability $\frac{1}{2}$).
[31] In the untrusted-device scenario, with Bob’s detector replaced by the eavesdropper, Eve should not send any photon to Bob when she receives an empty pulse from Alice, and therefore $R_0 = 0$. In the trusted-device scenario however, the dark counts could contribute to the key with a positive term $R_0$. For a similar observation, see [12].
[32] In the SARG protocol, the pulses with three or more photons could still give a small contribution to the key (Eve doesn’t have full information on these). For simplicity we limit ourselves to the 1- and 2- photon contributions.
[33] The difference for instance in the plots for BB84 in Fig. 9 of [22] and our figures [1] and [3] essentially come from a different definition of the dark count probabilities : in [22], $p_{\text{dark}}$ is the probability that one of the two detectors has a dark count, while here $p_d$ is the probability for each detector to have a dark count (therefore we have $p_{\text{dark}} \approx 2p_d$).
[34] A similar argument has also been used in [14, 22] to include this process.