PHYSICAL REVIEW A **72**, 032301 (2005)

Security of two quantum cryptography protocols using the same four qubit states

Cyril Branciard,[1,2] Nicolas Gisin,[1] Barbara Kraus,[1] and Valerio Scarani[1]
[1]*Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, 1211 Geneva 4, Switzerland*
[2]*Ecole Nationale Supérieure des Télécommunications, 46, rue Barrault, 75013 Paris, France*
(Received 10 May 2005; published 1 September 2005)

The first quantum cryptography protocol, proposed by Bennett and Brassard in 1984 (BB84), has been widely studied in recent years. This protocol uses four states (more precisely, two complementary bases) for the encoding of the classical bit. Recently, it has been noticed that by using the same four states, but a different encoding of information, one can define a protocol which is more robust in practical implementations, specifically when attenuated laser pulses are used instead of single-photon sources [V. Scarani *et al.*, Phys. Rev. Lett. **92**, 057901 (2004), referred to as the SARG04 protocol]. We present a detailed study of SARG04 in two different regimes. In the first part, we consider an implementation with a single-photon source: we derive bounds on the error rate Q for security against all possible attacks by the eavesdropper. The lower and the upper bound obtained for SARG04 ($Q \lesssim 10.95\%$ and $Q \gtrsim 14.9\%$, respectively) are close to those obtained for BB84 ($Q \lesssim 12.4\%$ and $Q \gtrsim 14.6\%$, respectively). In the second part, we consider a realistic source consisting of an attenuated laser and improve on previous analysis by allowing Alice to optimize the mean number of photons as a function of the distance. The SARG04 protocol is found to perform better than BB84, both in secret-key rate and in maximal achievable distance, for a wide class of Eve's attacks.

DOI: 10.1103/PhysRevA.72.032301 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography [1], or quantum key distribution (QKD), is the most mature field in quantum information, both in theoretical and in experimental advances. From the very beginning of quantum information, it was clear that QKD should be secure because of the no-cloning theorem, and also that it should be implementable with available technology. However, both rigorous proofs of security and truly practical implementations turned out to be serious challenges: one had to start from the situations which are easiest to handle. But what is easy for a theorist (small number of parameters, idealized components) is not what is easy for an experimentalist (practical, real components). Thence, research in QKD mostly split into two fields: proving security in theoretically idealized situations on the one hand, and realizing practical prototypes on the other. Important advances have been made in both directions; at present, while many open problems remain in both fields, an urgent task consists in bringing theory and application together again. Indeed, the theoretical tools have recently been applied to study the security of practical implementations [2]. This paper aims at the same goal, on a different protocol and with a different approach.

In any implementation of QKD, there is a large number of components which do not behave according to the simplest theoretical model. Such is the source: QKD protocols based on photon counting are most easily studied by assuming that a single-photon source or a source of entangled photons is used, but by far the most practical source is an attenuated laser [3]. This practical implementation can lead to secure QKD: the analysis of the security parameters, while more complex than in the case of single photons, is definitely important. A drawback of the practical implementation was noticed by some authors [4] and explicitly stated in 2000 by Lütkenhaus and co-workers [5]: weak laser pulses contain sometimes more than one photon; thus, if losses are expected in the quantum channel (as they always are), the eavesdropper Eve may take advantage of the multiphoton pulses by keeping some photons without introducing errors on those that she lets pass. These attacks are known as *photon-number-splitting* (PNS) attacks. Since then, several ways have been found to counter PNS attacks. An especially strong protection is obtained by introducing decoy states [6]; this requires some modification of the experimental devices. The idea behind the Scarani-Acín-Ribordy-Gisin 2004 (SARG04) protocol [7,8] is different and complementary: one can keep the hardware exactly as it is, but modify the classical communication between Alice and Bob (the so-called sifting phase). Note that one can implement both the sifting of SARG04 and a monitoring using decoy states: this is the protocol for which Tamaki and Lo have proved security for one- and two-photon pulses [9].

The goal of this paper is to improve the comparison between SARG04 and the original protocol of quantum cryptography which uses four states, the one devised by Bennett and Brassard in 1984 (BB84) [10]. The structure of the paper is as follows.

(1) *The protocol*. In Sec. II, we recall the basics of the SARG04 protocol and present its entanglement-based version.

(2) *Single-photon implementation*. This is the content of Sec. III. We compute a *lower bound* for security against all possible attacks of the eavesdropper (in particular, the most general coherent attacks) under one-way classical processing by Alice and Bob—a study usually called unconditional security. The bound we obtain is $Q \lesssim 10.95\%$ where Q is the quantum bit error rate (QBER). This bound is $Q \lesssim 12.4\%$ for the BB84 protocol [11,12]. An *upper bound* for security can also be computed by giving an explicit attack by Eve. We identify an incoherent attack which performs better than the one which uses the phase-covariant cloning machine [13].

The SARG04 protocol is found to be certainly insecure in a single-photon implementation as soon as $Q \gtrsim 14.9\%$, the corresponding upper bounds for BB84 being $Q \gtrsim 14.64\%$.

Thus, the lower and upper bounds for security under one-way classical postprocessing are similar for both protocols. However, suppose that the channel Alice-Bob is a depolarizing channel, as is the case in all experiments performed to date:

$$\mathcal{E}[|\psi\rangle] = F|\psi\rangle\langle\psi| + D|\psi^{\perp}\rangle\langle\psi^{\perp}| \tag{1}$$

where $F+D=1$. The channel is then characterized by the disturbance D, or equivalently, by the visibility V of the fringes one can observe in an interferometric setup defined by

$$F = \frac{1+V}{2}, \quad D = \frac{1-V}{2}. \tag{2}$$

Now, the link between the QBER and the visibility is different for the two protocols: $V=1-2Q$ for BB84, while $V=(1-2Q)/(1-Q)$ for SARG04. The comparison of the bound for the visibility is unfavorable for SARG04.

(3) *Attenuated laser pulses (Poissonian source), imperfect detectors*. In Sec. IV, we consider the more realistic situation for which SARG04 was devised. Alice's source is an attenuated laser, producing weak pulses, that is, pulses with a mean number of photons $\mu \lesssim 1$. A first comparison between SARG04 and BB84 in this implementation can be found in the original references [7,8]. Here we improve significantly on this analysis, although the study of ultimate security is still beyond reach. Anyway, for a broad class of incoherent attacks by Eve including various forms of PNS [14], we can compute the optimal secret key rate by optimizing over the mean number of photons μ describing the Poissonian statistics. We work in the trusted-device scenario: Eve cannot take advantage of the limited efficiency or of the dark counts of Bob's detectors. We find that the optimal mean number of photon goes as $\mu_{opt} \sim 2\sqrt{t}$ as a function of the transmission t of the quantum channel, while the much smaller value $\mu_{opt} \sim t$ holds for BB84 under identical conditions [15]. As a consequence, the secret-key rate (proportional to the detection rate μt) decreases as $t^{3/2}$ instead of the faster t^2 decrease of BB84. The limiting distance is also increased in SARG04 with respect to BB84, approximately by 10 km using typical values of the parameters of the detector and the channel. Thus, SARG04 compares favorably with BB84 in practical implementations for this class of attacks.

The conclusions of both Secs. III and IV strongly suggest that the same quantum correlations can be exploited differently according to the physical realization, by adapting the classical encoding and decoding procedures.

II. SARG04 PROTOCOL

A. SARG04: Prepare-and-measure version

The SARG04 protocol was introduced in Ref. [7] in a *prepare-and-measure* version. At the level of quantum processing, it is exactly equivalent to BB84. Alice prepares one of the four states belonging to two conjugated bases, e.g., $|+z\rangle \equiv |0\rangle$, $|-z\rangle \equiv |1\rangle$, $|+x\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$, and $|-x\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$. She sends the state to Bob, who measures either σ_z or σ_x. The difference from BB84 appears in the encoding and decoding of classical information. The classical bit is encoded in the basis: $|+z\rangle$ and $|-z\rangle$ code for 0, $|+x\rangle$ and $|-x\rangle$ code for 1. Since each basis codes for a bit, it is natural in SARG04 to admit that the two bases are chosen randomly with equal probability [16].

In the sifting phase, Alice does not reveal the basis (this would reveal the bit): she discloses the state she has sent and one of the states that code for the other value of the bit, which are *not* orthogonal to the first one. There are thus *a priori* four sifting sets: $\mathcal{S}_{++}=\{|+z\rangle, |+x\rangle\}$, $\mathcal{S}_{--}=\{|-z\rangle, |-x\rangle\}$, $\mathcal{S}_{+-}=\{|+z\rangle, |-x\rangle\}$, and $\mathcal{S}_{-+}=\{|-z\rangle, |+x\rangle\}$. For definiteness, suppose $|\text{sent}\rangle = |+z\rangle$ and $|\text{declared}\rangle = |+x\rangle$: Bob guesses correctly the bit if he measured σ_x and found $|\text{right}\rangle = |-x\rangle$; he guesses wrongly the bit if he measured σ_z and found $|\text{wrong}\rangle = |-z\rangle$. As usual, an error can happen only if the state has been modified by an eavesdropper, or in the presence of dark counts. In the absence of errors, the length of the sifted key is $\frac{1}{4}$ of the length of the raw key; in the presence of an error rate Q, this length increases.

This encoding is better to protect secrecy against incoherent PNS attacks when the source is not a single-photon source. In fact, suppose that a pulse contained two photons and Eve has kept one of them in a quantum memory. In BB84, by listening to the sifting, Eve learns the basis: she can measure the photon she has kept and learn the bit with certainty. In SARG04, in the sifting Eve learns that the state is either of two nonorthogonal states: she cannot learn the bit with certainty. In order to learn the bit with certainty without introducing errors, Eve has to implement an unambiguous state discrimination on the three-photon pulses, which succeeds with probability $\frac{1}{2}$. This suggests that SARG04 should be more robust than BB84 against incoherent PNS attacks. In Refs. [7,8] it was shown that this intuitive reasoning is correct and gives a real advantage over BB84; we shall confirm this conclusion with a significantly improved analysis in Sec. IV.

B. SARG04: Entanglement-based version

In order to determine a lower bound on the secret-key rate we will consider the equivalent entanglement-based version of the SARG04 protocol [9,17]. To this end we define the encoding operators

$$A_{\sigma\omega} = |0\rangle\langle\sigma z| + |1\rangle\langle\omega x| \tag{3}$$

where $\sigma, \omega = \pm 1$. Instead of preparing a state and sending the qubit to Bob, Alice prepares randomly one of the states

$$A_{\sigma\omega} \otimes \mathbb{1}|\Phi^{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\sigma z\rangle + |1\rangle|\omega x\rangle) \tag{4}$$

and sends the second qubit to Bob. Measuring Alice's qubit then in the computational basis $\{|0\rangle, |1\rangle\}$ prepares Bob's qubit in one of the four states used by the protocol. In order to decode the information sent by Alice, Bob applies one of the four operators

$$B_{\sigma\omega} = \frac{1}{\sqrt{2}}[\sigma|0\rangle\langle -\omega x| + \omega|1\rangle\langle -\sigma z|]. \quad (5)$$

After that, Bob measures his qubit in the computational basis.

Let us show that this description is indeed equivalent to the prepare-and-measure protocol described above. The preparation by Alice is equivalent since a measurement in the z basis performed on the first qubit described by one of the states $A_{\sigma\omega}\otimes\mathbb{1}|\Phi^+\rangle$ leads with equal probability to one of the states $|\sigma z\rangle, |\omega x\rangle$. On the other hand, Bob's measurement is

$$B^\dagger_{\sigma\omega}|0\rangle\langle 0|B_{\sigma\omega} = \frac{1}{2}|-\omega x\rangle\langle -\omega x|,$$

$$B^\dagger_{\sigma\omega}|1\rangle\langle 1|B_{\sigma\omega} = \frac{1}{2}|-\sigma z\rangle\langle -\sigma z|, \quad (6)$$

where σ, $\omega = \pm$. Thus, his measurement corresponds to measuring his qubit in either the z or x basis [18].

We dispose now of all the tools to tackle the security studies on the SARG04 protocol. As announced, we consider first the case of single-photon sources and will tackle the more realistic case of attenuated lasers in Sec. IV.

III. SINGLE-PHOTON SOURCES

A. Generalities: The scenario for security proofs

In this section we investigate the security of the SARG04 protocol, assuming that Alice is sending out single photons encoding the bit values. First of all, we compute a lower bound on the secret-key rate using the results presented in [11,12]. Then we compare those bounds to the bounds derived with proofs based on entanglement distillation [9]. After that we determine an upper bound on the secret-key rate for the SARG04 protocol. To this aim we explicitly construct an attack by Eve. This attack is incoherent, i.e., acting on each qubit individually and measuring each qubit right after the basis reconciliation.

B. Lower bound on the secret key rate

1. Review of the approach

Let us start by summarizing the results presented in [11,12], where a computable lower bound on the secret-key rate for a general class of QKD protocols using one-way classical postprocessing has been derived. We use the entanglement-based description of the protocol. Alice prepares n qubit pairs at random in one of the states defined in Eq. (4) and sends the second qubit of each pair to Bob. Eve might now apply the most general attack on all the qubits sent to Bob. Bob applies at random one of the operators defined in Eq. (5) on the qubits he received. After that Alice and Bob symmetrize their qubit pairs by applying a random permutation on them. On the other hand, Alice and Bob randomly choose for each qubit pair to apply the bit-flip operation $(\sigma_x\otimes\sigma_x)$. Both of those transformations commute with their measurement in the z basis. It has been shown in [11] that after randomly applying these transformation the form of the state describing Alice's and Bob's system is Bell diagonal, independently of the protocol. Its eigenbasis is given by $\{|\Phi^+\rangle^{\otimes n_1}|\Phi^-\rangle^{\otimes n_2}|\Psi^+\rangle^{\otimes n_3}|\Psi^-\rangle^{\otimes n_4}\}$, where $n_1+n_2+n_3+n_4=n$ and the states $|\Phi^\pm\rangle, |\Psi^\pm\rangle$ denote the Bell basis. Apart from that the state is symmetric with respect to exchanging the different qubit pairs. The only free parameters are the eigenvalues of the density operator. Those depend on the distribution of the quantum information, i.e., on the QKD protocol. It is important to note that when assuming that Eve has a purification of this state, i.e., $\rho_{ABE}=|\Psi\rangle_{ABE}\langle\Psi|$, for some state $|\Psi\rangle_{ABE}$, then her power is never underestimated. It has then been shown in [11,12] that a lower bound on the secret-key rate can then be determined considering only two-qubit density operators. In particular, for a given QBER Q, a lower bound on the secret-key rate (assuming that Alice and Bob apply optimal error correction and privacy amplification) is given by

$$r \geqslant r_1 = \sup_{A'\leftarrow A}\inf_{\sigma_{AB}\in\Gamma_Q} R(\sigma_{A'BE}) \quad (7)$$

with

$$R(\sigma_{A'BE}) = [S(\sigma_{A'E}) - S(\sigma_E)] - H(A'|B). \quad (8)$$

Here, $S(H)$ denotes the von Neumann (Shannon) entropy. It is important to take some space to describe these objects in detail.

(1) The first apparent thing is that Alice does something to her bit string A which transforms it to A'. This is called *preprocessing*. It is a classical operation, known only to her [just note that in the original formula, Eq. (2) in [11], there appears also the possibility, denoted V there, that Alice discloses something of her preprocessing publicly: neglecting this possibility here, we can nevertheless obtain a lower bound]. We consider here that Alice applies this preprocessing to each bit value independently. Thus, she can only flip her bit values with a certain probability. Note that this transformation reduces the information Bob has about Alice's bit string, but it turns out that it penalizes Eve more than Bob, which implies that this preprocessing increases the secret-key rate. Obviously, Alice will choose the preprocessing which maximizes the rate, whence the supremum in Eq. (7).

(2) The set Γ_Q can be assumed to contain only two-qubit Bell-diagonal density operators which are compatible with the measured QBER Q. In order to be more precise we have to introduce the following notation. We denote by $\rho_0 = \mathrm{tr}_E[\mathcal{E}(|\Phi^+\rangle_{AB}\langle\Phi^+|\otimes|0\rangle_E\langle 0|)]$, where $\mathcal{E}$ denotes a general map applied by Eve (we do not impose that this map is unitary, since we are going to consider in the following the state shared by Alice and Bob after sifting). Let us denote now by A_j and B_j the decoding and encoding operators defined by the considered protocol. For the SARG04 protocol, these are the operators defined in Eqs. (3) and (5), respectively. The state describing Alice's and Bob's qubit pairs after sifting can be considered to be

$$\rho_1 = \mathcal{D}_1(\rho_0) = C\sum_j A_j\otimes B_j\rho_0 A_j^\dagger\otimes B_j^\dagger \quad (9)$$

where C is a normalization constant which may depend on ρ_0 (recall that, e.g., in SARG04, the length of the sifted key

varies with the amount of errors). Recall that this state is measured by Alice and Bob in the z basis. Using this notation we can now define the set Γ_Q. It contains any state of the form

$$\rho_2 = \lambda_1 P_{\Phi^+} + \lambda_2 P_{\Phi^-} + \lambda_3 P_{\Psi^+} + \lambda_4 P_{\Psi^-} \tag{10}$$

with

$$\lambda_1 = \langle \Phi^+ | \rho_1 | \Phi^+ \rangle,$$

$$\lambda_2 = \langle \Phi^- | \rho_1 | \Phi^- \rangle,$$

$$\lambda_3 = \langle \Psi^+ | \rho_1 | \Psi^+ \rangle,$$

$$\lambda_4 = \langle \Psi^- | \rho_1 | \Psi^- \rangle. \tag{11}$$

Those coefficients have to satisfy the normalization condition and the fact that the state ρ_2 has to be compatible with the estimated error, Q. Since the state is measured in the computational basis this implies

$$\lambda_1 + \lambda_2 = 1 - Q,$$

$$\lambda_3 + \lambda_4 = Q. \tag{12}$$

The considered protocol, i.e., the map $\mathcal{D}_1$ confines the λ's further. Let us denote now by $\sigma_{AB} \in \Gamma_Q$ the state describing Alice's and Bob's qubit. Eve is supposed to hold a purification of this state, i.e., σ_{ABE} is pure. Obviously, one must suppose that Eve has made the best attack, whence the infimum in Eq. (7).

(3) The density matrix $\sigma_{A'E}$ is the state of the joint system of Alice and Eve, after Alice has performed the preprocessing.

(4) As for $R(\sigma_{A'BE})$: if one replaces the von Neumann entropy S by the Shannon entropy H, this boils down to $H(A'|E) - H(A'|B) = I(A':B) - I(A':E)$, giving the usual Csiszár-Körner bound [19] [see Eq. (29) below]. What appears in Eq. (7) is thus its quantum analog, given that Eve is allowed to keep her systems quantum.

Now, we have announced that one can compute a lower bound on the secret-key rate considering only two-qubit Bell-diagonal states. Precisely, this is true if Alice's preprocessing is bitwise. In general, it holds that if Alice's preprocessing is applied to strings of n bits, then one can restrict attention to Eve's collective attacks on n pairs. If we denote by r_n the corresponding bound for the secret-key rate r, one has $r \geqslant r_n \geqslant r_1$; it is an open problem whether strict inequalities hold.

In summary, we are going to compute the lower bound on the secret-key rate if Alice applies a bitwise preprocessing, i.e., Eq. (7). The quantity $R(\sigma_{A'BE})$ is given in Appendix A as an explicit function of the λ_i. This expression is independent of the protocol: as mentioned above, only the constraints on the λ_i, that is, the set Γ_Q, depend on the protocol. Possible improvements on the bound may come from more-than-one-bit preprocessing, and/or from revealing a part of the preprocessing publicly.

2. Lower bound for SARG04

The SARG04 protocol uses all the four sifting sets $\mathcal{S}_{\sigma\omega}$ (a different bound is found if one considers a modified protocol which uses only two sets; see Appendix B). One finds after some algebra

$$\lambda_1 = C \langle \Phi^+ | \rho_0 | \Phi^+ \rangle,$$

$$\lambda_2 = C(\langle \Psi^- | \rho_0 | \Psi^- \rangle + \langle \Phi^- | \rho_0 | \Phi^- \rangle + \langle \Psi^+ | \rho_0 | \Psi^+ \rangle),$$

$$\lambda_3 = \frac{C}{2}(\langle \Phi^- | \rho_0 | \Phi^- \rangle + \langle \Psi^+ | \rho_0 | \Psi^+ \rangle),$$

$$\lambda_4 = \frac{C}{2}(4\langle \Psi^- | \rho_0 | \Psi^- \rangle + \langle \Phi^- | \rho_0 | \Phi^- \rangle + \langle \Psi^+ | \rho_0 | \Psi^+ \rangle). \tag{13}$$

The following relations then hold:

$$\lambda_4 + 3\lambda_3 = 2\lambda_2, \tag{14}$$

$$\lambda_4 \geqslant \lambda_3. \tag{15}$$

Supposing that we leave $\lambda_2 = x$ free, we obtain $\lambda_1 = 1 - Q - x$ from Eq. (12), $\lambda_3 = x - Q/2$ and $\lambda_4 = 3Q/2 - x$ from Eq. (14); the positivity of λ_3 and Eq. (15) restrain x to lie in the range $[Q/2, Q]$. We optimize r_1 and find it positive provided $Q \leqslant 10.95\%$. If we had neglected the preprocessing, we would have found $Q \leqslant 9.68\%$, the same value obtained by Tamaki and Lo [9,20].

C. Single photon: Upper bound—an incoherent attack

As we noticed at the end of Sec. III B 1, the bounds we have just obtained may be subject to some future improvement when more complex preprocessing strategies are taken into account. In the meantime, we can easily derive an upper bound by computing explicitly a possible attack by Eve. We consider an incoherent attack, that is an attack consisting of (i) a unitary operation $\mathcal{U}$ coupling the qubit flying to Bob to Eve's systems; (ii) a suitable measurement on Eve's systems, after hearing the result of the sifting but before any other classical processing (this is the difference with collective attacks).

Even within the class of incoherent attacks, the full optimization is a hard task. The problem is not really at the level of the unitary $\mathcal{U}$. In fact, since both Alice's and Bob's system are qubits, Eve's ancilla may be taken without restriction to be four dimensional. Thus, the action of the unitary on states of the form $|\psi\rangle_A |R\rangle_E$ can be specified by only 16 parameters, not all independent—apart from the requirement of unitarity, we have imposed a symmetry on the set of states, namely, that $\mathcal{U}$ realizes a depolarizing channel (1) between Alice and Bob with the same D for $|\psi\rangle$ belonging to the x or to the z basis. In summary, the unitary is defined by a number of parameters which is small (at least for numerical optimization). What is not known at all *a priori*, is the kind of measurement Eve has to perform on her system, which would give her the best information on Alice's and Bob's bits. Here, we choose a specific kind of measurement that can be de-

fined for any $\mathcal{U}$ (Helstrom measurement, see below) and optimize the parameters of $\mathcal{U}$ in order to maximize Eve's information in such a measurement. The best $\mathcal{U}$ found with this method is *not* the phase-covariant cloning machine, i.e., the cloner which copies all the states of the x and the z bases with the same fidelity [13].

This result is interesting in itself because it shows that cryptography and cloning are clearly different tasks. In fact, the "states to be copied" are the same ones in SARG04 as in BB84, so the optimal cloner is the phase-covariant cloning machine in both cases. It turns out this cloner enters also the construction of the optimal incoherent eavesdropping for BB84; for SARG04, however, it is not the case. The cause of the difference is clear: in optimal cloning, one wants to optimize the fidelity of the output states to the input state; in optimal incoherent eavesdropping, one wants to optimize Eve's information, and this is *a priori* a completely different problem.

1. Eve's unitary operation

We start by describing the unitary $\mathcal{U}$ which we have found. It is defined by its action on the z basis of the qubit flying from Alice to Bob and on a reference state used by Eve as

$$\mathcal{U}|\sigma z\rangle_A|R\rangle_E = \sqrt{F}|\sigma z\rangle_B|0\rangle_{E_1}|\psi_\sigma(D)\rangle_{E_2} + \sqrt{D}|-\sigma z\rangle_B|1\rangle_{E_1}|0\rangle_{E_2} \tag{16}$$

with $\sigma=\pm$ and $|\psi_\sigma(D)\rangle=\sqrt{1-D/F}|0\rangle+\sigma\sqrt{D/F}|1\rangle$. Here, $D \in \left[0,\frac{1}{2}\right]$ is the only free parameter of the transformation. Note that Eve's system is only three dimensional; we used a two-qubit notation for convenience. In fact, with this notation, the action of the unitary in the x basis is similar to its action on the z basis, but the roles of E_1 and E_2 are reversed: writing with $\omega=\pm$, one has

$$\mathcal{U}|\omega x\rangle_A|R\rangle_E = \sqrt{F}|\omega x\rangle_B|\psi_\omega(D)\rangle_{E_1}|0\rangle_{E_2} + \sqrt{D}|-\omega x\rangle_B|0\rangle_{E_1}|1\rangle_{E_2}. \tag{17}$$

We suppose in the following that Alice publicly announces the set $\{|+z\rangle,|+x\rangle\}$ (i.e., Alice actually sends one of these two states), and that Bob accepts the bit. It has been verified that thanks to the symmetries of the attack, all the following still holds if Alice sends another state and/or announces another set.

Bob's states. Suppose for definiteness that Alice sends the state $|+z\rangle$. If we trace over Eve's system, we get Bob's state

$$\rho_B^{+z} = F|+z\rangle\langle+z| + D|-z\rangle\langle-z|. \tag{18}$$

Thus the effective channel induced on Alice-Bob by Eve's attack is a depolarizing channel (1) with disturbance D. If Bob measures his qubit in the z basis, then he will accept the (wrong) conclusive result $|-z\rangle$ with probability $p_{acc}^z=D$. If Bob now measures his qubit in the x basis, he will accept the (right) conclusive result $|-x\rangle$ with probability $p_{acc}^x=\langle-x|\rho_B|-x\rangle=1/2$. The quantum bit error rate after sifting is therefore

$$Q = \frac{p_{acc}^z}{p_{acc}^z + p_{acc}^x} = \frac{D}{1/2 + D}. \tag{19}$$

Note that, contrary to the case of BB84, $Q \neq D$; for small values of D we have actually $Q \simeq 2D$. We shall come back to this point in the comparison with BB84, Sec. III D below.

Eve's states. After sifting, Eve has to distinguish between four states, corresponding to the two possible states announced by Alice and the two cases in which Bob accepts the item. We write these states as $|\tilde{\psi}_E^{ab}\rangle$, where $a(b) \in \{0,1\}$ denotes Alice's (Bob's) classical bit:

$$|\tilde{\psi}_E^{00}\rangle = {}_B\langle -x|\mathcal{U}|+z\rangle|R\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{1-2D}|00\rangle + \sqrt{2D}|\Psi^-\rangle\right), \tag{20}$$

$$|\tilde{\psi}_E^{01}\rangle = {}_B\langle -z|\mathcal{U}|+z\rangle|R\rangle = \sqrt{D}|10\rangle, \tag{21}$$

$$|\tilde{\psi}_E^{10}\rangle = {}_B\langle -x|\mathcal{U}|+x\rangle|R\rangle = \sqrt{D}|01\rangle, \tag{22}$$

$$|\tilde{\psi}_E^{11}\rangle = {}_B\langle -z|\mathcal{U}|+x\rangle|R\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{1-2D}|00\rangle - \sqrt{2D}|\Psi^-\rangle\right), \tag{23}$$

with $|\Psi^-\rangle=(1/\sqrt{2})(|01\rangle-|10\rangle)$. Note that these states are not normalized, but the square of their norms corresponds to the probabilities with which they appear. Eve should now distinguish at best between these four states.

2. Eve's measurement: Helstrom strategy

We suppose that Eve uses the Helstrom strategy to guess Alice's bit [21]. This strategy, which may not be the optimal one for the present problem, consists in measuring the observable

$$M_A = \rho_E^{A=0} - \rho_E^{A=1} \tag{24}$$

where

$$\rho_E^{A=j} = \frac{1}{\frac{1}{2}+D}\left(|\tilde{\psi}_E^{j0}\rangle\langle\tilde{\psi}_E^{j0}| + |\tilde{\psi}_E^{j1}\rangle\langle\tilde{\psi}_E^{j1}|\right). \tag{25}$$

Some analytical results, which provide also a different perspective on Helstrom's strategy, are given in Appendix C. Here we just sketch the calculation that can also be implemented numerically from the beginning. There are three possible outcomes e for Eve's variable E. The probability of each outcome is

$$p_{E=e} = \langle m_e|\rho_E|m_e\rangle \tag{26}$$

with $\rho_E=\frac{1}{2}\rho_E^{A=0}+\frac{1}{2}\rho_E^{A=1}$. The information Eve gets on Alice's bit is

$$I(A:E) = H(A) - H(A|E) = 1 - \sum_e p_{E=e} H(A|_{E=e})$$

$$= 1 - \sum_e p_{E=e} h(p_{A=0|E=e}) \tag{27}$$

where h is binary entropy and where

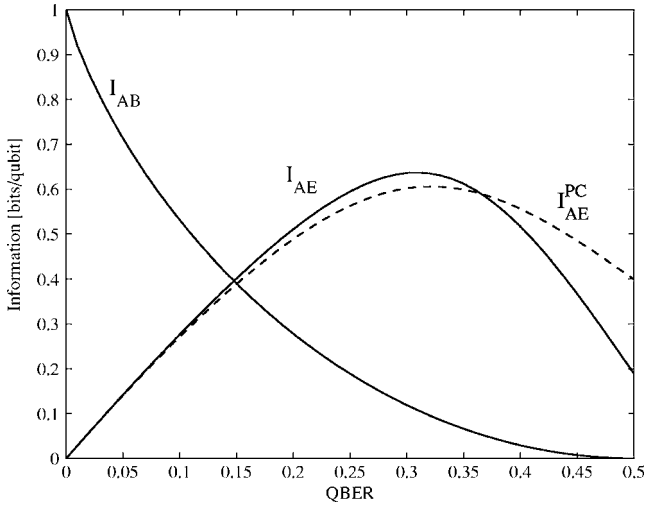

FIG. 1. Bob's and Eve's information on Alice's bit (before her possible preprocessing) for our individual attack and the attack using the phase-covariant (PC) cloning machine.

$$p_{A=0|E=e} = p_{A=0}\frac{p_{E=e|A=0}}{p_{E=e}} = \frac{1}{2}\frac{p_{E=e|A=0}}{p_{E=e}} \tag{28}$$

with $p_{E=e|A=0}=\langle m_e|\rho_E^{A=0}|m_e\rangle$. This information is plotted together with Bob's information $I(A:B)=1-h(Q)$ as a function of the QBER, Eq. (19), in Fig. 1. The curve of $I(A:E)$ for the attack using the phase-covariant cloning machine, taken from Ref. [8], is included for comparison. Our attack is slightly more efficient in the interesting region.

Actually, if Eve performs the measurement of M_A, she has a good guess on Alice's bit but very poor information on Bob's bit (the only thing she knows is that Bob's bit is equal to Alice's with probability $1-D$). Similarly, with reversed roles, if Eve measured $M_B=\rho_E^{B=0}-\rho_E^{B=1}$: numerically, the $I(B:E)$ so found is equal to $I(A:E)$ found when measuring M_A; but now, Eve has poor information on Alice's bit. For BB84 and the six-state protocols, measurements have been explicitly found which attain the optimal value for both Alice's and Bob's bits. We did not find such a measurement here. However, this is not important: before starting error correction and privacy amplification, Alice and Bob must choose whether to perform the direct or the reverse reconciliation; thus Eve can simply choose the suitable measurement.

3. Bound on the secret-key rate

An upper bound on the attainable secret-key rate using one-way communication and single-bit preprocessing is given by the Csiszar-Körner bound [19] which reads

$$r \leqslant R_{sk} = \max_{A'\leftarrow A}\{I(A':B) - I(A':E)\} \tag{29}$$

where A' is the result of a local processing of Alice's variables. The need for this maximization went unnoticed in the field of QKD until very recently [11], but is indeed present in the original paper. Here, we consider the case when the process $A\rightarrow A'$ consists in Alice's flipping her bit with some probability q. Bob's information is now

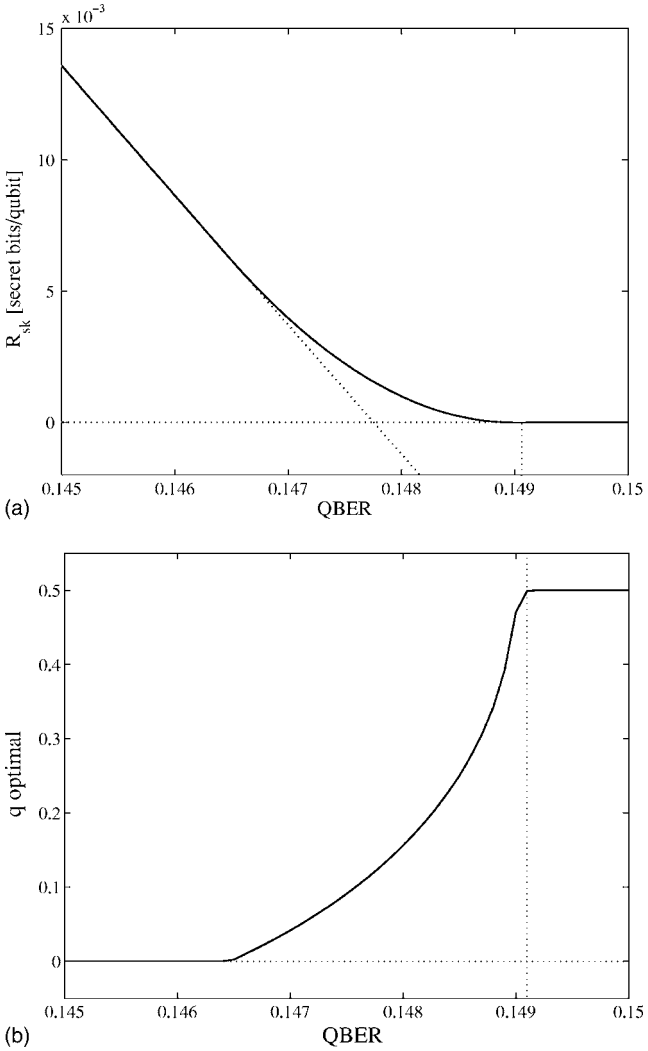

FIG. 2. Top: upper bound R_{sk} on the secret-key rate obtained with the attack under study with (solid lines) and without (dotted lines) Alice's optimal preprocessing, as a function of the QBER. Bottom: corresponding value of the optimal q. The preprocessing slightly increases the bound where the achievable secret-key rate becomes 0 (which we find to be 14.9%).

$$I(A':B) = 1 - h(Q') \tag{30}$$

where

$$Q' = (1-q)Q + q(1-Q). \tag{31}$$

As for Eve's information, it can be calculated with Eq. (27) upon changing $p_{A=0|E=e}$ to

$$p_{A'=0|E=e} = (1-q)p_{A=0|E=e} + qp_{A=1|E=e}. \tag{32}$$

Figure 2 displays the upper bound on the secret-key rate Eq. (29), with and without Alice's bit flipping (top) and the corresponding optimal value of q (bottom) as a function of the QBER. We can see that this preprocessing allows Alice and Bob to slightly increase the bound on the QBER where the achievable secret-key rate becomes zero. In the case

where Alice performs bitwise preprocessing as we consider here, this bound is 14.9%. Alice will do this preprocessing only for a QBER close to the bound of 14.9%, with q increasing as the QBER increases. At the bound, $q=0.5$: Alice flips half of her bits, so that both Bob's and Eve's information on her bits is completely randomized. After this optimal preprocessing, Fig. 1 would look as follows: both $I(A:B)$ and $I(A:E)$ stay the same up to $Q\approx 14.6\%$; then suddenly both drop rapidly to zero, with their difference given in the left graph of Fig. 2.

No preprocessing was taken into account in Ref. [8] for the attack using the phase-covariant cloner. When one includes bitwise preprocessing, the bound for that attack moves from 15.03% to 15.12%. Consequently, the attack presented here is still more efficient from Eve's standpoint.

D. Single photon: Comparison with BB84 protocol

In the previous paragraphs, we have provided lower and upper bounds for the security of SARG04 in a single-photon implementation, under the assumptions of one-way classical processing and bitwise preprocessing on Alice's side. The corresponding bounds for BB84 are known from Refs. [11,12]. The results are for the lower bound,

$$\text{extract a key if} \begin{cases} \text{BB84} & Q \lesssim 12.4\,\%\,, \\ \text{SARG04} & Q \lesssim 10.95\,\%\,; \end{cases} \tag{33}$$

and for the upper bound

$$\text{abort if} \begin{cases} \text{BB84} & Q \gtrsim 14.6\,\%\,, \\ \text{SARG04} & Q \gtrsim 14.9\,\%\,. \end{cases} \tag{34}$$

Looked at that way, SARG04 compares almost on equal grounds with BB84 in a single-photon implementation.

Experimentalists would, however, have a different look. Consider for a moment a detector with no dark counts, or more realistically, a situation in which the number of dark counts is negligible compared with the detection rate. In all practical experiments to date, the noise is such that the effective channel $\mathcal{E}$ between Alice and Bob becomes a depolarizing channel (1) characterized by its visibility V.

In BB84, for such a channel, the error rate on the sifted key is independent of the state $|\psi\rangle$: in fact, when the good basis has been chosen, one has simply $p_{right}=(1+V)/2$ and $p_{wrong}=(1-V)/2$. Consequently

$$Q = \frac{p_{wrong}}{p_{right}+p_{wrong}} = \frac{1-V}{2} \quad \text{(BB84)}. \tag{35}$$

In SARG04, the situation is different. If Bob chooses the good decoding basis (which is not the basis in which the qubit was encoded), then whenever he accepts, he guesses always right, and this happens with probability $p_{right}=\frac{1}{2}$ independently of V. If Bob chooses the wrong decoding basis and accepts, then he always guesses wrongly; and this happens with probability $p_{wrong}=(1-V)/2$. Thus

$$Q = \frac{p_{wrong}}{p_{right}+p_{wrong}} = \frac{1-V}{2-V} \approx 1-V \quad \text{(SARG04)}. \tag{36}$$

Note that we have already derived this formula above, Eq. (19) with $D=(1-V)/2$. For a fixed visibility, the QBER of SARG04 is almost twice the QBER of BB84. In this sense, the bounds of SARG04 compare unfavorably to those of BB84 in a single-photon implementation [22].

IV. PRACTICAL IMPLEMENTATION

As we stressed in the Introduction, it has not yet been possible to give the most general security criteria without adding assumptions about some simplified components. While theory progresses, experimentalists need realistic figures to design their experiments and to evaluate their results. These figures must take into account all the meaningful parameters characterizing Alice's source, the line ("quantum channel") linking Alice to Bob and Bob's detectors.

To compute these figures, we have to make several assumptions, which will be stated precisely in what follows, but in general fall into two categories.

(1) We restrict the class of Eve's attacks, taking into account only incoherent attacks, among which the PNS and its variants play the most important role. This assumption leads to an underestimate of Eve's power.

(2) We also have to specify the kind of check that Alice and Bob perform on their data. Apart from the estimate of the QBER, Alice and Bob can check the transmission of the line and more precisely the statistics of the number of photons.

The section is structured as follows. First, we describe the source, the line, and the detectors (Sec. IV A), the expected parameters in the absence of Eve (Sec. IV B), and the hypotheses on Eve's attack (Sec. IV C). Then we present the results of numerical optimizations (Sec. IV D); in the case of perfect optical visibility $V=1$, we provide also approximate analytical formulas. The last subsection (Sec. IV E) is devoted to a balance of the results obtained for SARG04, in comparison with BB84.

A. Description of the source, the line, and the detectors

1. Alice's source

Alice encodes her classical bits in light pulses; since a reference for the phase is not available to Eve and to Bob, the effective state prepared by Alice is a mixture which is diagonal in the photon-number basis:

$$\rho_A = \sum_{n=0}^{\infty} p_A(n)|n_\psi\rangle\langle n_\psi| \tag{37}$$

where $|n_\psi\rangle$ represents the state in which n photons are present in the state $|\psi\rangle$. In most practical QKD setups, Alice's source is an attenuated laser pulse, so

$$p_A(n) = p(n|\mu) = e^{-\mu}\frac{\mu^n}{n!}, \tag{38}$$

the Poissonian distribution of mean photon number μ. In this paper, the formulas where the notation $p_A(n)$ [or $p_B(n)$, see

below] appears explicitly are general; all the others suppose Eq. (38) to hold.

2. Alice-Bob quantum channel

The quantum channel which connects Alice and Bob is characterized by the losses α, usually given in dB/km (for optical fibers at the telecom wavelength 1550 nm, the typical value is $\alpha \simeq 0.25$ dB/km). The *transmission* of the line at a distance d is therefore

$$t = 10^{-\alpha d/10}. \tag{39}$$

The probability that Bob receives n photons is

$$p_B(n) = \sum_{m \geqslant n} p_A(m) C_m^n t^n (1-t)^{m-n} = p(n|\mu t) \tag{40}$$

through Eq. (38), where $C_m^n = m!/n!(m-n)!$. The other meaningful parameter of the channel is the fidelity of the transmission F (or the disturbance $D=1-F$). We assume a depolarizing channel (1):

$$\mathcal{E}[|+z\rangle] = F|+z\rangle\langle+z| + D|-z\rangle\langle-z| \tag{41}$$

$$= \tfrac{1}{2}|+x\rangle\langle+x| + \tfrac{1}{2}|-x\rangle\langle-x| + (\text{off-diagonal terms}). \tag{42}$$

and recall the link (2) between the parameters F and D, and the visibility V.

3. Bob's detectors

Bob uses single-photon counters with a limited quantum efficiency η and a probability of dark count per gate p_d. For simplicity of writing, in some intermediate formulas we shall write $\bar{\eta}=1-\eta$ and $\bar{p}_d=1-p_d$. The gate here means that Bob knows when a pulse sent by Alice is supposed to arrive, and opens his detectors only at those times; so here, "per (Bob's) gate" and "per (Alice's) pulse" are equivalent. Typical values nowadays are $\eta \simeq 0.1$ and $p_d \sim 10^{-5}$–10^{-6} for the detection of photons at telecom wavelengths.

B. Bob's detection and error rates

Bob receives n photons with probability $p_B(n)$ given in Eq. (40). We want to compute his detection and his error rate. For definiteness, we suppose from now on that Alice sends $|\text{sent}\rangle = |+z\rangle$, and publicly declares this state and $|\text{declared}\rangle = |+x\rangle$. Bob guesses correctly if he measures in the x basis and finds $|\text{ok}\rangle = |-x\rangle$; he guesses wrongly if he measures in the z basis and finds $|\text{wrong}\rangle = |-z\rangle$.

Among the peculiarities of SARG04 which must be discussed, is the role of *double clicks*. In BB84, when both detectors click, the item is discarded: in fact, a double click can appear only if (i) Bob has received and detected two photons, in the wrong basis, or (ii) Bob has detected just one photon but has had a dark count in the other detector; in both cases, there is no way to tell the value of the bit sent by Alice. In SARG04, things are different because Bob guesses correctly the bit when he measures in the "physically wrong" basis (basis x with our convention). A double click may mean precisely that the basis chosen by Bob is not the one chosen by Alice, and this gives the information on the bit. But the dark count case is still there, and introduces errors. In this paper, for simplicity we suppose that items with *double clicks are discarded* from the key, as in BB84; however, their rate is monitored, to prevent Eve from achieving an effective modification of η (see Sec. IV C).

1. Zero-click rate

When n photons arrive, the probability of not having any click is independent of the basis chosen by Bob and is given by

$$p_0(n) = (1-p_d)^2 (1-\eta)^n. \tag{43}$$

The corresponding zero-click rate is $C_0 = \Sigma_{n \geqslant 0} p_B(n) p_0(n) = (1-p_d)^2 p(0|\mu t \eta)$, i.e., there are no dark counts and no photon is detected.

2. Sifted key and QBER

The accepted-click rate on Bob's side is the sum of two terms. When Bob measures in the z basis, he accepts the (wrong) bit if there is one click in the $|-z\rangle$ detector (whether it is due to a photon or to a dark count), and no click in the $|+z\rangle$ detector. When n photons arrive, the probability of having a click only on the $|-z\rangle$ detector is

$$p_{acc}^z(n,V) = \sum_{k=0}^{n} C_n^k F^k D^{n-k} (\bar{p}_d \bar{\eta}^k)(1 - \bar{p}_d \bar{\eta}^{n-k}) = (1-p_d)[(1-F\eta)^n - (1-p_d)(1-\eta)^n], \tag{44}$$

with $C_n^k = n!/k!(n-k)!$. The accepted-click rate in the z basis is then $C_{acc}^z(V) = \Sigma_{n \geqslant 0} p_B(n) p_{acc}^z(n,V)$; using some standard calculation [23], we obtain for a Poissonian distribution

$$C_{acc}^z(V) = (1-p_d)[p(0|F\mu t\eta) - (1-p_d)p(0|\mu t\eta)]. \tag{45}$$

In the limit $\mu t \eta \ll 1$ (and $p_d \ll 1$, which is always the case), one finds $C_{acc}^z(V) \approx D\mu t\eta + p_d$. We highlighted the dependence of these quantities on V because it will be important for what follows.

When Bob now measures in the x basis, he accepts the (right) bit if he gets a click on the $|-x\rangle$ detector, and no click on the $|+x\rangle$ detector. Because of Eq. (42), we just have to change F to $\frac{1}{2}$ in the previous formulas:

$$p_{acc}^x(n) = (1-p_d)[(1-\eta/2)^n - (1-p_d)(1-\eta)^n], \tag{46}$$

so that for Poissonian sources $C_{acc}^x = (1-p_d)[p(0|\mu t\eta/2) - (1-p_d)p(0|\mu t\eta)] \approx \frac{1}{2}\mu t\eta + p_d$. Since the two bases are randomly chosen, the global probability for Bob to accept a click is

$$p_{acc}(n,V) = \frac{1}{2} p_{acc}^x(n) + \frac{1}{2} p_{acc}^z(n,V), \tag{47}$$

and the accepted-click rate on Bob's side (i.e., the length of the sifted key) is

$$C_{acc}(V) = \frac{1}{2}C^x_{acc} + \frac{1}{2}C^z_{acc}(V). \tag{48}$$

All the items C^x_{acc} being correct and all the items $C^z_{acc}(V)$ being wrong, the QBER is

$$Q = \frac{\frac{1}{2}C^z_{acc}(V)}{C_{acc}(V)}. \tag{49}$$

For $p_d \ll \mu t \eta \ll 1$ and $D \ll \frac{1}{2}$, we find

$$Q \approx 2D + 2\frac{p_d}{\mu t \eta} \equiv Q_{opt} + Q_{det}, \tag{50}$$

$$C_{acc}(V) \approx \frac{1}{4}\mu t \eta (1 + Q_{opt} + 2Q_{det}). \tag{51}$$

As expected, the sifted-key rate increases in the presence of errors. Note also that the QBER is twice the one expected for BB84, for the same parameters: now, μ is going to be larger for SARG04 than it is for BB84, so that Q_{det} is not really larger; however, D is fixed by the visibility: SARG04 is thus more sensitive to losses of visibility than BB84 is.

Finally, allowing for Alice's preprocessing, the mutual information between Alice and Bob is

$$I(A':B) = C_{acc}(V)[1 - h(Q')] \tag{52}$$

with Q' related to Q [Eq. (49)] as in Eq. (31).

3. Double-click rate

The calculation of the double-click rates $C^{x,z}_2$ is similar to the one of $C^{x,z}_{acc}$. For each basis, it holds that $C^{x,z}_2 = \Sigma_{n\geq 2} p_B(n) p^{x,z}_2(n)$ where $p^{x,z}_2(n)$ is the probability of a double click conditioned on the fact that exactly n photons reach Bob. Consider first the z basis: one has to modify Eq. (44) in order to describe a click in both detectors, so we have to replace $(\bar{p}_d \bar{\eta}^k)$ with $(1 - \bar{p}_d \bar{\eta}^k)$. Thence

$$p^z_2(n,V) = 1 - (1-p_d)[(1-F\eta)^n + (1-D\eta)^n] + (1-p_d)^2(1-\eta)^n. \tag{53}$$

The double-click probability in the x basis is obtained by replacing both F and D by $\frac{1}{2}$; by comparison with Eqs. (43) and (46), one finds

$$p^x_2(n) = 1 - p_0(n) - 2p^x_{acc}(n). \tag{54}$$

For Poissonian sources, this yields [23]

$$C^z_2(V) = 1 - (1-p_d)[p(0|\mu t \eta F) + p(0|\mu t \eta D)] + (1-p_d)^2 p(0|\mu t \eta), \tag{55}$$

and $C^x_2 = [1 - (1-p_d)p(0|\mu t \eta/2)]^2$. Having written down all Bob's parameters, we can move on to present the class of attacks by Eve that we consider.

C. Eve's attacks: Hypotheses, information, and constraints

1. Overview of the hypotheses

Some of the hypotheses on Eve's attacks have been rapidly introduced in the previous sections. Here we make the exhaustive list of the assumptions.

Hypothesis 1. Eve performs incoherent attacks: she attacks each pulse individually, and measures her quantum systems just after the sifting phase. This hypothesis allows us to perform explicit calculations of an upper bound for the secret-key rate. We shall say more on these attacks in the next section (Sec. IV C 2). The hypothesis of incoherent attacks implies in particular that after sifting, Alice, Bob and Eve share several independent realizations of a random variable distributed according to a classical probability law. Under this assumption and the assumption of one-way error correction and privacy amplification, the Csiszár-Körner bound applies [19] and the achievable secret-key rate is given by Eq. (29) [24].

Hypothesis 2. Eve can replace the actual channel with a lossless channel. This allows her to take advantage of the losses: she can block pulses on which she has poor or no information, keep some photons out of multiphoton pulses, etc. Because of Eve's intervention, the pulses that reach Bob obey the statistics $p_{B|E}(n)$, *a priori* different from the expected one (40). The most general assumption would consist in leaving $p_{B|E}(n)$ completely free, and estimate Eve's information from it. The most conservative assumption consists in requiring $p_{B|E}(n) = p_B(n)$ for all n, and aborting the protocol if this requirement is not satisfied; this is the spirit of decoy-state protocols [6]. In this paper, we choose an intermediate requirement: we constrain Eve to reproduce the expected count rates C^x_{acc}, C^x_2, and the rate of no detection (note that the rate of inconclusive detections will be reproduced as well). This assumption is consistent with the idea of introducing no modification in the hardware: without allowing for decoy states and/or more detectors, these rates are the only parameters that can be measured. Eve has also a constraint on C^z_{acc} and C^z_2, though of a different nature: these two quantities must depend on a single parameter V according to Eqs. (45) and (55).

Hypothesis 3. We work in the *trusted-device scenario*. While the optical error D in the quantum channel (the imperfect visibility) is entirely attributed to Eve's intervention, we assume that Eve has no access to Bob's detector: η and p_d are given parameters for both Bob and Eve. Eve will of course adapt her strategy to the value of these parameters, but she cannot modify them [25].

2. More on the class of attacks

In Hypothesis 1, we have explained that we restrict our attention to incoherent attacks. Here is a detailed description of Eve's strategy. Eve, located immediately outside Alice's station, makes a *nondemolition measurement of the number of photons n* in each pulse. This does not introduce any error because ρ_A [Eq. (37)] is diagonal in the Fock basis. Based on this information, Eve implements an attack $\mathbf{K}$ with probability $p_{\mathbf{K}}(n)$, so that the channel Alice-Bob is of the form

$$\rho_B = \mathcal{E}[\rho_A] = \sum_n p_A(n) \sum_{\mathbf{K}_n} p_{\mathbf{K}}(n) \mathcal{E}_{\mathbf{K}}[|n_\psi\rangle\langle n_\psi|]. \tag{56}$$

These are the attacks that we investigate.

Storage attack **S**. If $n \geq 2$, Eve can choose to store $k < n$ photons, while forwarding the remaining n-k photons to Bob

on the lossless line. When Alice reveals the states, Eve makes the measurement that maximizes her information, thus guessing Alice's bit correctly with probability $p_k=1/2+(1/2)\sqrt{1-1/2^k}$. This is the original type of PNS attack [5]. After Alice's possible preprocessing (bit flip with probability q), Eve's guess is correct with probability $p'_k=(1-q)p_k+q(1-p_k)$; whence Eve's information becomes

$$I_{\mathbf{S}}(k)=1-h(p'_k) \tag{57}$$

conditioned on Bob's accepting the item. We denote by $s(k|n)$ the probability that Eve, having chosen to perform a storage attack, stores exactly k photons.

Intercept-resend attack **I**. If $n\geqslant 3$, the four states $|\psi\rangle^{\otimes n}$, with $|\psi\rangle=|\pm z\rangle$ or $|\pm x\rangle$, become linearly independent. Eve can then perform an unambiguous discrimination of the sent state, whose probability of success is

$$p_{OK}(n)=1-\left(\frac{1}{2}\right)^{\lfloor (n-1)/2\rfloor} \tag{58}$$

(for $n>3$, this is a numerical result [8]). In case of success, Eve has full information about the bit and she forwards m new photons to Bob prepared in the state $|\psi\rangle$ [any value m is chosen with probability $r(m|n)$]. Otherwise, she blocks the item. Note that this strategy, contrary to the storage attack, requires neither a quantum memory (obviously) nor a lossless line: having succeeded in unambiguous discrimination, Eve has the new photons prepared by an accomplice of hers who is close to Bob's laboratory. This form of PNS attack was first discussed by Dušek and coworkers [26]. After Alice's preprocessing, Eve's information in case of success becomes

$$I_{\mathbf{I}}(n)\equiv I_{\mathbf{I}}=1-h(q), \tag{59}$$

again conditioned on Bob's accepting the item.

Unitary interaction **U**. Both the **S** and the **I** attacks provide Eve with information only thanks to the losses, and do not introduce any error in Alice-Bob correlations ($V=1$). If there is a reduced visibility $V=1-\varepsilon$, Eve can also take advantage of it by performing an attack which introduces some errors (and no losses). Noting that information on pulses with $n\geqslant 2$ can be obtained using **S** or (for $n\geqslant 3$) **I**, we suppose that errors will be introduced only to gain information about $n=1$ items. Moreover, as mentioned above, ε is typically quite small: instead of tackling the very hard problem of optimizing this family of attack, for simplicity we choose a representative, namely the attack developed in Sec. III C. As described there, she obtains an information

$$I_{\mathbf{U}}(\tilde{D})=1-\sum_e p_{E=e}h(p_{A'=0|E=e}). \tag{60}$$

The important point to stress is that in the unitary operation $\mathcal{U}$ one must insert a value $\tilde{D}=\frac{1}{2}(1-\tilde{V})$ which is in general *larger* than the average error D (in other words, $\tilde{V}\leqslant V$). This is because Eve introduces only errors in a fraction of the pulses, so in those items she can introduce more perturbation than the average [27].

Blocking **B**. Eve blocks all the n photons. In this case of course, Bob receives nothing and can accept the item only in the case of a dark count. On the one hand, Eve is willing to block a pulse only when she has little or no information on it (typically, one- and two-photon pulses). On the other hand, Alice and Bob will always choose μ such that Eve will not be able to block all single- and two-photon pulses without changing Bob's expected detection rate. Therefore, we set

$$p_{\mathbf{B}}(n)=0 \quad \text{for } n\geqslant 3. \tag{61}$$

Letting the photons pass **L**. Finally, Eve may be forced to let all the photons in the pulse go to Bob in order to preserve the counting rates. In this case, Bob may accept the item but Eve does not get any information on Alice's bit. However, we shall consider

$$p_{\mathbf{L}}(n)=0 \quad \text{for all } n. \tag{62}$$

The reason is as follows. For $n=1$, Eve applies the **U** strategy which does not reduce the counting rates and gives her some information [for $V=1$, the **U** strategy with a disturbance $\tilde{D}=0$ is equivalent to $p_{\mathbf{L}}(1)$]. For $n>1$, when losses are large enough, that is at not too short distances, condition (62) is obviously part of the best strategy for Eve. So the only effect of this condition is to prevent us from studying SARG04 at short distances (for the values of the parameters used below, in particular for $\eta=0.1$, the shortest distance at which constraints can be satisfied is found to be $\sim$24 km).

Note that, for the qubit encoding, the channel (56) behaves as a depolarizing channel. In fact, attacks **S** and **I** do not introduce any error, and attack **U** was shown in Sec. III C to induce a depolarizing channel between Alice and Bob.

A comment is needed about the exhaustiveness of our list of attacks. We have stressed enough that **U** is not optimized. The list of zero-error attacks, on the contrary, is fairly complete among the incoherent PNS attacks for the analysis of SARG04 [28]. One may well construct more general strategies: e.g., for $n=5$, Eve may try **I** on three photons, and if she does not succeed, she performs **S** on the remaining two. However, the mean number of photons μ will be chosen small enough so that the meaningful items are those with $n\leqslant 3$, $n=4$ items playing the role of a small correction, and all the higher-number items being completely negligible.

3. Eve's information and constraints

We are now able to write down formulas for $I(A':E)$ and for the constraints that Eve must satisfy. For each n, Eve uses strategy **X** with probability $p_{\mathbf{X}}(n)$, so that we have

$$p_{\mathbf{B}}(1)+p_{\mathbf{U}}(1)=1, \quad n=1, \tag{63}$$

$$p_{\mathbf{B}}(2)+p_{\mathbf{S}}(2)=1, \quad n=2, \tag{64}$$

$$p_{\mathbf{S}}(n)+p_{\mathbf{I}}(n)=1, \quad n\geqslant 3. \tag{65}$$

Under this family of attacks, Eve's information on Alice's bits after sifting and preprocessing is

$$I(A':E) = p_A(1)p_{\mathbf{U}}(1)I_{\mathbf{U}}(\tilde{D})p_{acc}(1,\tilde{V}) + \sum_{n\geqslant 2} p_A(n)\Bigg(p_{\mathbf{S}}(n)\sum_{k=1}^{n-1} s(k|n)I_{\mathbf{S}}(k)p_{acc}(n-k,1) + p_{\mathbf{I}}(n)p_{OK}(n)I_{\mathbf{I}} \sum_{m\geqslant 1} r(m|n)p_{acc}(m,1)\Bigg) \quad (66)$$

where the $p_{acc}(n,V)$ are given in Eq. (47).

Eve is going to choose her parameters in order to maximize $I(A':E)$, under the constraints described in Hypothesis 2. To write down these constraints, one first notes that the number of photons that reach Bob is distributed according to

$$p_{BE}(n>0) = \delta_{n,1}p_A(1)p_{\mathbf{U}}(1) + \sum_{m>n} p_A(m)p_{\mathbf{S}}(m)s(m-n|m) + \sum_{m\geqslant 3} p_A(m)p_{\mathbf{I}}(m)p_{OK}(m)r(n|m), \quad (67)$$

$$p_{BE}(n=0) = 1 - \sum_{n>0} p_{BE}(n). \quad (68)$$

Of course, there is no reason for $p_{B|E}(n)$ to be Poissonian, even if $p_A(n)$ is. Now, according to Hypothesis 2, Eve is constrained to satisfy

$$\sum_n p_{BE}(n)p_0(n) \equiv \sum_n p_B(n)p_0(n), \quad (69)$$

$$\sum_n p_{BE}(n)p^x_{acc}(n) \equiv \sum_n p_B(n)p^x_{acc}(n), \quad (70)$$

$$\sum_n p_{BE}(n)p^x_2(n) \equiv \sum_n p_B(n)p^x_2(n), \quad (71)$$

$$\sum_n p_{BE}(n)p^z_{acc}(n,1) + q(1)[p^z_{acc}(1,\tilde{V}) - p^z_{acc}(1,1)] \equiv \sum_n p_B(n)p^z_{acc}(n,V), \quad (72)$$

$$\sum_n p_{BE}(n)p^z_2(n,1) + q(1)[p^z_2(1,\tilde{V}) - p^z_2(1,1)] \equiv \sum_n p_B(n)p^z_2(n,V) \quad (73)$$

with V the average visibility that Eve chooses to introduce and $q(1)=p_A(1)p_{\mathbf{U}}(1)$ the only cases where Eve introduces errors. Note that the value of $\tilde{V}$ is defined by Eqs. (72) and (73).

The five constraints (69)–(73) are actually not independent and can be reduced to the following set (derivation in Appendix D):

$$\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1) = \vec{\mathcal{P}}_B\cdot\vec{\Gamma}(1), \quad (74)$$

$$\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1/2) = \vec{\mathcal{P}}_B\cdot\vec{\Gamma}(1/2), \quad (75)$$

$$p_A(1)p_{\mathbf{U}}(1)\eta\tilde{D} = \vec{\mathcal{P}}_B\cdot[\vec{\Gamma}(F) - \vec{\Gamma}(1)], \quad (76)$$

where we have stored the probabilities $p_B(n)$ and $p_{B|E}(n)$ in the vectors $\vec{\mathcal{P}}_B$ and $\vec{\mathcal{P}}_{B|E}$ and where the vectors $\vec{\Gamma}(x)$ depend only on the detector's efficiency η, their respective components being $\gamma_n(x)=(1-x\eta)^n$ for all $n\geqslant 0$. In particular, the last condition (76) together with (63) determines the error $\tilde{D}$ that Eve can introduce on all the one-photon pulses that she does not block. As expected, this relation reduces to $\tilde{D}=0$ in the case $V=1$.

In the case where Alice holds a Poissonian source with mean photon number μ, we have $\vec{\mathcal{P}}_B\cdot\vec{\Gamma}(x)=p(0|x\,\mu t\eta)$, whence Eqs. (74)–(76) read explicitly

$$\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1) = p(0|\mu t\eta), \quad (77)$$

$$\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1/2) = p(0|\mu t\eta/2), \quad (78)$$

$$p(1|\mu)p_{\mathbf{U}}(1)\eta\tilde{D} = p(0|\mu t\eta F) - p(0|\mu t\eta). \quad (79)$$

D. Optimization over Eve's strategy and Alice's parameters

We have at present collected all the pieces that are needed for our study. For any fixed value of μ and q, Eve is going to choose her parameters $p_{\mathbf{X}}(n)$, $s(k|n)$, and $r(m|n)$ in order to maximize $I(A':E)$ [Eq. (66)] under the constraints (77)–(79). Alice and Bob must choose μ and q in order to maximize R_{sk} [Eq. (29)], with $I(A':B)$ given in Eq. (52) and with $I(A':E)$ computed as just described. This double optimization will be done numerically; for the case $V=1$, we shall also provide some analytical approximations, both as a consistency check for the numerics and as a tool for practical estimates.

1. Restricting the number of free parameters

Even in the perspective of using a computer, we have to simplify the problem further: the number of free parameters is *a priori* infinite. In particular, we have to discuss the probabilities $s(k|n)$ and $r(m|n)$ associated, respectively, with the **S** and **I** attacks. These are related to the number of photons that Eve forwards to Bob. We first notice that the constraints (77) and (78) can be satisfied up to the order $O(\mu t\eta)^3$ by setting

$$p_{BE}(1) = \mu t - (\mu t)^2, \quad (80)$$

$$p_{BE}(2) = \frac{1}{2}(\mu t)^2, \quad (81)$$

and all the others $p_{B|E}(n>2)=0$; that is, for each item, Eve forwards either one or two photons to Bob. We consider that Eve forwards two photons only after some **I** attacks, because this does not cost her any information; whereas, were she to forward two photons in an **S** attack, fewer photons would be left in her quantum memory to estimate the state. When Eve performs the **I** attack on a three-photon pulse, she can forward either one or two photons; when she performs it on a

higher-n pulse, she always forwards two photons. In conclusion, we assume

$$s(k|n) = \delta_{k,n-1} \quad \text{for all } n, \tag{82}$$

$$r(2|3) = 1 - r(1|3), \tag{83}$$

$$r(m|n) = \delta_{2,m} \quad \text{for all } n \geq 4. \tag{84}$$

Summarizing, the free parameters for Eve's attack are

$$\{p_{\mathbf{U}}(1), p_{\mathbf{S}}(2), p_{\mathbf{S}}(3), p_{\mathbf{I}}(3,2), p_{\mathbf{S}}(4), \ldots, p_{\mathbf{S}}(n_{max})\} \tag{85}$$

where $p_{\mathbf{I}}(3,2) = p_{\mathbf{I}}(3) r(2|3)$ and n_{max} is a cutoff in the number of photons allowed in a pulse—we have chosen $n_{max}=7$ in what follows, although *a posteriori* we verified that $n_{max}=5$ would have given the same results except for the shortest distances that we considered. This choice of free parameters, in particular the choice of $p_{\mathbf{I}}(3,2)$ instead of $r(2|3)$, is useful because all the constraints (79)–(81) become *linear* in the parameters; of course, one must add a fourth linear constraint, namely,

$$p_{\mathbf{S}}(2) + p_{\mathbf{I}}(3,2) \leq 1. \tag{86}$$

Maximization of a function (here, Eve's information) under a set of linear constraints is achieved in MATLAB with the predefined function "fmincon." At this point, we can run our numerical optimization of μ as a function of the distance.

2. Results, part 1: Eve's parameters

We have run our software with the following parameters: $\alpha=0.25$, $\eta=0.1$, $p_d=10^{-5}$. These are not the very best values that we can achieve in the laboratory, but we have already used them many times and it will be useful for comparison, especially with Ref. [15]. The numerical simulation achieves a faithful result only for $d \gtrsim 24$ km, because of Eq. (62), and for $V \gtrsim 0.92$ (recall that for $V \lesssim 0.825$ the secret-key rate becomes zero even in a single-photon implementation; it is then not astonishing that the visibility becomes more critical when Eve can take advantage also of multiphoton pulses). Here is what is observed for the optimal parameters of Eve's attack.

(1) $n=1$. $p_{\mathbf{U}}(1)$ is always zero for $V=1$. This means that in this case Eve blocks all the single-photon pulses. For $V<1$, it turns out that $\tilde{D}$ is constant at the value $\tilde{D}_0=0.191$ over all the distances (more precisely, over all the distances for which the best preprocessing by Alice consists in doing nothing, which are all the region of interest as will be explained later). The value of $p_{\mathbf{U}}(1)$ is thus determined by Eq. (79).

(2) $n=2$. $p_{\mathbf{S}}(2)$ is between zero and one. This means that Eve cannot block all the two-photon items.

(3) $n=3$. $p_{\mathbf{S}}(3)$ is zero, $p_{\mathbf{I}}(3,2)$ is between zero and one. That is, when the pulse contains three photons, Eve always performs the **I** attack; sometimes she sends out one photon and sometimes two. Actually, this rate of forwarding two photons is already enough to reproduce the constraint (81), as is implied by the following item.

(4) $n \geq 4$. $p_{\mathbf{S}}(n)=1$: Eve performs always the **S** attack.

Remarkably, most of the features of Eve's optimal attack can be rederived analytically and the derivation is *independent* of the form of the $p_A(n)$. This is expected, because Eve first measures the number of photons n, then adapts her strategy to her result; thus, the frequency of occurrence of any value of n does not play any role in defining her best attack for each n—although it will of course determine the fraction of information that each attack provides her. The price to pay for the analytical approach is that, to avoid getting lost, one had better neglect the constraint (81) on two photons. We present this analytical derivation in Appendix E. In summary, a numerical approach, which assumes a Poissonian distribution for Alice's source and can deal with the full set of constraints, and an analytical one, in which the independence of the source's statistics is explicit but the constraints must be simplified, converge to the same result: we have indeed found Eve's optimal attacks within the class which we are considering, independently of the statistics of Alice's source—our assumptions on Eve's attacks are reasonable provided the source is such that $p_A(1) > p_A(2) > p_A(3) \ldots$

3. Results, part 2: μ and R_{sk}

Having Eve's best attack, we can compute for any distance the optimal value of μ and the corresponding upper bound R_{sk} on the secret-key rate. The results of numerical optimization are shown in Fig. 3. Several points are worth stressing.

(1) We recall first that these results are valid for a large but still restricted class of attacks by the eavesdropper, according to the hypotheses described in Secs. IV C and IV D 1. Moreover, the curve for $V=0.95$ depends also on our choice of introducing a **U** attack only on the $n=1$ pulses. Thus, R_{sk} is an upper bound on the achievable secret-key rate, which remains to be computed.

(2) The optimal value of μ is above 0.1 for all the range that we considered, both for $V=1$ and for $V=0.95$; for $d=24$ km and $V=1$ we have $\mu_{opt}=1.55$. In contrast to the case of BB84 [15], μ does not decrease faster to zero as the critical distance approaches.

(3) Alice's preprocessing is nontrivial ($q>0$) only in the critical region where the presence of dark counts bends the curve below the linear (in logarithmic scale) regime. In principle, one tends to avoid working in that region.

As in the case of Eve's parameter, we complement the numerical optimization with some analytical studies, even at the price of some approximations: this is useful both to legitimate the numerical result and to provide formulas for rapid estimates. We consider $\mu t \eta \ll 1$ and obviously $p_d \ll 1$. We suppose that Eve forwards always one photon to Bob, thus taking the one-photon constraint (80) at the leading order and neglecting the two-photon constraint (81); in addition, we restrict to the case $V=1$, whence constraint (79) is automatically satisfied, and we neglect Alice's preprocessing by setting $q=0$. From the study of Eve's attack we know that we can set $p_{\mathbf{U}}(1)=0$, $p_{\mathbf{S}}(3)=0$, and $p_{\mathbf{S}}(n \geq 4)=1$. For a Poissonian source then

$$I(A:B) \simeq \left(\frac{\mu t \eta}{4} + p_d \right) [1 - h(Q(\mu))], \tag{87}$$

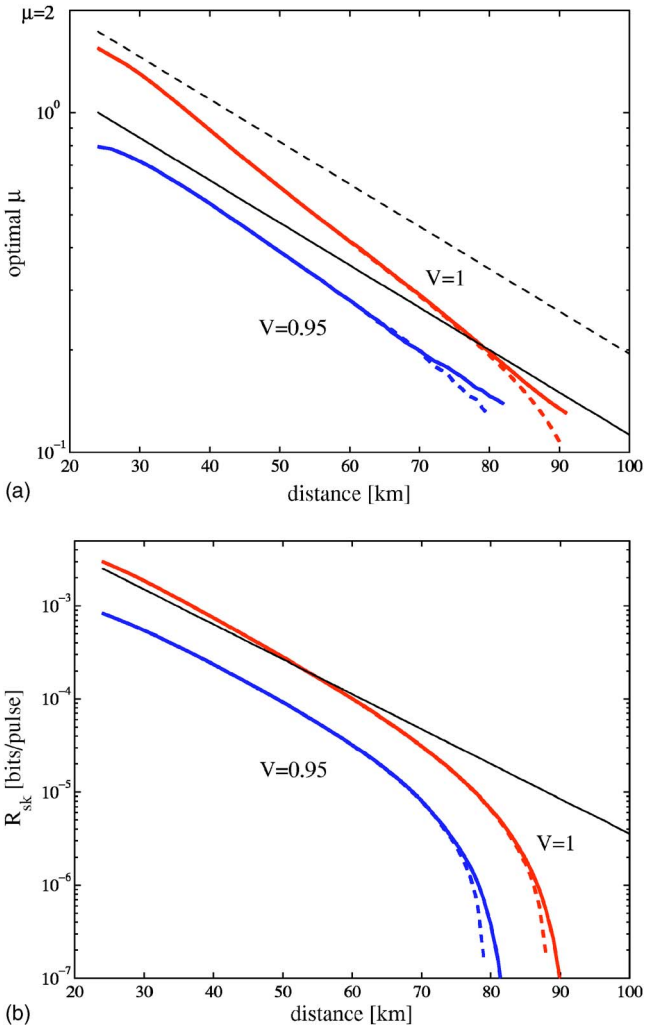

FIG. 3. (Color online) Optimal μ and upper bound R_{sk} on the secret-key rate per pulse (logarithmic scale) for Poissonian sources as a function of the distance, for $\alpha=0.25$, $\eta=0.1$, and $p_d=10^{-5}$, and for $V=1$ and 0.95. The full thick lines are the result of the numerical optimization, considering also Alice's preprocessing; the dashed thick lines are the same, without Alice's preprocessing ($q=0$). The full thin lines are the analytical approximations for $V=1$, Eq. (91); the dashed thin line in the upper figure is the critical value $\mu=2\sqrt{3t}$ at which $R_{sk}=0$ according to the approximate formula (90).

$$I(A:E) \simeq \frac{\eta}{4}\left(\mu t I_{\mathbf{S}}(1) + \tfrac{1}{2}p(3|\mu)[1-I_{\mathbf{S}}(1)] + \sum_{n\geqslant 4} p(n|\mu)[I_{\mathbf{S}}(n-1)-I_{\mathbf{S}}(1)]\right), \tag{88}$$

with

$$Q(\mu) = \frac{1}{2+\mu t\eta/2p_d}. \tag{89}$$

These are nonalgebraic functions, so the analytical maximization of R_{sk} is still impossible; but it is easily done numerically. It yields a careful estimate of both μ and R_{sk} in the typical working regime (40–70 km in Fig. 3), diverges for shorter distances, and underestimates the limiting distance. Thus, in practice, one can use these two equations to estimate the optimal parameters and to keep away from the limiting distance.

In order to reach analytical approximate solutions to the maximization problem, we further neglect the correction $1-h(Q)$ in the expression of $I(A:B)$ (i.e., we suppose $\mu t\eta \gg p_d$), the contribution of the pulses with $n\geqslant 4$ photons in the expression of $I(A:E)$, and the factor $e^{-\mu}$ in $p(3|\mu)$—this last assumption is the worst one, because we are dealing with $\mu\gtrsim 1$ at short distance. That leads to

$$R_{sk} \approx \frac{\eta}{4}[1-I_{\mathbf{S}}(1)]\left(\mu t - \frac{\mu^3}{12}\right). \tag{90}$$

The optimum is

$$R_{sk} \approx \frac{\eta}{3}[1-I_{\mathbf{S}}(1)]t^{3/2} \quad \text{for } \mu_{opt}=2\sqrt{t}. \tag{91}$$

These values are plotted in Fig. 3 together with the result of the exact numerical optimization. We see that the approximations are rough as expected but grasp the correct order of magnitude. Finally note that, contrary to the case of BB84 [15], we have not been able to find a closed analytical expression for the limiting distance, the difference here being that μ does not fall rapidly to zero when approaching this distance.

E. Attenuated laser: Comparison with BB84 protocol

Finally, we compare the performances of the SARG04 and those of the BB84 under identical conditions, from Ref. [15]. Since Alice's preprocessing was not taken into account in that work, for coherence we compare the results for $q=0$—it is not difficult to see that the contribution of this preprocessing in BB84 is numerically negligible, as it is for SARG04 [29].

The optimal μ and the upper bound R_{sk} on the secret-key rate are plotted in Fig. 4. We see that SARG04 allows an increase of the secret-key rate at moderately large distance, and of the limiting distance. It seems that BB84 achieves a better secret-key rate at short distance. Although we cannot make any final commitment because we have made hypotheses that prevent us from studying that regime, one might understand it from the following argument: at short distance, Eve can do essentially no PNS attack for inefficient detectors; therefore, the sifting ratio becomes the important parameter—now, in SARG04 only one-quarter of the items are kept, while in BB84 half of the items are kept.

The present analysis supersedes the one made in Refs. [7,8], which supposed a fixed value of μ for all distances.

V. CONCLUSION

In conclusion, we have studied the SARG04 protocol for two different types of source of light on Alice's side.

For the implementation using single-photon sources, we have obtained a lower and an upper bound for security against all possible attacks by the eavesdropper. These bounds are close to those obtained for the BB84 protocol.

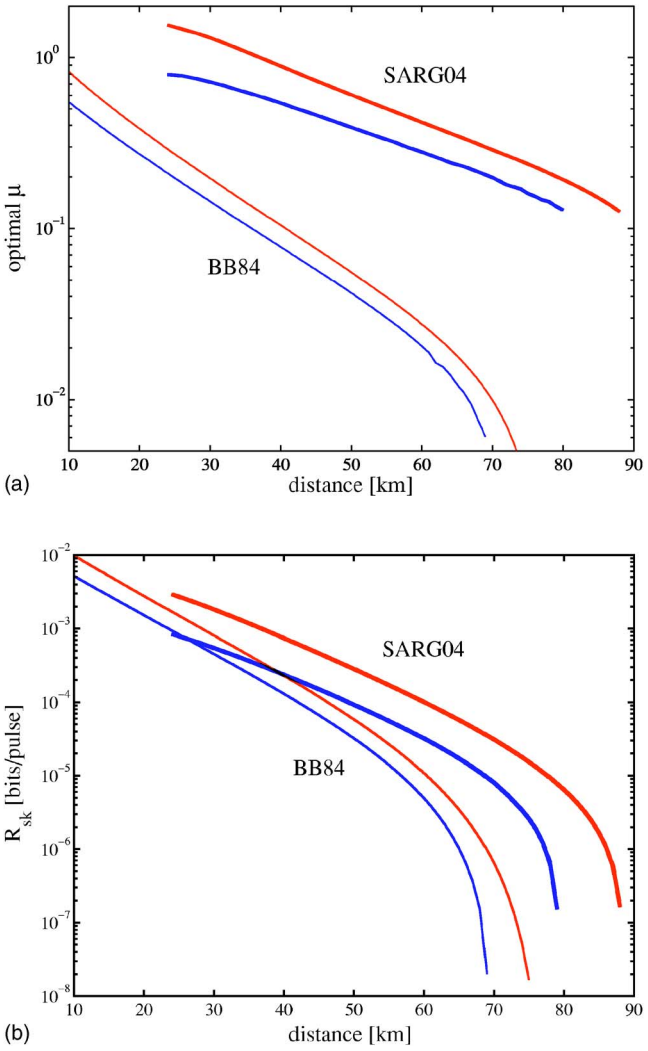

FIG. 4. (Color online) Optimal μ and upper bound R_{sk} on the secret-key rate per pulse (logarithmic scale) for Poissonian sources as a function of the distance, for $\alpha=0.25$, $\eta=0.1$, and $p_d=10^{-5}$, and for $V=1, 0.95$. Thick lines, SARG04 (identical to Fig. 3, with $q=0$); thin lines, BB84, under the same conditions.

However, if a channel of a given visibility is available, then the QBER of SARG04 is twice the QBER of BB84. Interestingly, the upper bound for SARG04 was obtained for an incoherent attack based on a unitary which is not the phase-covariant quantum cloner.

For the realistic implementation using an attenuated laser (Poissonian source), we have restricted the class of Eve's attacks to incoherent attacks, in particular the most studied forms of PNS attacks. In this case, SARG04 performs better than BB84, both in the achievable secret-key rate and in the limiting distance.

These results strengthen the conclusion of Refs. [7,8,30]: once quantum correlations have been distributed, different ways of encoding and decoding the classical information lead to different performances according to the physical characteristics of the setup. The full potentialities of this insight have still to be developed.

ACKNOWLEDGMENTS

We thank Antonio Acín and the members of the QIT workgroup in the SECOQC network for discussions, and Armand Niederberger for help with the software. We acknowledge financial support from the European Project SECOQC and from the Swiss NCCR "Quantum Photonics."

APPENDIX A

In this appendix we give more details about the calculation of the lower bound. The following is not specific to the SARG04 protocol, but can be applied to any protocol. As discussed in Sec. III B, in order to compute a lower bound on the secret-key rate, we can consider the state that Alice and Bob share before the preprocessing to be of the form (10), which we rewrite here:

$$\rho_2 = \lambda_1 P_{\Phi^+} + \lambda_2 P_{\Phi^-} + \lambda_3 P_{\Psi^+} + \lambda_4 P_{\Psi^-}. \tag{A1}$$

Eve holds a system which makes a purification of ρ_2:

$$|\chi\rangle_{ABE} = \sqrt{\lambda_1}|\Phi^+\rangle_{AB}|00\rangle_E + \sqrt{\lambda_2}|\Phi^-\rangle_{AB}|01\rangle_E + \sqrt{\lambda_3}|\Psi^+\rangle_{AB}|10\rangle_E + \sqrt{\lambda_4}|\Psi^-\rangle_{AB}|11\rangle_E. \tag{A2}$$

Eve's and Bob's partial states are, respectively,

$$\rho_E = \mathrm{diag}(\lambda_1,\lambda_2,\lambda_3,\lambda_4), \quad \rho_B = \frac{1}{2}\mathbb{1} \tag{A3}$$

whence $S(\rho_E) = -\Sigma_i \lambda_i \ln \lambda_i$ and $S(\rho_B)=1$.

When Alice has measured $|0\rangle$ or $|1\rangle$, Bob and Eve share one of the states

$$|\chi_0\rangle_{BE} \propto {}_A\langle 0|\chi\rangle_{ABE} = |0\rangle_B(\sqrt{\lambda_1}|00\rangle + \sqrt{\lambda_2}|01\rangle)_E + |1\rangle_B(\sqrt{\lambda_3}|10\rangle + \sqrt{\lambda_4}|11\rangle)_E, \tag{A4}$$

$$|\chi_1\rangle_{BE} \propto {}_A\langle 1|\chi\rangle_{ABE} = |0\rangle_B(\sqrt{\lambda_3}|10\rangle - \sqrt{\lambda_4}|11\rangle)_E + |1\rangle_B(\sqrt{\lambda_1}|00\rangle - \sqrt{\lambda_2}|01\rangle)_E, \tag{A5}$$

which give in the computational bases

$$\rho_E^0 = \begin{pmatrix} \lambda_1 & \sqrt{\lambda_1\lambda_2} & & \\ \sqrt{\lambda_1\lambda_2} & \lambda_2 & & \\ & & \lambda_3 & \sqrt{\lambda_3\lambda_4} \\ & & \sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix}, \tag{A6}$$

$$\rho_E^1 = \begin{pmatrix} \lambda_1 & -\sqrt{\lambda_1\lambda_2} & & \\ -\sqrt{\lambda_1\lambda_2} & \lambda_2 & & \\ & & \lambda_3 & -\sqrt{\lambda_3\lambda_4} \\ & & -\sqrt{\lambda_3\lambda_4} & \lambda_4 \end{pmatrix}, \tag{A7}$$

and

$$\rho_B^0 = \begin{pmatrix} \lambda_1+\lambda_2 & \\ & \lambda_3+\lambda_4 \end{pmatrix} = \begin{pmatrix} 1-Q & \\ & Q \end{pmatrix}, \tag{A8}$$

$$\rho_B^1 = \begin{pmatrix} \lambda_3+\lambda_4 & \\ & \lambda_1+\lambda_2 \end{pmatrix} = \begin{pmatrix} Q & \\ & 1-Q \end{pmatrix}. \tag{A9}$$

If $q=p_{A'\neq A}$ denotes the probability for Alice to flip her bit (preprocessing), the state of Alice and Eve is

$$\rho_{A'E} = \frac{1}{2}[((1-q)|0\rangle\langle 0| + q|1\rangle\langle 1|) \otimes \rho_E^0 + (q|0\rangle\langle 0| + (1-q)|1\rangle \times \langle 1|) \otimes \rho_E^1] = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_E^0 + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_E^1, \tag{A10}$$

where $\sigma_E^0=(1-q)\rho_E^0+q\rho_E^1$ and $\sigma_E^1=q\rho_E^0+(1-q)\rho_E^1$. Then,

$$S(\rho_{A'E}) = 1 + \frac{1}{2}S(\sigma_E^0) + \frac{1}{2}S(\sigma_E^1). \tag{A11}$$

With similar notations,

$$S(\rho_{A'B}) = 1 + \frac{1}{2}S(\sigma_B^0) + \frac{1}{2}S(\sigma_B^1). \tag{A12}$$

Finally,

$$R(\sigma_{A'BE}) = S(\rho_{A'E}) - S(\rho_E) - [S(\rho_{A'B}) - S(\rho_B)] = \frac{1}{2}[S(\sigma_E^0) + S(\sigma_E^1) - S(\sigma_B^0) - S(\sigma_B^1)] + 1 - S(\rho_E). \tag{A13}$$

This is the function which must be optimized over the λ_i compatible with the constraints (which define the protocol) and over the bitwise preprocessing:

$$r_1 = \sup_{q\in[0,0.5[} \inf_{\lambda' s} R(\sigma_{A'BE}). \tag{A14}$$

APPENDIX B

In the main text, we have computed the lower bound for the SARG04 protocol implemented with single-photon sources. One might ask what happens if the SARG04 protocol is modified if only two "opposite" sifting sets, say $\mathcal{S}_{++}$ and $\mathcal{S}_{--}$, are used instead of all the four.

The interest in the two-set protocol is a practical one. The sifting of the four-set protocol requires Alice to use a random bit for each item (for instance, if she has sent $|+z\rangle$, she must still decide whether to announce $\mathcal{S}_{++}$ or $\mathcal{S}_{+-}$). In a true implementation, the production of local random bits is one of the most time-consuming tasks. In the two-set protocol, an easier sifting procedure can be implemented: for instance, Bob reveals whether he has got a detection in the + or in the − detector. If Alice has sent a state in $\mathcal{S}_{++}(\mathcal{S}_{--})$, the detection in −(+) is conclusive: then, Alice tells Bob whether the bit is accepted or discarded. Obviously, no random bit is needed for such a sifting.

The intuition based on incoherent attacks suggests that the two- and the four-set protocols are equivalent: after all, Eve has to distinguish among the same four states before sifting takes place; and after sifting, her knowledge is the same in both protocols. While this equivalence probably holds indeed, the lower bound computed with our method is slightly less favorable in the two-set case. In fact, one finds after some algebra

$$\lambda_1 = \tilde{C}\langle\Phi^+|\rho_0|\Phi^+\rangle,$$

$$\lambda_2 = \tilde{C}[\langle\Psi^-|\rho_0|\Psi^-\rangle + 2\langle\chi^-|\rho_0|\chi^-\rangle],$$

$$\lambda_3 = \tilde{C}\langle\chi^+|\rho_0|\chi^+\rangle,$$

$$\lambda_4 = \tilde{C}[2\langle\Psi^-|\rho_0|\Psi^-\rangle + \langle\chi^-|\rho_0|\chi^-\rangle] \tag{B1}$$

where $|\chi^\pm\rangle=(1/\sqrt{2})(|\Phi^-\rangle\pm|\Psi^+\rangle)$ and $\tilde{C}=C/2$ with C defined in Eq. (9). Note that C is not the same as in Eq. (13); also, the structure of Eq. (13) would be recovered if we replaced the states $|\chi^\pm\rangle$ by the incoherent mixture $\frac{1}{2}|\Phi^-\rangle\langle\Phi^-| + \frac{1}{2}|\Psi^+\rangle \times \langle\Psi^+|$.

The constraints imposed by (B1) are less tight than those imposed by Eq. (13): actually, λ_1 and λ_3 are unconstrained but for Eq. (12). For λ_2 and λ_4, it is easy to see that $\lambda_2 - 2\lambda_4 = -3\tilde{C}\langle\Psi^-|\rho_0|\Psi^-\rangle \leqslant 0$ and symmetrically $\lambda_4 - 2\lambda_2 = -3\tilde{C}\langle\chi^-|\rho_0|\chi^-\rangle \leqslant 0$, whence

$$\frac{\lambda_2}{2} \leqslant \lambda_4 \leqslant \min(2\lambda_2, Q). \tag{B2}$$

Using this constraint, the optimization of r_1 gives a lower bound $Q \leqslant 8.90\%$ ($Q \leqslant 7.74\%$ if we had neglected preprocessing). Thus, the lower bound obtained for the two-set protocol is worse than the one found for the original four-set protocol. This is not a conclusive proof of inequivalence, in so far as we do not know whether each bound is tight.

APPENDIX C

The calculations leading to the expression of Eve's information (27) plotted in Fig. 1 can be done analytically up to some extent. The three eigenvalues of M_A are $\lambda_\pm = \pm 2\sqrt{D(2-3D)}/(1+2D)$ and $\lambda_0=0$, whence the natural labeling for the index e of the main text is

$$e \in \{0, +, -\}. \tag{C1}$$

In the basis where $|00\rangle \equiv \hat{e}_1$, $|01\rangle \equiv \hat{e}_2$, and $|10\rangle \equiv \hat{e}_3$, and with $\alpha_\pm = (\sqrt{D} \pm \sqrt{2-3D})/\sqrt{1-2D}$, the corresponding normalized eigenvectors are

$$|m_\pm\rangle = \frac{1}{1+\frac{1}{2}\alpha_\pm^2}\begin{pmatrix} \alpha_\pm \\ 1 \\ -\frac{1}{2}\alpha_\pm^2 \end{pmatrix},$$

$$|m_0\rangle = \frac{1}{\sqrt{2-3D}}\begin{pmatrix} \sqrt{D} \\ \sqrt{1-2D} \\ \sqrt{1-2D} \end{pmatrix}.$$

One sees that the calculation is heavy, and since the function (27) is not algebraic, ultimately one must make use of the computer; that is why these analytical results are of limited utility. Still, we can use them to obtain more insight on Helstrom's strategy. In fact, the general calculation scheme described in the main text can be described as follows.

(1) When Eve finds the positive eigenvalue λ_+, she guesses Alice's bit to be 0 (see the definition of M_A); when she finds the negative eigenvalue λ_-, she guesses Alice's bit to be 1. These two cases appear with the same probability ($p_{E=+}=p_{E=-}$) and Eve's guess is correct with the same probability $p_{guess}=p_{A=0|E=+}=p_{A=1|E=-}$.

(2) With probability $p_{E=0}$, Eve finds the eigenvalue λ_0, from which she cannot draw any conclusion. Indeed, it is the case: $\langle m_0|M_A|m_0\rangle=0$ implies $\langle m_0|\rho_E^{A=0}|m_0\rangle=\langle m_0|\rho_E^{A=1}|m_0\rangle$, whence $p_{E=0|A=0}=p_{E=0|A=1}=p_{E=0}$. Consequently, using Bayes' rule (28), we find $p_{A=0|E=0}=\frac{1}{2}$.

Following these remarks, Eve's information (27) can be rewritten as

$$I(A:E)=(1-p_{E=0})[1-h(p_{guess})]. \tag{C2}$$

APPENDIX D

In this appendix we show how the five constraints (69)–(73) reduce to the three conditions (74)–(76), as claimed in Sec. IV C 3.

Using the expression (43) for $p_0(n)$, we can rewrite the first constraint (69) as

$$\sum_n p_{BE}(n)(1-\eta)^n \equiv \sum_n p_B(n)(1-\eta)^n \tag{D1}$$

which is Eq. (74). By replacing the expression (46) for $p_{acc}^x(n)$ into Eq. (70), we find that this second constraint is satisfied by adding to Eq. (D1) the condition

$$\sum_n p_{BE}(n)(1-\eta/2)^n \equiv \sum_n p_B(n)(1-\eta/2)^n \tag{D2}$$

which is Eq. (75). Finally, because of Eq. (54), the third constraint (71) is automatically satisfied if the first two are. In summary, the first three constraints (69)–(71) are equivalent to the two conditions (74) and (75).

Consider now constraint (72). From Eq. (44), we have

$$p_{acc}^z(n,1)=p_d(1-p_d)(1-\eta)^n \quad \text{for all } n, \tag{D3}$$

$$p_{acc}^z(1,\tilde{V})=(1-p_d)\eta\tilde{D}+p_{acc}^z(1,1), \tag{D4}$$

whence the left-hand side (LHS) of Eq. (72), up to the factor $(1-p_d)$, reads

$$p_A(1)p_{\mathbf{U}}(1)\eta\tilde{D}+p_d\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1).$$

Using again Eq. (44), the RHS of Eq. (72), up to the factor $(1-p_d)$, reads

$$\sum_n p_B(n)[(1-F\eta)^n-(1-\eta)^n]+p_d\vec{\mathcal{P}}_B\cdot\vec{\Gamma}(1).$$

Since we have already imposed (74), equality of these two expressions is obtained if and only if (76) holds.

Finally, we have to discuss Eq. (73). From Eq. (53) we note that $p_2^z(1,V)$ is actually independent of V because this parameter appears in the combination $F+D=1$. In particular, $p_2^z(1,\tilde{V})=p_2^z(1,1)$ whence the LHS of Eq. (73) becomes

$$1-(1-p_d)[1+\vec{\mathcal{P}}_{B|E}\cdot\vec{\Gamma}(1)]+(1-p_d)^2\vec{\mathcal{P}}_{BE}\cdot\vec{\Gamma}(1),$$

which is entirely determined by Eq. (74) and is independent of $\tilde{V}$. However, the RHS of Eq. (73) *does* depend on V. Consequently, for the strategies that we have considered, constraint (73) is automatically satisfied by Eq. (74) if $V=1$ and cannot be satisfied exactly if $V<1$. In this last case, however, the discrepancy is rather small. In fact

$$p_2^z(n,V)=p_2^z(n,1)+n\eta D[1-(1-\eta)^{n-1}]+O(\eta D)^2$$

and the leading term in the discrepancy will be the one associated with $n=2$, that is,

$$p_{BE}(2)|p_2^z(2,V)-p_2^z(2,1)|\approx p_{BE}(2)2\eta^2 D. \tag{D5}$$

Specifically, for a Poissonian source the discrepancy is $|C_2^z(V)-C_2^z(1)|$, i.e., using Eq. (55)

$$[p(0|x)+1]-[p(0|xF)+p(0|xD)]=FDx^2+O(x^3)$$

with $x=\mu t\eta$, consistent with Eq. (D5) using Eq. (81). Since typical values are $\eta\approx 0.1$ and $D\lesssim 1\%$, this discrepancy is small. Thus, we can assume that Eq. (73) is satisfied as well, and we have proved that the constraints (69)–(73) reduce to (74)–(76)claimed.

APPENDIX E

In this appendix, we rederive the results on the optimal parameters for Eve's attack that have been obtained by numerical optimization (see sec. IV D 2. As we said there, we work in a more restricted setting, by neglecting the possibility of double counts: Eve forwards always one photon (if any) to Bob, that is, $s(m|n)=r(m|n)=\delta_{m,1}$ for all n. We also neglect Alice's preprocessing, which makes very minor modifications in the end (i.e., $q=0$). However, we do not assume that Alice's source is Poissonian.

We study the constraints first. Since Eve forwards only one photon to Bob, $p_{B|E}(n>1)=0$ and $p_{B|E}(0)=1-p_{B|E}(1)$. Constraint (75) cannot be satisfied, but at long distance this is supposed to be a very small contribution. Constraint (74) reads $p_{B|E}(1)=C$ where $C=[\vec{\mathcal{P}}_B\cdot\vec{\Gamma}(1)-1]/\eta$ depends only on parameters that are outside Eve's control; and

$$p_{BE}(1)=p_A(1)p_{\mathbf{U}}(1)+p_A(2)p_{\mathbf{S}}(2)+\sum_{n\geq 3}p_A(n)[p_{\mathbf{S}}(n)+p_{\mathbf{I}}(n)p_{OK}(n)].$$

The constraint (76) is of the form $p_A(1)p_{\mathbf{U}}(1)=(1/\tilde{D})C'$ where $C'=\vec{\mathcal{P}}_B\cdot[\vec{\Gamma}(F)-\vec{\Gamma}(1)]/\eta$ depends only on parameters that are outside Eve's control. Using these two constraints, we can express $p_A(1)p_{\mathbf{U}}(1)$ and $p_A(2)p_{\mathbf{S}}(2)$ as a function of the other parameters. The quantity that Eve must optimize [Eq. (66)] reads now

$$I(A:E) = p_A(1)p_{\mathbf{U}}(1)I_{\mathbf{U}}(\tilde{D})\tilde{\xi} + p_A(2)p_{\mathbf{S}}(2)I_{\mathbf{S}}(1)\xi + \sum_{n\geqslant 3} p_A(n) \times [p_{\mathbf{S}}(n)I_{\mathbf{S}}(n-1) + p_{\mathbf{I}}(n)p_{OK}(n)]\xi = \xi\Big(C' K(\tilde{D}) + \sum_{n\geqslant 3} p_A(n)p_{\mathbf{S}}(n)\mathcal{L}(n) + C\, I_{\mathbf{S}}(1) + \sum_{n\geqslant 3} p_A(n)p_{OK}(n) \times [1 - I_{\mathbf{S}}(1)]\Big) \quad \text{(E1)}$$

where we have defined $\tilde{\xi}=p_{acc}(1,\tilde{V})$, $\xi=p_{acc}(1,1)$ and

$$K(\tilde{D}) = \frac{1}{\tilde{D}}\left(\frac{\tilde{\xi}}{\xi} I_{\mathbf{U}}(\tilde{D}) - I_{\mathbf{S}}(1) \right), \quad \text{(E2)}$$

$$\mathcal{L}(n) = I_{\mathbf{S}}(n-1) - I_{\mathbf{S}}(1) - p_{OK}(n)[1 - I_{\mathbf{S}}(1)]. \quad \text{(E3)}$$

In writing Eq. (E1) we made explicit use of the constraints and of $p_{\mathbf{I}}(n)=1-p_{\mathbf{S}}(n)$ for $n\geqslant 3$. The problem of finding Eve's best attack is thus reduced to the study of $K(\tilde{D})$ and of $\mathcal{L}(n)$ for all n. These functions are independent of the statistics $p_A(n)$ of Alice's source.

The function $K(\tilde{D})$ depends only on one free parameter $\tilde{D}$ and is independent of the distance. Therefore, Eve will maximize her information by introducing always the same amount of error $\tilde{D}_0$, the one that maximizes $K(\tilde{D})$. If we insert $\eta=0.1$ and $p_d=10^{-5}$ in $\tilde{\xi}/\xi$, the maximum is obtained for $\tilde{D}_0\simeq 0.191$, which is exactly the value found by the numerical optimization.

The study of the $\mathcal{L}(n)$ is just as easy. In fact, by using the explicit expressions (57) for $I_{\mathbf{S}}(n)$ and (58) for $p_{OK}(n)$, one sees that $\mathcal{L}(3)\simeq -0.054$ while $\mathcal{L}(n)>0$ for $n\geqslant 4$. Thence Eve's information (E1) is maximized by the choice $p_S(3)=0$ and $p_S(n\geqslant 4)=1$: Eve performs always the **I** attack when $n=3$ and the **S** attack when $n\geqslant 4$. Again, this is exactly what has been found in the numerical optimization.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004); see references therein for previous works.

[3] We do not consider here QKD with continuous variables, which uses homodyne measurements instead of photon counting. A protocol with photon counting which needs intrinsically a weak laser source has been proposed recently: N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, e-print quant-ph/0411022.

[4] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995);H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[5] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000);G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003);X.-B. Wang, *ibid.* **94**, 230503 (2005);H.-K. Lo, X. Ma, and K. Chen, *ibid.* **94**, 230504 (2005).

[7] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[8] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).

[9] K. Tamaki and H.-K. Lo, e-print quant-ph/0412035.

[10] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[11] B. Kraus, N. Gisin, and R. Renner, e-print quant-ph/0410215.

[12] R. Renner, N. Gisin, and B. Kraus, e-print quant-ph/0502064.

[13] R. B. Griffiths and C.-S. Niu, Phys. Rev. A **56**, 1173 (1997);D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, *ibid.* **62**, 012302 (2000);N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).

[14] Here we study only individual PNS attacks, as in all the works devoted to PNS attacks we are aware of. In principle, one can define a general PNS attack, in which Eve starts by counting the number of photons in each pulse, but may then adopt a coherent strategy.

[15] A. Niederberger, V. Scarani, and N. Gisin, Phys. Rev. A **71**, 042316 (2005).

[16] For a BB84-like encoding, one can modify the protocol in order to use almost always one basis, and use the other just for monitoring the presence of the eavesdropper. The analog here would consist in Alice sending almost always either $|+z\rangle$ or $|+x\rangle$: this makes SARG04 similar to the Bennett 1992 protocol [C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)], where the monitoring is not made by a strong pulse but by some decoy states.

[17] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[18] In fact, any definition of Bob's operators $B_{\sigma\omega}$ that would lead to Eq. (6)is valid. The one we have chosen is such that $A_{\sigma\omega}\otimes B_{\sigma\omega}|\Phi^+\rangle=(1/2)|\Phi^+\rangle$ (up to a global phase): if the state arrives unperturbed at Alice and Bob, the sifting operators simply introduce losses (the factor 1/2, which leads to the expected sifting rate of SARG04).

[19] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978).

[20] In the first version of their work [9], still available on the ArXiV, Tamaki and Lo found a worse bound as follows: they found $e^1_{phase}=(3/2)e^1_{bit}$, where e^1_{bit} is the same as our Q. This is plugged into $1-h(e^1_{bit})-h(e^1_{phase})\geqslant 0$, h being binary entropy, and gives $e^1_{bit}\lesssim 8.90\%$.

[21] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[22] One can easily translate the lower and upper bounds for Q in terms of V, but this translation is not really meaningful: the bounds have been obtained, as they should be, without any hypothesis on Eve's attack; while a visibility can be defined

only if we assume that Eve's attack is such that the channel Alice-Bob becomes depolarizing.

[23] For a Poissonian distribution $\Sigma_n p(n|\nu)(1-\xi)^n = e^{-\nu}\Sigma_n [\nu(1-\xi)^n/n!] = e^{-\nu}e^{\nu(1-\xi)} = e^{-\nu\xi} = p(0|\nu\xi)$.

[24] To be precise, one should replace $I(A':E)$ with $I(B':E)$, because $I(A:E) > I(B:E)$ in the presence of imperfect detectors. The reason is the following. Eve interacts with photons sent by Alice, and forwards some to Bob; but she cannot ensure that Bob detects a photon: Bob may have missed the photon but have got a dark count. Now, since Eve forwards photons to Bob on a lossless line, the correction to her information is of the order of $1-h(x)$ with $x = p_d/\eta \simeq 10^{-4}$. Therefore, we neglect this correction.

[25] If Eve could modify p_d, she could take advantage of these errors as well to obtain information, but dark counts can not be modified unless by changing the detector—and if Eve has access to Bob's laboratory, it is certainly easier to put an antenna in the computer. The case of η is different, because there is a way for Eve to increase η from outside: in an intercept-resend kind of strategy, Eve may resend a much stronger pulse, thus forcing the detection. However, this procedure would significantly increase the double-click rate. Our assumption, that η is not modified, is thus consistent with the requirement that double-click rates should be monitored.

[26] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000)

[27] Actually, we could imagine that Eve applies this attack for various disturbances $\tilde{D}$, according to some probability law $p(\tilde{D})$ [in which case, if $p(0) \neq 0$, she would still sometimes apply the **L** strategy]. However, due to the convexity of the function $I_{\mathbf{U}}(\tilde{D})$, she gets more information if she always applies the attack for the same disturbance $\tilde{D}$.

[28] Note that we do not consider here "realistic attacks" which depend on the details of the implementation, like the Trojan-horse or faked-state attacks: A. Vakhitov, V. Makarov and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001);V. Makarov, and D. R. Hjelme, *ibid.* **52**, 691 (2005).

[29] The effect of $q > 0$ on BB84 can easily be estimated referring to Sec. V of Ref. [15]. Letus consider just the case $V=1$. Eve's information becomes $I(A:E) = (1/4)\eta\mu^2[1-h(q)]$; in Bob's information, one has to replace Q with $Q' = Q(1-q)+q(1-Q)$. Two regimes can be distinguished. (I) At relatively short distance, $\mu t \eta \gg p_d$ whence $Q \approx 0$ and $Q' \approx q$; therefore Bob's information is reduced by a factor $1-h(q)$, exactly like Eve's. So $q \neq 0$ does not help, and would actually decrease the secret key rate. (II) Close to the limiting distance, one can repeat the argument of Sec. V D of Ref. [15]: if $Q = 1/2-\varepsilon$ then $Q' = 1/2-\varepsilon'$ with $\varepsilon' = \varepsilon(1-2q)$; and $I(A:E)$ is still the same. Thus for any given q, the condition for the limiting distance is found to be $t_{lim}(q) = t_{lim}(q=0)f(q)$ with $f(q) = \sqrt{1-h(q)/(1-2q)^2}$. The minimum of f is attained for $q = 1/2$, and it can be calculated analytically by setting $q = 1/2-\delta$ and letting $\delta \to 0$. One finds $f(1/2) = \sqrt{1/2 \ln 2}$. This small decrease in t_{lim} corresponds to an increase in the distance of ~ 3 km.

[30] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).