Higher-security thresholds for quantum key distribution by improved analysis of dark counts

J.-C. Boileau,[1,2] J. Batuwantudawe,[1] and R. Laflamme[1,2]
[1]*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
[2]*Perimeter Institute for Theoretical Physics, 35 King Street North, Waterloo, Ontario N2J 2W9, Canada*
(Received 28 June 2005; published 16 September 2005)

We discuss the potential of quantum key distribution (QKD) for long-distance communication by proposing an analysis of the errors caused by dark counts. We give sufficient conditions for a considerable improvement of the key generation rates and the security thresholds of well-known QKD protocols such as the Bennett-Brassard 1984, Phoenix-Barnett-Chefles 2000, and six-state protocols. This analysis is applicable to other QKD protocols like the Bennett 1992 protocol. We examine two scenarios: a sender using a perfect single-photon source and a sender using a Poissonian source.

DOI: 10.1103/PhysRevA.72.032321 PACS number(s): 03.67.Dd

The goal of quantum key distribution (QKD) is to extend a shared secret key for use as a one-time pad to encode classical messages. The advantage of QKD is that its security is based on the laws of quantum mechanics and not on the unproven complexity of a mathematical problem as in classical cryptography. These last few years, many encouraging experiments demonstrated QKD, some spanning more than 100 km through optical fibers [1]. The main source of errors is usually due to dark counts from the detectors. A dark count is when a detector fires independently (or in the absence) of a qubit state encoded by the sender, Alice. If qubit losses are considerable, then the receiver, Bob, will receive many empty pulses, and dark counts from his detectors will induce a high error rate.

In this paper, for simplicity, we refer specifically only to four different QKD protocols: the Bennett 1992 (B92), Phoenix-Barnett-Chefles 2000 (PBC00), Bennett-Brassard 1984 (BB84), and six-state protocols, which are two-, three-, four-, and six-state protocols, respectively [2–5]. In the B92 protocol, Alice encodes random bits using two nonorthogonal states—say, $|\psi_1\rangle$ and $|\psi_2\rangle$—and sends them to Bob. He makes the measurement corresponding to the positive operator-valued measure (POVM) $\{\alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|, \mathbb{1} - \alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1| - \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|\}$, where $|\bar{\psi}_j\rangle$ is orthogonal to $|\psi_j\rangle$ and α equals $1/(1+|\langle\psi_1|\psi_2\rangle|)$. Bob's measurement either determines which state Alice did not send (from which Bob can deduce the encoded bit) or is inconclusive. The PBC00 protocol is similar to the B92 protocol but uses three nonorthogonal states—say, $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$—that form an equilateral triangle in the *X-Z* plane of the Bloch sphere. She encodes her random bits using random bases from either $\{|\psi_1\rangle, |\psi_2\rangle\}$, $\{|\psi_2\rangle, |\psi_3\rangle\}$, or $\{|\psi_3\rangle, |\psi_1\rangle\}$. Bob performs the POVM $\{\frac{2}{3}|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \frac{2}{3}|\bar{\psi}_2\rangle\langle\bar{\psi}_2|, \frac{2}{3}\langle\bar{\psi}_3\rangle\langle\bar{\psi}_3|\}$. After Bob measures all of the qubits, Alice declares publicly which basis she used for each. By deduction, Bob can sometimes retrieve Alice's state. Alice and Bob discard the other results. It can be shown that, neglecting the qubit losses, the rate of conclusive results is $1/(2-e_x)$ where e_x is the bit error rate. A *conclusive* result corresponds to any pair of qubits not discarded by Alice and Bob.

To implement the BB84 protocol, Alice encodes a random bit in either $\{|0\rangle, |1\rangle\}$ or its conjugate basis $\{|+\rangle, |-\rangle\}$. For each qubit, Bob randomly measures in one of these bases. They only keep results for which they used the same basis. The six-state protocol is identical to the BB84 protocol except that Alice and Bob choose from three different bases: $\{|0\rangle, |1\rangle\}, \{|+\rangle, |-\rangle\}$, and $\{(1/\sqrt{2})(|0\rangle + i|1\rangle), (1/\sqrt{2})(|0\rangle - i|1\rangle)\}$. We can modify the BB84 and six-state protocols by choosing bases with nonequal probabilities, increasing the chance of agreement [6]. The rate of results for which identical bases are used converges asymptotically to 1. Below, we calculate the key generation rates of the BB84 and six-state protocols using this asymptotic result.

Mayers [7] produced the first unconditional security proof of the BB84 protocol. Shor and Preskill [8] proposed a simpler proof based on ideas from Lo and Chau [9]. Their security proof has been generalized to other protocols including the B92, PBC00, and six-state protocols [10–13]. We improve the secret key generation rate of these QKD protocols by proposing a slight modification of these proofs. Our main idea is based on a variation of a theorem proved in Ref. [14]. We assume that an eavesdropper, Eve, can perform any attack consistent with quantum mechanics, but cannot get any information about Alice's or Bob's laboratories or control their apparatus. We discuss later how realistic these assumptions are and how it is possible to slightly relax them. We study two cases: one where Alice's source can create a single photon on demand and another where it follows a Poisson distribution. For simplicity, we give details only about Shor and Preskill's security proof of the BB84 protocol and not other protocols.

At the end of this paper, we compare the updated error rate thresholds and key generation rates of the BB84, PBC00, and six-state protocols with previous results. The same arguments could improve other QKD protocols, including the B92 protocol. However, the B92 protocol's phase estimation bound depends on qubit losses in the channel and the number of inconclusive results, complicating the analysis. Since our goal is to describe a general technique to improve security thresholds, we only treat the simpler cases as examples.

The Shor-Preskill proof first shows the security of an entanglement distillation protocol (EDP) for QKD and subse-

quently reduces the EDP to the BB84 protocol. For convenience, we define $|\Phi^{\pm}\rangle=(1/\sqrt{2})(|0\rangle|0\rangle\pm|1\rangle|1\rangle)$ and $|\Psi^{\pm}\rangle=(1/\sqrt{2})(|0\rangle|1\rangle\pm|1\rangle|0\rangle)$.

The structure of the *EDP that can be reduced to the BB84 protocol* in Shor and Preskill's proof is as follows.

(i) Alice creates n pairs of the form $|\Phi^{+}\rangle$ and sends the second half of each pair to Bob after randomly applying the identity or the Hadamard gate on it.

(ii) After Bob confirms that he has received all of Alice's states, Alice publicly declares the random rotation that she used on each qubit. Bob undoes the transformations on the corresponding qubits.

(iii) With no eavesdropping or channel noise, Alice and Bob will share n perfect pairs of the form $|\Phi^{+}\rangle$. They can now measure their qubits in the same basis to share a secret key. However, noise and eavesdropping induce errors. If the bit and phase error rates are low enough, then error correction can be applied to obtain m perfect pairs of the form $|\Phi^{+}\rangle$ where $m\leqslant n$.

(iv) Alice and Bob can estimate the bit error rate by comparing bit measurements from a sample of pairs, called test bits. A bit (or X) error on a pair occurs when Alice and Bob share either $|\Psi^{+}\rangle$ or $|\Psi^{-}\rangle$. A phase (or Z) error corresponds to $|\Phi^{-}\rangle$ or $|\Psi^{-}\rangle$. A Y error corresponds to $|\Phi^{-}\rangle$ or $|\Psi^{+}\rangle$. Y error estimation could provide information about the correlation between bit and phase errors. Because Alice randomly applies the identity or Hadamard gate, it can be shown that the bit error rate e_x and the phase error rate e_z are approximately equal, independent of channel noise and Eve's strategy. In the BB84 protocol, Alice and Bob have no information about Y errors.

(v) Depending on the bit error rate measured on the test bits, Alice and Bob apply error correction on the other pairs. If we suppose one-way error correction using CSS codes [15], a lower bound for generation rate m/n for the perfect pairs is given asymptotically by

$$S=p_c[1-H(e_x,e_z)], \tag{1}$$

where H is the Shannon entropy $[H(e_x,e_z)=H(e_x)+H(e_z|e_x)$ is the entropy of the bit-phase error pattern] and p_c is the rate of conclusive results. For simplicity, we assume that the proportion of test bits is negligible. □

Shor and Preskill showed that this EDP, and thus the BB84 protocol, were unconditionally secure with a key generation rate given by Eq. (1). Since $H(e_x)$ is asymptotically the fraction of bits sacrificed for bit error correction, it implies that $H(e_z|e_x)$ is an upper bound on the fraction of information that Eve has about the key after bit error correction. A consequence is that privacy amplification, as introduced in Ref. [16], can be used to simplify the post-processing of the QKD protocol. As shown in Ref. [17], privacy amplification can generate a secret key by sacrificing a number of bits asymptotically proportional to Eve's information.

The reduction of the EDP to the BB84 protocol assumes that Alice uses a source which emits a single photon on demand. In a more realistic situation, Alice's source would emit a photon pulse following a Poisson distribution. Unfortunately, when Alice sends two or more photons containing the same quantum information at the same time, Eve can measure one to gain information about the key without detection. Accounting for this attack (but assuming Eve has no information about the random phase of the signal emitted by a coherent light source), a more general equation of the secret key generation rate, combining results from Refs. [14,12], and using the improvement suggested in Ref. [18], is given asymptotically by

$$S=p_c[\omega_0+\omega_1-H(e_x)-\omega_1H(e_z^1|e_x)], \tag{2}$$

where ω_1 is the fraction of the conclusive results corresponding to single-photon pulses, ω_0 is the fraction of the conclusive results corresponding to empty pulses (the presence of background noise, for example), and $e_x^1(e_z^1)$ is the bit (phase) error rate restricted to conclusive results from single-photon pulses. $e_x(e_z)$ is still the bit (phase) error rate over all conclusive results. If Alice has a source that emits a single photon on demand, then $\omega_0=0$, $\omega_1=1$, $e_j^1=e_j$ for $j\in\{x,y,z\}$, and $S=p_c[1-H(e_x,e_z)]$ as expected.

To prove Eq. (2), it was argued that since Alice and Bob want an identical key and cannot differentiate multiphoton from single-photon pulses, they must correct all bit errors, asymptotically losing a fraction $H(e_x)$ of the results in the process. To apply privacy amplification on the remaining bits and obtain a secret key, Alice and Bob must upper bound Eve's information. If we assume that the phase of the signal is random,[1] there is no coherence between states with different photon numbers. Thus, we can categorize each bit of the resulting key as being associated with an empty, single-photon, or multiphoton pulse. Assuming the worst case, Eve has full information about the results associated with multiphoton pulses. On the other hand, she has no information about Alice's bits corresponding to empty pulses. By the Shor-Preskill arguments discussed earlier, the fraction of information that Eve could extract from the results corresponding to single-photon pulses is upper bounded by $H(e_z^1|e_x)$. Consequently, Eve's information about Alice's remaining key is upper bounded by $(1-\omega_0-\omega_1)+\omega_1H(e_z^1|e_x)$. After privacy amplification, Eve has no information about Alice's key. The same is true of Bob's key since it is identical to Alice's. Therefore, the secret key generation rate is given by Eq. (2).

Similarly, since the Shor-Preskill proof can be adapted to the B92, PBC00, and six-state protocols [10–12], these protocols can be shown unconditionally secure with a key generation rate given by Eq. (2).

The above argument does not differentiate between a single photon emitted by Alice that is successfully measured by Bob and a single photon that is lost in the channel (or taken by Eve) followed by a dark count measured by Bob. However, these cases may be analyzed separately. Consider the following four types of conclusive results.

(i) Successful measurement of a *qubit state* (physically

[1]Recently, it was shown that Eve could use extra information about the phase of the signal to her advantage [19], though the extent is unknown.

corresponding to a photon received from the channel) that originated from a single-photon pulse. Note that the qubit state could have been manipulated by Eve.

(ii) Successful measurement of a qubit state that originated from a multiphoton pulse.

(iii) Empty pulses from Alice followed by a successful measurement of a qubit state by Bob (i.e., Eve may send a qubit state to Bob even if Alice emits nothing).

(iv) Dark count events: Bob does not receive a qubit state, but one of his detectors fires.

The dark count events are independent of Alice's or Eve's actions. We define p_c^{emp}, p_c^{sq}, and p_c^{mq} as the rate of conclusive results corresponding to qubit states, received by Bob, associated with empty pulses, single-photon pulses, and multiphoton pulses, respectively. We define p_c^{dk} as the rate of conclusive results associated with dark counts. Note that

$$p_c = p_c^{emp} + p_c^{sq} + p_c^{mq} + p_c^{dk}. \tag{3}$$

We remark that the background noise has two different contributions: intrinsic and extrinsic. The intrinsic contribution is caused by elements from Bob's laboratory while the extrinsic contribution is from external sources. The Sun and backscattering light in the two-way QKD are examples of external sources of background noise. Based on our assumptions, Eve may control the external sources of background noise, but not the ones inside Bob's laboratory. Following our previous definitions, the only contribution to p_c^{dk} is intrinsic. Any external sources will contribute to p_c^{emp}, p_c^{sq}, and p_c^{mq} since they correspond to Bob receiving a qubit state from the channel. For convenience, in this paper, *dark counts* always refer to the intrinsic contribution of background noise. We assume for simplicity that dark counts are independent of other measurement results.

We now explain how it is possible to achieve a better bound for the secret key generation rate than Eq. (2). As before, a fraction $H(e_x)$ of the results are lost due to bit error correction. Assuming again that the phase of the signal is random from Eve's perspective, each bit of the resulting key corresponds to one of the four types of conclusive results described above. From previous arguments, Eve has a fraction $H(e_z^{sq}|e_x)$ of information about conclusive results from category (i) and, in the worst case scenario, full information about those from category (ii). e_x^{sq} and e_z^{sq} are defined as the bit and phase error rates on the conclusive results restricted to category (i). When Alice emits an empty pulse and it is followed by a successful measurement of a qubit state by Bob, we assume that the qubit state was created by Eve. A conservative assumption is that Eve has full information about Bob's results from category (iii).[2] Supposing dark count rates are the same in all detectors and independent of Eve and other measurement results, Bob's results from category (iv) are completely random and Eve has no information about them.[3] Consequently, the fraction of information that Eve has on Bob's key after bit error correction is upper bounded by $(1/p_c)[p_c^{emp}+p_c^{mq}+p_c^{sq}H(e_z^{sq}|e_x)]$. Therefore, the secret key generation rate is lower bounded by

$$S_b = p_c^{sq} + p_c^{dk} - p_c H(e_x) - p_c^{sq} H(e_z^{sq}|e_x). \tag{4}$$

We emphasize that it is not necessary for Alice and Bob to know which events correspond to each class of conclusive results.

In the derivation of Eq. (4), we bounded Eve's information about Bob's key. However, we could have instead bounded Eve's information about Alice's key. In this case, Eve has no information about the bit chosen by Alice when she sends a vacuum states. But she could have some information about Alice's portion of the key corresponding to dark counts (unless Alice sent an empty pulse). Using similar arguments, we obtain

$$S_a = p_c^{sq} + p_c \omega_0 - p_c H(e_x) - p_c^{sq} H(e_z^{sq}|e_x). \tag{5}$$

Combining Eqs. (4) and (5), we obtain a new lower bound for the secret key generation rate,

$$S = \max[S_a, S_b]. \tag{6}$$

TABLE I. Bit error rate thresholds for the BB84, PBC00, and six-state protocols using a single-photon source and assuming fixed values of e_x^{sq}, which is the bit error rate of the results not associated with dark counts.

	$e_x^{sq}=0$	$e_x^{sq}=0.01$	$e_x^{sq}=0.1$
PBC00	50%	43%	insecure
BB84	50%	44%	13%
Six-state protocol	50%	46%	19%

[2]In the case of the B92 protocol, it is easy to show that this assumption is necessary, but it might be too strict for other protocols like the PBC00, BB84, and six-state protocols.

[3]For simplicity, we suppose that the dark count rates are uniform over all detectors and that they are independent of other measurement results. If dark count rates differ from detectors, we suggest two options. In one, Bob uses a random transformation to switch the role of the detectors in the measurement. For example, in the BB84 protocol, Bob could apply, at random, an extra Y operation on the received qubits to switch the role of the detectors when measuring in the $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ bases. A second option is to bound Eve's information from an estimate of the probability that a detector fires relative to the others in the case of a dark count. Assuming dark counts are independent of other measurement results, in the BB84 and six-state protocols, with only two detectors, Eve's information is bounded by $1-H(q)$ where q is the probability that the first detector fires in the case of a dark count. It is interesting to note that if Eve has some control over the probability q and could change it from one dark count event to another, then, by entropic concavity, Eve's information is bounded by $1-H(q_{worst}^{ave})$, where q_{worst}^{ave} is the worst estimate of the average of q. Determining the value of q_{worst}^{ave} can be very hard, but it is related to the level of confidence that Alice and Bob have on their ability to counter or detect Eve if she tries to change the properties of the detectors. Similarly, if dark counts are correlated to other measurement results, we can upper bound Eve's information with restrictions on the correlations.

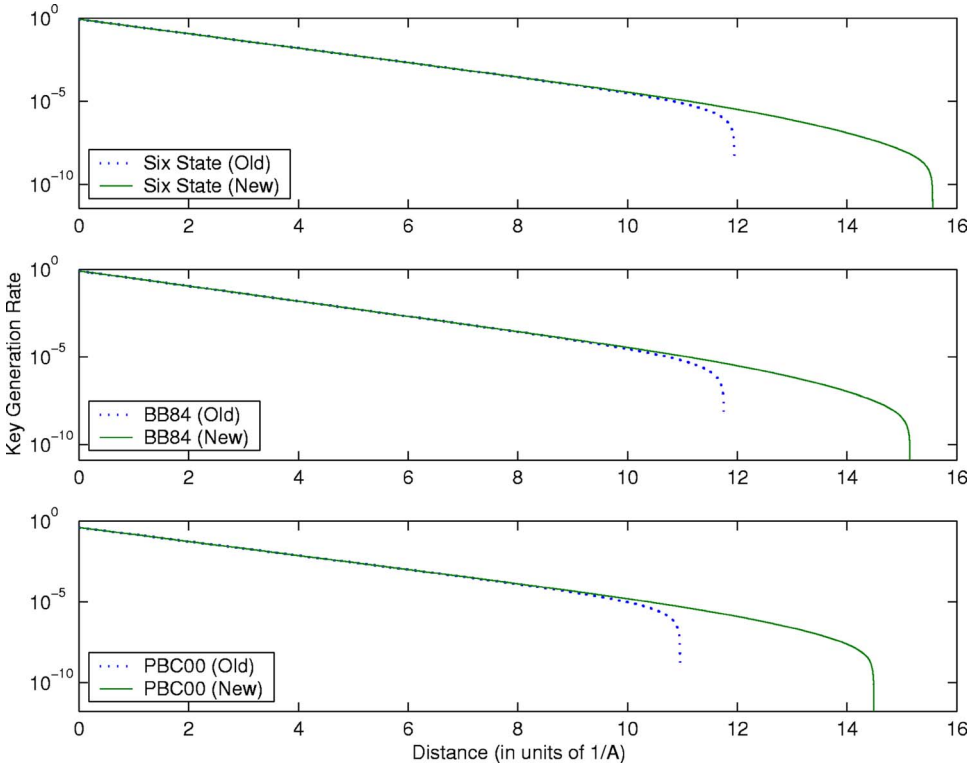

FIG. 1. Semilogarithmic graph of the key generation rate of the PBC00, BB84, and six-state protocols as a function of distance, l, for $e_x^{sq}=0.01$ and $C=10^{-6}$ calculated using the old method [Eq. (2)] and the new one [Eq. (6)] assuming a perfect single-photon source ($p_c^{mq}=0$).

We remark that the concavity of entropy and $\omega_1 e_z^1 = (p^{sq}/p^c)e_z^{sq} + (\omega_1 - p^{sq}/p^c)e_z^{dk}$ imply that $\omega_1 H(e_z^1|e_x) \geqslant (p^{sq}/p^c)H(e_z^{sq}|e_x) + (\omega_1 - p^{sq}/p^c)H(e_z^{dk}|e_x)$. We can rewrite this as $\omega_1[1-H(e_z^1|e_x)] \leqslant (p^{sq}/p^c)[1-H(e_z^{sq}|e_x)]$, since it can be argued that $e_z^{dk}=\frac{1}{2}$. Therefore, the secret key generation rate given by Eq. (5) [and Eq. (6)] is always greater than or equal to the one given by Eq. (2).

To evaluate Eq. (6), Alice and Bob must be able to determine all quantities involved in it. For this purpose, we study two different situations: Alice has a source that emits a single photon on demand or one that follows a Poisson distribution.

In both situations, e_x is estimated from test bits and p_c^{dk} can be calculated from the predetermined dark count probability C of the detectors and the number of empty pulses not associated with dark counts that Bob receives. If C is not fixed, Bob might block his detection units randomly and estimate p_c^{dk} from these results. For this to be true, it is important that Eve is not allowed to reduce the dark count probability without being detected. But is this a valid assumption? In practice, Eve could try to cool down the detectors or send bright pulses to disable them at will. Furthermore, there might be some uncertainty in the measurement of p_c^{dk}, even in the absence of an eavesdropper. Since a dark count could be interpreted as Eve sending a random state to Bob, we remark that lower bounds for C and p_c^{dk} are sufficient to obtain a better key generation rate using Eq. (6). Establishing a high level of confidence on a lower bound for p_c^{dk} seems very hard in practice. However, it might be possible through experimental research and tests on reducing dark count rates of detectors.

If Alice has a source that emits single photons, $\omega_0=0$ and $p_c^{mq}=0$, then Eq. (6) reduces to Eq. (4) and $e_x=(1/p_c)\times(p_c^{sq}e_x^{sq}+p_c^{dk}e_x^{dk})$, where e_x^{dk} is the bit error rate over conclusive events associated with dark counts. $e_x^{dk}=\frac{1}{2}$ which implies that Bob can estimate e_x^{sq} from the value of e_x measured on test bits. $H(e_z^{sq}|e_x)=H(e_z^{sq}|e_x^{sq})$ can be evaluated depending on the protocol used. It can easily be shown that, for the six-state protocol, $e_x^{sq}=e_y^{sq}=e_z^{sq}$ [12]. For the BB84 protocol,

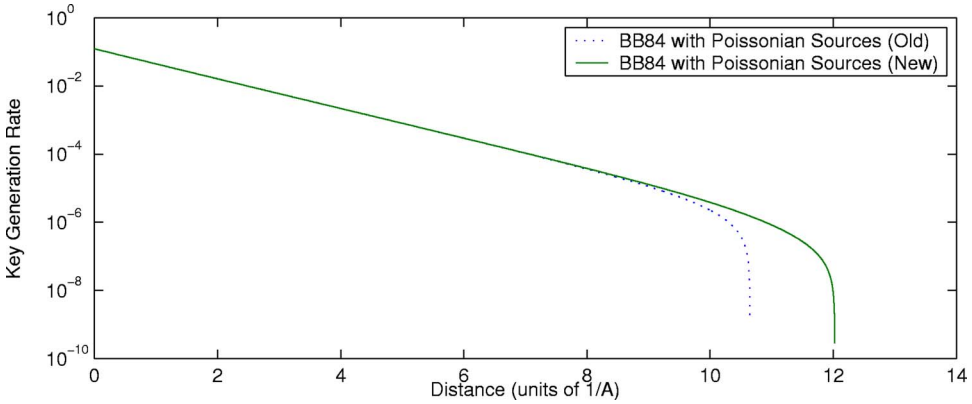

FIG. 2. Semilogarithmic graph of the key generation rate of the BB84 protocol as a function of distance, l, for $e_x^{sq}=0.01$ and $C=10^{-6}$ assuming a Poissonian source and combined with the decoy state method with $\bar{\mu}=0.5$. We compare the key generation rates calculated using Eqs. (2) and (6).

$e_x^{sq}=e_z^{sq}$ and $0\leqslant e_y^{sq}\leqslant 2e_x^{sq}$ [8]. For the PBC00 protocol, it was shown that $e_z^{sq}=\frac{5}{4}e_x^{sq}$ and $\frac{1}{4}e_x^{sq}\leqslant e_y^{sq}\leqslant\frac{9}{4}e_x^{sq}$ [11].

In the absence of errors due to dark counts, $p_c^{dk}=0$. By solving $S(e_x)=0$, we find that the bit error rate threshold is 12.6% for the six-state protocol, 11.0% for the BB84 protocol, and 9.81% for the PBC00 protocol. If we now suppose that e_x^{sq} is fixed, then the bit error rate threshold increases as shown in Table I. Note that the bit error rate threshold depends on the contribution of errors not associated to dark counts.

Table I reflects the potential of a special analysis for dark counts. For any of the previous QKD protocols, if the errors are only caused by dark counts ($e_x^{sq}=0$), then the bit error rate threshold is $\frac{1}{2}$, which implies that there is no bound on the distance for communication. However, we must keep in mind that this result is derived using many special conditions. In practice, e_x^{sq} is nonzero, and since there is decoherence in the channel and extrinsic sources of background noise, e_x^{sq} usually increases with the distance of communication. We also assumed that Alice and Bob perfectly know the dark counts rates of their detectors, that they are the same for all detectors, that they are independent of other measurements, and that Eve cannot lower them. However, even if one or more of these assumptions are not respected, it is still possible to slightly modify Eq. (6), as we explained earlier, and obtain an improvement over Eq. (2).

In Fig. 1, we observe that our method of calculating the key generation rate, using Eq. (6), improves the achievable distance for the PBC00, BB84, and six-state protocols assuming a single-photon source. For simplicity, we suppose that the dark count probability C is the same for all detectors and that e_x^{sq} is fixed and independent of distance. We assume no qubit losses at $l=0$, where l is the length of the channel, and neglect events when two different detectors fire simultaneously. Under these conditions, for the BB84 and six-state protocols, $p_c^{sq}\approx\eta$ and $p_c^{dk}\approx 2C(1-\eta)$, where $\eta=e^{-Al}$ is the probability that a photon successfully travels through the channel and A is the attenuation in the fiber. For the PBC00 protocol, $p_c^{sq}\approx[1/(2-e_x)]\eta$ and $p_c^{dk}\approx 2C(1-\eta)$. Note that, since p_c^{dk}/p_c is always equal or higher in the PBC00 protocol than for the BB84 or six-state protocols, the PBC00 protocol's maximum achievable distance is lower for the same bit error rate.

We now consider the case where Alice uses a source that follows a Poisson distribution ($p_c^{mq}\neq 0$). We only provide the result for the BB84 protocol, but our arguments are valid for other QKD protocols, including the B92, PBC00, and six-state protocols.

Decoy states [20] could be used to evaluate p_c^{sq} and e_x^{sq} precisely. References [21,22] explain how Alice could randomly vary the average photon number μ of her source to obtain, from statistics, precise estimates of the rate of conclusive results associated with single-photon pulses, $p_c\omega$, and the corresponding bit error rate e_x^1. p_c^{sq} and e_x^{sq} can be easily derived from the following two relations: $p_c\omega=p_c^{sq}+2Ce^{-\bar{\mu}}\bar{\mu}(1-\eta)$ and $e_x^1=e^{-\bar{\mu}}\bar{\mu}[\eta e_x^{sq}+2C(1-\eta)e_x^{dk}]/(p_c\omega)$, where $\bar{\mu}$ is the global average photon number. Figure 2 shows that the decoy state method can also be improved by using Eq. (6).

If we do not use decoy states, a worst case estimate of p_c^{sq} and e_x^{sq} is possible. However, Eq. (6) provides only a small improvement since, without decoy states, multiphoton pulses are usually a much more important limiting factor than dark counts.

In this paper, we showed that a high confidence in the stability of the dark counts of the detectors against the possible attack of an eavesdropper implies a significant increase of the robustness of most QKD protocols against dark counts, one of most important contributors of noise in quantum communication. We studied particularly the cases of the PBC00, BB84, and six-state protocols. We explained how to get an improvement of the secret key generation rate and of the achievable distance in some nonideal situations, including when Alice uses a Poissonian photon source, when Alice and Bob know only a lower bound for the dark count rates of their detectors, and when the dark count rates are not uniform over the detectors. Further improvements to the secret key generation rate might come from using two-way error correction [23] and by artificially adding some errors in the key [24].

Our results benefited from discussions with Daniel Gottesman and Hoi-Kwong Lo, whose contributions are greatly appreciated. We thank Nicolas Gisin who proposed using reverse reconciliation. We also thank Tony Anderson for his assistance. J.-C.B. and R.L. acknowledge support from the Government of Ontario, J.B. and R.L. from NSERC, and R.L. from CIAR, MITACS and ARDA.

[1] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004); T. Kimura, Y. Nambu, T. Hatanaka, A. Tomita, H. Kosaka, and K. Nakamura Jpn. J. Appl. Phys., Part 2 **43** L1217 (2004).

[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

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

[4] S. Phoenix, S. Barnett, and A. Chefles, J. Mod. Opt. **47**, 507 (2000).

[5] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).

[6] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

[7] D. Mayers, in *Advances in Cryptology: Proceedings of Crypto'96*, edited by Neil Kolitz, *Lecture Notes in Computer Science*, Vol. 1109 (Springer-Verlag, Berlin, 1996), p. 343.

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

[9] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[10] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003); K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).
[11] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[12] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[13] J. M. Renes and M. Grassl, e-print quant-ph/0505061.
[14] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[15] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996); A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[16] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[17] R. Renner and R. Koenig, Second Theory of Cryptography Conference **3378**, 407 (2005).
[18] H.-K. Lo, e-print quant-ph/0503004.
[19] H.-K. Lo and J. Preskill, e-print quant-ph/0504209.
[20] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[21] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[22] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005). X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[23] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[24] B. Kraus, N. Gisin, and R. Renner, e-print quant-ph/0410215.