# Security proof of a three-state quantum-key-distribution protocol without rotational symmetry

Chi-Hang Fred Fung* and Hoi-Kwong Lo†

*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario M5S 3G4, Canada*

(Received 8 July 2006; published 31 October 2006)

Standard security proofs of quantum-key-distribution (QKD) protocols often rely on symmetry arguments. In this paper, we prove the security of a three-state protocol that *does not* possess rotational symmetry. The three-state QKD protocol we consider involves three qubit states, where the first two states $|0_z\rangle$ and $|1_z\rangle$ can contribute to key generation, and the third state $|+\rangle=(|0_z\rangle+|1_z\rangle)/\sqrt{2}$ is for channel estimation. This protocol has been proposed and implemented experimentally in some frequency-based QKD systems where the three states can be prepared easily. Thus, by founding on the security of this three-state protocol, we prove that these QKD schemes are, in fact, unconditionally secure against any attacks allowed by quantum mechanics. The main task in our proof is to upper bound the phase error rate of the qubits given the bit error rates observed. Unconditional security can then be proved not only for the ideal case of a single-photon source and perfect detectors, but also for the realistic case of a phase-randomized weak coherent light source and imperfect threshold detectors. Our result in the phase error rate upper bound is independent of the loss in the channel. Also, we compare the three-state protocol with the Bennett-Brassard 1984 (BB84) protocol. For the single-photon source case, our result proves that the BB84 protocol strictly tolerates a higher quantum bit error rate than the three-state protocol, while for the coherent-source case, the BB84 protocol achieves a higher key generation rate and secure distance than the three-state protocol when a decoy-state method is used.

DOI: 10.1103/PhysRevA.74.042342 PACS number(s): 03.67.Dd

## I. INTRODUCTION

Quantum key distribution (QKD) [1,2] allows two distant parties to expand a previously shared secret key by sending quantum states through a quantum channel. The most well-known QKD protocol is the Bennett-Brassard 1984 (BB84) protocol [1], which has been proved unconditionally secure against any attacks allowed by quantum mechanics [3–11]. Standard security proofs of many QKD protocols, including the BB84 protocol, the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol [12–15], the symmetric three-state protocol [16,17], and the generalized rotationally symmetric protocol [18,19], often rely on rotational symmetries. In this paper, we prove the security of a QKD protocol that *does not* possess rotational symmetry. The protocol involves Alice sending one of the three qubit states $\{|0_z\rangle,|1_z\rangle,(|0_z\rangle+|1_z\rangle)/\sqrt{2}\}$ to Bob, where the first two states are for key generation and the third state is for channel estimation. Note that this protocol is similar to the BB84 protocol in that they share the same three qubit states. In fact, in practical implementations of the BB84 protocol, when one of the four laser sources is out of operation (due to, for example, malfunctioning), the QKD scheme implemented becomes the three-state protocol that we consider in this paper. The security proof of the three-state protocol analyzed in this paper then assures us that even the handicapped BB84 protocol can still be secure in these situations [20]. This three-state protocol has also been proposed and implemented in some frequency-based QKD systems [21–23].[1] In these frequency-based systems, the state $|0_z\rangle$ ($|1_z\rangle$) is represented by a pulse in frequency $\omega_0$ ($\omega_1$), while the state $(|0_z\rangle+|1_z\rangle)/\sqrt{2}$ is represented by a pulse in a superposition of the two frequencies. In these systems, it is relatively easy to generate the three states and thus the three-state protocol is well suited for these systems. In order to understand the security of these systems, a rigorous security analysis of the three-state protocol is in order and it is the purpose of this paper to provide such an analysis. We note that a similar protocol has been proposed and implemented in some time-bin-based QKD systems [24–28]. In one time-bin-based scheme [28], each signal is associated with two time positions and there are three different signals. A logic 0 (1) is represented by a light pulse in the first (second) position and no pulse in the other position, while a decoy signal is represented by a superposition of a pulse in the first position and a pulse in the second position. The channel is estimated by checking the coherence between two consecutive nonempty pulses appearing within or across the bit separations. This gives rise to the difference between this protocol and the one we consider in this paper. If only the coherence within the bit separations was checked, then it is equivalent to our protocol. Thus, the analysis in the paper does not directly apply to this particular time-bin-based scheme. On the other hand, the result of this paper suggests that even if only the coherence within the bit separations is checked, unconditional security can still be established, thus making it unnecessary to check for the across-the-bit coher-

*Electronic address: cffung@comm.utoronto.ca
†Electronic address: hklo@comm.utoronto.ca

[1]Note that some of these systems actually prepare the state $|0_z\rangle+|1_z\rangle$ instead, which has a different normalization (without the factor of $\sqrt{2}$) than the one we consider. These QKD systems are not qubit based, and thus our security proof is not directly applicable to them.

 

ence for the sake of achieving unconditional security. This means that a secure time-bin-based scheme can be built by implementing the three-state protocol analyzed in this paper, where the channel-estimation state is realized by checking the within-the-bit coherence.

In this paper, we prove the unconditional security of the three-state protocol not only for the case of a single-photon source, but also for the case of a phase-randomized weak coherent-state source. Essentially, the reason that the protocol is secure is because the information gain by an eavesdropper implies disturbance in the signals received by a legitimate receiver. Here, our main task is to make this argument rigorous and quantitative. To do this, we upper bound the phase error rate of the key-generating qubits using the bit error rates of the key-generating qubits and the channel-estimation qubits [cf. Eq. (26)] with the assumption that a single-photon source is used. Once the phase error rate is estimated, we may establish the security of the protocol by applying Shor and Preskill's argument [6] when a single-photon source is used and by applying the result of Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [8] and the decoy-state method [29–38] when a coherent light source is used. We remark that our result on the phase error rate upper bound is independent of the loss in the channel, similar to the BB84 protocol.

The paper is organized as follows: We first describe the three-state protocol in Sec. II. In Sec. III, we upper-bound the phase error rate of the key-generating qubits. This upper bound can then be used to compute the key generation rate for both the ideal case and the realistic case in Sec. IV. We finally conclude in Sec. V.

## II. THE PROTOCOL

In this section, we outline the three-state protocol in prepare-and-measure version which is how it can be implemented in reality without a quantum computer and in an entanglement-distillation-protocol- (EDP-) based version which is equivalent to the prepare-and-measure form and is used mainly for proving the security. In the following, we assume that Alice and Bob are equipped with a perfect single-photon source and perfect detectors. Also, only the qubits detected by Bob are considered, and thus the security proof of this protocol is loss independent.

We use the following notations: the eigenstates in the $Z$ basis are $|0_z\rangle$ and $|1_z\rangle$, whereas the eigenstates in the $X$ basis are $|+\rangle \triangleq (|0_z\rangle + |1_z\rangle)/\sqrt{2}$ and $|-\rangle \triangleq (|0_z\rangle - |1_z\rangle)/\sqrt{2}$.

### A. Prepare-and-measure version

We outline the protocol as follows.

(i) Alice chooses a random $8N(1+\delta)$-bit string $\mathbf{a}$, where $\delta > 0$ is a small parameter. For each bit $i$, if $a_i = 0$, she transmits a state randomly chosen in the $|0_z\rangle$, $|1_z\rangle$ basis; if $a_i = 1$, she transmits $|+\rangle$.

(ii) Bob receives the $8N(1+\delta)$ qubits and using a random $[8N(1+\delta)]$-bit string $\mathbf{b}$ measures each qubit in the $Z$ basis (if $b_i = 0$) or the $X$ basis (if $b_i = 1$).

(iii) Alice announces $\mathbf{a}$ and Bob announces $\mathbf{b}$.

(iv) They discard any results where $a_i \neq b_i$. With high probability, there are at least $4N$ bits left and $2N$ of them belong to each basis. Alice decides $N$ bits in the $Z$ basis as the check bits and the remaining $N$ bits in the $Z$ basis as the data bits.

(v) Alice and Bob announce the values of the $N$ check bits in the $Z$ basis and the $2N$ check bits in the $X$ basis. They compute the quantum bit error rates for the two sets separately. We denote the two quantum bit error rate (QBER) values by $e_b$ and $\alpha$, respectively.

(vi) They choose an error correcting code capable of correcting errors at a bit error rate of $e_b$. Alice computes the bit error syndrome of her data bits using this code and transmits the syndrome to Bob. Bob corrects the errors in his data bits.

(vii) They estimate the phase error rate $e_p$ of the data bits from $e_b$ and $\alpha$ and choose a binary block code capable of correcting errors at a rate of $e_p$. They apply the generator matrix of the code to their data bits, producing the final secret key.

We remark that the data bits consist of only the key-generating qubits $\{|0_z\rangle, |1_z\rangle\}$, while the check bits consist of all qubits $\{|0_z\rangle, |1_z\rangle, |+\rangle\}$ of which the first two are also used for the key generation and the third is only for channel estimation. The task is to estimate the phase error rate $e_p$ of the data bits from the bit error rates $e_b$ and $\alpha$ of the check bits. Also note that this three-state protocol is very similar to the BB84 protocol. The only difference is that the $|-\rangle$ state in BB84 is not used in this protocol.

### B. EDP-based version

Now we describe the equivalent EDP-based QKD protocol. During the quantum state transmission phase, Alice sends Bob $4N$ quantum signals through a channel controlled by an eavesdropper Eve. Specifically, for the $l$th signal, Alice prepares the state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}|0\rangle_K \left[ \frac{1}{\sqrt{2}}|0_z\rangle_A|0_z\rangle_B + \frac{1}{\sqrt{2}}|1_z\rangle_A|1_z\rangle_B \right] + \frac{1}{\sqrt{2}}|1\rangle_K|+\rangle_A|+\rangle_B \quad (1)$$

and sends system $B$ to Bob through Eve while keeping system $A$ to herself. In the most general attack by Eve, she interacts the $4N$ signals sent by Alice and some ancilla with an unitary operation. An output qubit from the unitary operation is then sent to Bob for the $l$th transmission. We assume that Bob always uses the same basis as Alice for each qubit pair, since the qubit pairs where Alice and Bob measure with different bases are discarded. Specifically, for the $2N$ check qubit pairs in the $|1\rangle_K$ part, Bob measures in the $\{|+\rangle, |-\rangle\}$ basis, and since Alice always sends the $|+\rangle$ state to Bob, he declares an error (no error) if the measurement outcome is $|-\rangle$ ($|+\rangle$). This allows him to compute the QBER for this part, which we denote by $\alpha$. For the $2N$ qubit pairs in the $|0\rangle_K$ part, Alice and Bob randomly choose $N$ of them as check qubit pairs and compare their values publicly. They both perform $Z$ basis measurements on them and announce their measurement outcomes in order to compute the QBER

for these $N$ qubit pairs, which we denote by $e_b$. An error correcting code capable of correcting errors up to a bit error rate of $e_b$ can be used by Alice and Bob to remove errors in the remaining $N$ data qubit pairs, which are then privacy amplified to produce the final key. Since the amount of privacy amplification needed to eliminate Eve's information on the final key is indicated by the phase error rate of the data qubit pairs (denoted by $e_p$), Alice and Bob need to upper bound this quantity from what they observed, $e_b$ and $\alpha$. In what follows, we solve this problem of upper bounding $e_p$ given fixed values of $e_b$ and $\alpha$. Once $e_p$ is obtained, the key generation rate can easily be computed using $e_p$ and $e_b$.

## III. UPPER-BOUNDING THE PHASE ERROR RATE

In this section, we solve the main problem of upper-bounding the phase error rate in the data qubit pairs, using the bit error rates observed in the check qubit pairs. The values $e_b$ and $\alpha$ are actually observed in the check qubit pairs, not in the data qubit pairs. On the other hand, we are interested in the bit error rates of the data qubit pairs, not the check qubit pairs. In order to relate $e_b$ and $\alpha$ to the data qubit pairs, we apply a random sampling argument to infer that what is observed in the check qubit pairs is very close to what could be observed in the data qubit pairs. Specifically, the random sampling argument can be stated as follows

*Lemma 1 [random sampling test (see, for example, [39])].* Given $2N$ bits, they are randomly divided into two sets, each containing $N$ bits. Then,

$$\Pr\{c_1 < \delta N \text{ and } c_2 > (\delta+\epsilon)N\} < \exp[-O(\epsilon^2 N)], \quad (2)$$

where $c_1$ and $c_2$ are the number of ones in the two sets, $\delta \leqslant 1$ is some fraction representing the number of ones, and $\epsilon > 0$ is a small parameter.

Therefore, with high probability, the bit error rates of $e_b$ and $\alpha$ could be observed in the data qubit pairs. Note that the use of classical probability argument is valid here, since the events contributing to $e_b$, $e_p$, and $\alpha$ are outcomes of a projection measurement projecting onto the states $\{|0\rangle_K|\phi_{ij}\rangle, |1\rangle_K|\phi_{i'j'}\rangle : i,j,i',j' = 0,1\}$. Here, $|\phi_{ij}\rangle$ are the Bell states:

$$|\phi_{ij}\rangle = \frac{1}{\sqrt{2}}(|0i\rangle_z + (-1)^j|1\bar{i}\rangle_z). \quad (3)$$

In what follows, because of this random sampling argument, we assume that the QBER's $e_b$ and $\alpha$ are also observed in the $N$ data qubit pairs. Now the model becomes Alice sending $N$ data qubits to Bob through Eve who may perform on them any joint operation that are consistent with $e_b$ and $\alpha$. Since we only consider the data qubit pairs, we index them from $l=1$ to $l=N$ for simplicity. Eve's operation on the $l$th data qubit pair can conveniently be represented in the Kraus (or operator sum) form $\mathcal{E}^{(l)}(\rho) = \Sigma_f E^{(l,f)} \rho E^{(l,f)\dagger}$, where the set of operator $\{E^{(l,f)} : \forall f\}$ defines the mapping for the $l$th data qubit pair and all the other data qubit pairs have been traced over. Recall that the our main problem is to upper bound $e_p$ over all Eve's operations $\mathcal{E}^{(l)}(\cdot)$ that are consistent with the observed values of $e_b$ and $\alpha$. Essentially, there are two constraints in our optimization problem: one associated with $e_b$ and the other with $\alpha$. We first consider the constraint with $\alpha$ by computing the correct and incorrect probabilities associated with each data qubit pair if a measurement in the $|1\rangle_K$ basis were to be performed. In this basis, there are only two outcomes: either that Alice sends $|+\rangle$ and Bob receives $|+\rangle$ (no bit error) or that Alice sends $|+\rangle$ and Bob receives $|-\rangle$ (a bit error). The corresponding probabilities are

$$p_{+-}^{(l)} \triangleq \Pr\{\text{error at position } l\} = {}_{KAB}\langle 1+-|\mathcal{E}^{(l)}(|\Psi\rangle\langle\Psi|)|1+-\rangle_{KAB}, \quad (4)$$

$$p_{++}^{(l)} \triangleq \Pr\{\text{no error at position } l\} = {}_{KAB}\langle 1++|\mathcal{E}^{(l)}(|\Psi\rangle\langle\Psi|)|1++\rangle_{KAB}. \quad (5)$$

[The notation used is that $+-$ $(++)$ in the subscript means that Alice sends $|+\rangle$ and Bob measures $|-\rangle$ $(|+\rangle)$.] To construct the first constraint, we need to relate these two probabilities for the data bits to $\alpha$. Note that they are not related in a straightforward manner, since $\alpha$ is the observed bit error rate in the data qubit pairs (inferred from that of the check qubit pairs using the random sampling argument) while we only have probabilities of each data qubit pair on hand. In this situation, we utilize Azuma's inequality [40] to establish the relation, as used similarly in [14,15,17]. To proceed, we obtain Eve's operation on the $l$th qubit pair, $\mathcal{E}^{(l)}(\cdot)$, by tracing over the previously measured qubit pairs conditional on their measurement outcomes and unconditionally tracing over the qubit pairs to be measured later. This means that the two probabilities in Eqs. (4) and (5) are now *conditional* probabilities, conditional on the measurement outcomes of the previously measured qubits. Considering each event separately, Azuma's inequality asserts that the sum of the error (no error) probabilities over all qubits is close to the observed counts of the error (no error) events. Mathematically, it means that

$$\Pr\left[\left|\frac{c_{+\pm} - \sum_{l=1}^{N} p_{+\pm}^{(l)}}{N}\right| \geqslant \epsilon\right] \leqslant 2\exp^{-N\epsilon^2/2}, \quad (6)$$

where $c_{+-}$ $[c_{++}]$ is the observed counts of the error [no error] events, $p_{+-}^{(l)}$ $[p_{++}^{(l)}]$ is the error [no error] probability for the $l$th qubit pairs given by Eq. (4) [Eq. (5)], and $\epsilon > 0$ is a small quantity. Note that this probability drops exponentially as $N$ increases. Now, since $\alpha = c_{+-}/(c_{+-}+c_{++})$ by definition, it is easy to relate $p_{+\pm}^{(l)}$ to $\alpha$ as $N$ goes to infinity as follows:

$$\alpha = \frac{\sum_{l=1}^{N} p_{+-}^{(l)}}{\sum_{l=1}^{N} p_{+-}^{(l)} + p_{++}^{(l)}}. \quad (7)$$

Note that no actual measurement in the $\{|+\rangle, |-\rangle\}$ basis is performed on the data qubit pairs (only measurements in the $\{|0_z\rangle, |1_z\rangle\}$ basis are performed on them), and thus we have no

measurement outcomes of the earlier qubit pairs to explicitly form $\mathcal{E}^{(l)}(\cdot)$. Nevertheless, Eq. (7) holds for any measurement outcomes, and there is no need to know what these outcomes are. Note that as an alternative to Azuma's inequality, the quantum de Finetti theorems [41–44] may be used to argue that the entanglement between a subset of the randomly permuted qubit pairs vanishes, establishing Eq. (7) also. In this case, a sublinear number of qubit pairs have to be discarded.

By the same token, the second constraint of our optimization problem associated with $e_b$ can be constructed in a similar way. In this case, there are four possibilities associated with the data qubit pairs: no error, a bit error, a phase error, and both types of errors. Thus, they give rise to the following four probabilities:

$$q_{rs}^{(l)} \triangleq {}_K\langle 0|_{AB}\langle \phi_{rs}|\mathcal{E}^{(l)}(|\Psi\rangle\langle\Psi|)|\phi_{rs}\rangle_{AB}|0\rangle_K,$$

$$r,s = 0,1, \tag{8}$$

where $|\phi_{rs}\rangle$ are the Bell states defined in Eq. (3). Applying Azuma's inequality gives

$$e_b = \frac{\sum_{l=1}^{N} q_{10}^{(l)} + q_{11}^{(l)}}{\sum_{l=1}^{N} q_{00}^{(l)} + q_{10}^{(l)} + q_{11}^{(l)} + q_{01}^{(l)}}, \tag{9}$$

$$e_p = \frac{\sum_{l=1}^{N} q_{01}^{(l)} + q_{11}^{(l)}}{\sum_{l=1}^{N} q_{00}^{(l)} + q_{10}^{(l)} + q_{11}^{(l)} + q_{01}^{(l)}}. \tag{10}$$

Therefore, our optimization problem becomes maximizing $e_p$ given in Eq. (10) over Eve's operations $\mathcal{E}^{(l)}(\cdot)$ subject to Eqs. (7) and (9). To simplify the problem, by using the parametrization $E^{(l,f)} = a_I^{(l,f)} I + a_X^{(l,f)} X + a_Y^{(l,f)} Y + a_Z^{(l,f)} Z$ and explicitly evaluating $p_{+\pm}^{(l)}$ and $q_{rs}^{(l)}$, we rewrite the maximization problem as follows:

$$\text{maximize} \quad e_p = \frac{\sum_{l,f} |a_Z^{(l,f)}|^2 + |a_Y^{(l,f)}|^2}{\sum_{l,f} |a_I^{(l,f)}|^2 + |a_X^{(l,f)}|^2 + |a_Y^{(l,f)}|^2 + |a_Z^{(l,f)}|^2}, \tag{11}$$

$$\text{subject to} \quad e_b = \frac{\sum_{l,f} |a_X^{(l,f)}|^2 + |a_Y^{(l,f)}|^2}{\sum_{l,f} |a_I^{(l,f)}|^2 + |a_X^{(l,f)}|^2 + |a_Y^{(l,f)}|^2 + |a_Z^{(l,f)}|^2}, \tag{12}$$

$$\alpha = \frac{\sum_{l,f} |i a_Y^{(l,f)} - a_Z^{(l,f)}|^2}{\sum_{l,f} |i a_Y^{(l,f)} - a_Z^{(l,f)}|^2 + |a_I^{(l,f)} + a_X^{(l,f)}|^2}, \tag{13}$$

where the maximization is over all $a_\beta^{(l,f)}$, $\beta = I,X,Y,Z$. Note that the summation over all the qubit pairs $l$ in this problem signifies that Eve's attack is a joint attack. However, the following theorem says that a collective attack by Eve is as powerful as a joint attack in the sense of causing the same bit and phase error rates $\{e_b, \alpha, e_p\}$. Furthermore, Eve's collective attack only needs to consist of one Kraus operator. This theorem essentially eliminates the need to consider joint attacks in upper bounding the phase error rate.

*Theorem 1 (reduction from a joint attack to a collective attack).* For the three-state protocol, any values of the bit and phase error rates $\{e_b, \alpha, e_p\}$ achievable by any joint attack consisting of any number of Kraus operators are also achievable by a collective attack consisting of only one Kraus operator.

*Proof.* The idea is that any two sets $\{a_I^{(l,f)}, a_X^{(l,f)}, a_Y^{(l,f)}, a_Z^{(l,f)}\}$ and $\{a_I^{(l',f')}, a_X^{(l',f')}, a_Y^{(l',f')}, a_Z^{(l',f')}\}$ can be combined into one set without changing the values of $e_b$, $\alpha$, and $e_p$ (see the Appendix). Repeated applications of this idea can reduce any number of sets into one set. This means that whatever values of $\{e_b, \alpha, e_p\}$ achievable by any number of sets are also achievable by just one set. ■

The consequence of this theorem is that it is sufficient to consider $(l,f)$ taking on only one value (i.e., dropping the summations over $l$ and $f$) in the maximization problem in Eq. (11) without loss of generality. This is an important consequence since the original maximization problem in Eq. (11) involves infinitely many optimization variables $(a_\beta^{(l,f)}, \forall l,f)$ and the new maximization problem involves only four optimization variables $(a_I, a_X, a_Y, a_Z)$. This is a significant simplification in the problem. Note that the reduction from joint attacks to collective attacks was first discussed in Ref. [45]. The idea was also implicitly used in Ref. [10]. Similar reduction results with explicit proofs were also obtained in an information-theoretic security proof [46] and can also be deduced from the quantum de Finetti theorems [41–44]. These two techniques are different from ours. In particular, the difference between the techniques involving the quantum de Finetti theorems and ours is that the former requires discarding a sublinear number of qubits and ours does not require any discarding. This difference may have practical implications when the number of qubits is finite. Even though the number of discarded qubits in the de Finetti approximation is insignificant in the asymptotic case, it may be significant in the finite situation. The difference between the information-theoretic security proof and ours is that in the former, a collective attack is equal to a joint attack in the sense that the smooth Rényi entropies of the states in the two attacks are roughly equal, and in our proof, the two attacks are equal in the sense that they both cause exactly the same bit and phase error rates. Also, we further show that it is sufficient to consider a collective attack consisting of only one Kraus operator as opposed to infinitely many Kraus operators.

### A. Exact upper bound

In order to simplify the maximization problem in Eq. (11), we first write it as

$$\max \quad (|a_Z|^2 + |a_Y|^2)e_b, \tag{14}$$

$$\text{subject to} \quad |a_X|^2 + |a_Y|^2 = 1, \tag{15}$$

$$\frac{1-e_b}{e_b} = |a_I|^2 + |a_Z|^2, \tag{16}$$

$$\frac{1-\alpha}{\alpha} = \frac{|a_I + a_X|^2}{|ia_Y - a_Z|^2}, \tag{17}$$

where the first constraint is introduced to fix the scaling of $a_\beta$'s and the second and third constraints are rearrangements of Eqs. (12) and (13). To simplify the problem further, we note that in order to maximize the objective, the third constraint should be taken so that $a_I$ and $a_X$ are in phase with each other and $ia_Y$ and $a_Z$ are in phase with each other. This results in the following problem:

$$\max \quad (|a_Z|^2 + |a_Y|^2)e_b, \tag{18}$$

$$\text{subject to} \quad |a_X|^2 + |a_Y|^2 = 1, \tag{19}$$

$$\hat{e_b} := \frac{1-e_b}{e_b} = |a_I|^2 + |a_Z|^2, \tag{20}$$

$$\hat{\alpha} := \frac{1-\alpha}{\alpha} = \frac{|a_I|^2 + |a_X|^2 + 2|a_I||a_X|}{|a_Y|^2 + |a_Z|^2 - 2|a_Y||a_Z|}. \tag{21}$$

Since the feasible region in $(|a_I|,|a_X|,|a_Y|,|a_Z|)$ is described by three constraints, we can eliminate two of them—namely, $a_I$ and $a_X$—to get one single constraint describing the feasible region in terms of $(|a_Y|,|a_Z|)$ by substituting Eqs. (19) and (20) into Eq. (21):

$$(\hat{e_b} - |a_Z|^2) + (1-|a_Y|^2) + 2\sqrt{1-|a_Y|^2}\sqrt{\hat{e_b} - |a_Z|^2} = \hat{\alpha}(|a_Y|^2 + |a_Z|^2 - 2|a_Y||a_Z|). \tag{22}$$

Squaring both sides gives a quartic equation, which admits four solutions for $|a_Z|$ in terms of $|a_Y|$. However, there are only two valid solutions in the region $e_b \leq 1/2$ and $\alpha \leq 1/2$:

$$|a_Z| = \frac{1}{1+\hat{\alpha}}[\hat{\alpha}|a_Y| \pm \sqrt{\hat{\alpha}(1-|a_Y|^2)} \pm \sqrt{-1 + \hat{e_b}(1+\hat{\alpha}) - |a_Y|^2(\hat{\alpha}-1) \pm 2|a_Y|\sqrt{\hat{\alpha}(1-|a_Y|^2)}}], \quad e_b, \alpha \leq 1/2, \tag{23}$$

where the signs are $(--+)$ and $(++-)$. Since $|a_Z|$ is part of the objective function of the problem in Eq. (18), we want to use of the solution of $|a_Z|$ that is the largest. Therefore, we use the solution of $|a_Z|$ with signs $(++-)$ and the problem becomes

$$\max_{|a_Y| \leq 1} \quad (|a_Z|^2 + |a_Y|^2)e_b, \tag{24}$$

where $|a_Z|$ substituted from Eq. (23) with signs $(++-)$. This problem can be solved numerically for some fixed $e_b$ and $\alpha$ to obtain an upper bound on $e_p$ (which is the objective value of the problem). Note that Eve can always construct an attack with $e_p = 1/2$ that is as powerful as any arbitrary attack with an arbitrary $e_p \leq 1$ [47]. She can construct this new attack by launching half of the time the arbitrary attack and the other half of the time the arbitrary attack with a phase flip operation. In this way, the phase error rate of this new attack is 1/2.

### B. Limiting cases

We need to deal with the cases that $e_b = 0$, $\alpha = 0$, or both separately. For the case that $e_b = 0$ and $\alpha > 0$, we see from Eq. (12) that $a_X = a_Y = 0$ and thus $e_p = \alpha$. For the case that $e_b > 0$ and $\alpha = 0$, we see from Eq. (13) that $a_Z = ia_Y$ and thus $e_p \leq 2e_b$. For the case that $e_b = 0$ and $\alpha = 0$, we have $a_X = a_Y = a_Z = 0$ and thus $e_p = 0$. Note that the last case is consistent with the idea that information gain implies disturbance. Since there is no disturbance in that case, no information is gained by Eve and thus $e_p = 0$.

### C. Closed-form approximate upper bound

It may be difficult to solve the problem in Eq. (24) analytically. Thus, in order to obtain an analytical upper bound on $e_p$, instead of using the exact value for $|a_Z|$ from Eq. (23), we use an upper bound of $|a_Z|$ which is given by

$$|a_Z| \leq \frac{1}{1+\hat{\alpha}}[\hat{\alpha}|a_Y| + \sqrt{\hat{\alpha}(1-|a_Y|^2)} + \sqrt{-1 + \hat{e_b}(1+\hat{\alpha})}]. \tag{25}$$

We use this upper bound for $|a_Z|$ in the problem $\max_{|a_Y| \leq 1}(|a_Z|^2 + 1)e_b$. Since the objective value of this problem is larger than or equal to the objective value of the original problem in Eq. (24), the solution of this problem is definitely an upper bound (but may not be tight) on $e_p$. The solution to the approximate upper bound is

$$\begin{aligned} e_p &\leq \left[1 + \left(\sqrt{\frac{\hat{\alpha}}{1+\hat{\alpha}}} + \frac{1}{1+\hat{\alpha}}\sqrt{-1 + \hat{e_b}(1+\hat{\alpha})}\right)^2\right]e_b \\ &= \left[1 + \left(\sqrt{1-\alpha} + \alpha\sqrt{-1 + \frac{1-e_b}{e_b\alpha}}\right)^2\right]e_b \\ &= \alpha + e_b(2 - 2\alpha - \alpha^2) \\ &\quad + 2\sqrt{\alpha(1-\alpha)e_b(1-e_b-e_b\alpha)}, \quad e_b, \alpha \leq 1/2. \end{aligned} \tag{26}$$

Note that the three special cases in Sec. III B can be obtained by taking the corresponding limit in Eq. (26). In order to illustrate how good the approximate upper bound in Eq. (26) is compared to the optimal one obtained by solving the problem in Eq. (24) numerically, we plot in Fig. 1 the two bounds on $e_p$ over different values of $e_b$ assuming $e_b = \alpha$. It can be seen that the approximate bound is very close to the optimal

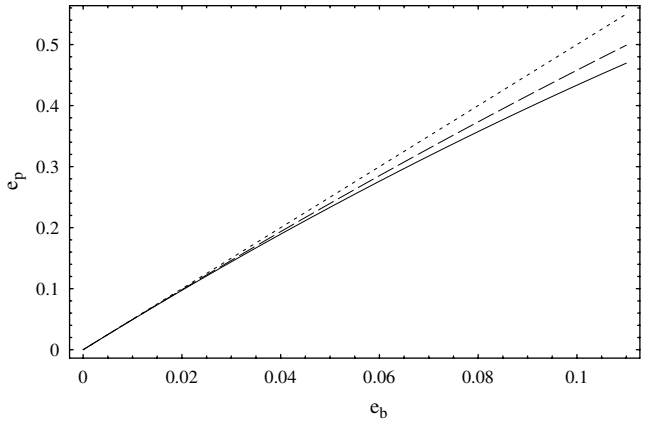


FIG. 1. Comparison of the approximate upper bounds on $e_p$ in Eqs. (26) and (28) with the optimal one obtained by solving the problem in Eq. (24), assuming $e_b=\alpha$. The solid, dashed, and dotted curves (from bottom to top) correspond to the optimal bound [Eq. (24)], the general approximate bound [Eq. (26)], and the specific approximate bound [Eq. (28)].

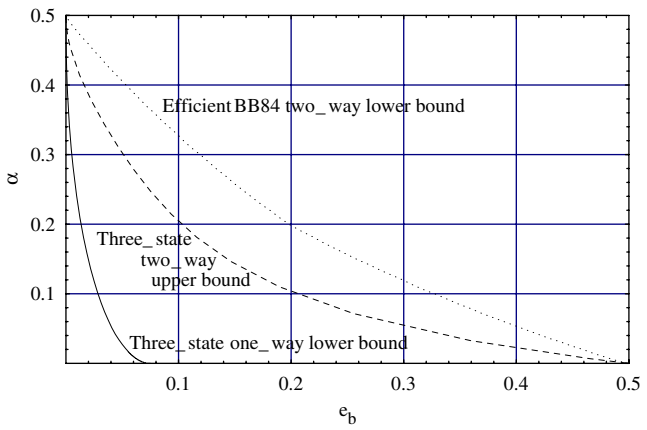


FIG. 2. (Color online) QBER bounds of the three-state protocol and the efficient BB84 protocol. For the three-state protocol, the region below the solid curve is secure with 1-LOCC and the region above the dashed curve is insecure with 2-LOCC. The solid curve is computed using the approximate phase error rate upper bound in Eq. (26), while the dashed curve is computed using a method based on intercept-and-resend attacks [48]. For the three-state protocol, the QBER lower bound for the $Z$-basis states (the $x$ intercept) is 0.075 and the QBER lower bound for the $|+\rangle$ state (the $y$ intercept) is 1/2. The 2-LOCC lower bound for the efficient BB84 protocol (dotted curve) is reproduced from Ref. [49] with a higher precision.

one, especially for small $e_b$. Note that one may obtain another simple bound on $e_p$ from Eq. (26) as

$$e_p \leqslant \alpha + 2e_b + 2\sqrt{e_b\alpha}. \tag{27}$$

This bound is close to the bound in Eq. (26) when both $e_b$ and $\alpha$ are small.

### D. Special case: $e_b=\alpha$

For the special case $e_b=\alpha$, a linear relation between $e_b$ and the approximate $e_p$ can be derived easily. Substituting $\alpha=e_b$ in Eq. (27), we get

$$e_p \leqslant 5e_b. \tag{28}$$

This linear relation, which can readily be observed in Fig. 1, is in sharp contrast to the $e_p=e_b$ relation for the BB84 protocol; specifically, there is a factor of 5 increase (approximately) in the relation for this three-state protocol.

## IV. KEY GENERATION RATE

In the previous section, we derived two upper bounds on the phase error rate for the three-state protocol; an optimal one is given by the solution of the problem in Eq. (24) and an approximate one is given by Eq. (26). Using the phase error rate upper bounds, the key generation rate can be readily obtained both for the single-photon source case and for the coherent-source case. Obviously, when comparing the performance of the three-state protocol and the BB84 protocol, the three-state protocol can only perform as good as, but no better than, the BB84 protocol, since one state is absent in the three-state protocol. Indeed, as we show in the following, the BB84 protocol is superior to the three-state protocol in the tolerable QBER, the key generation rate, and the maximal secure distance.

### A. Single-photon source and perfect detectors

When a single-photon source and perfect detectors are used, the key generation rate on the sifted key using local operations and one-way classical communications (1-LOCC) can be obtained by applying Shor-Preskill's argument [6]:

$$R = 1 - H_2(e_b) - H_2(e_p), \tag{29}$$

where $e_p$ is either the approximate upper bound in Eq. (26) or the solution of the problem in Eq. (24), and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function. Figure 2 shows the secure region using this key generation rate with the approximate upper bound in Eq. (26). The curve is found by searching for $(e_b, \alpha)$ such that the key rate in Eq. (29) is zero. The highest tolerable QBER of the data bits is $e_b=0.075$ when $\alpha=0$; whereas the highest tolerable QBER of the check bits is $\alpha=1/2$ when $e_b=0$. Also shown in the figure are the upper bound for the protocol with local operations and two-way classical communications (2-LOCC), computed using a method based on intercept-and-resend attacks proposed by us [48], and the lower bound for the efficient BB84 protocol [50] with 2-LOCC. The latter is reproduced from Ref. [49] (the "Gottesman-Lo" curve in Fig. 2 of Ref. [49]) with a higher precision. We can compare the three-state protocol with the efficient BB84 protocol regarding the tolerable bit error rates. It can be seen that the lower bound curve for the efficient BB84 protocol is above the upper bound curve for the three-state protocol. Thus, the efficient BB84 protocol can tolerate higher bit error rates than the three-state protocol.

We consider the special case $e_b=\alpha$, which corresponds to a 45° line in Fig. 2. In this case, we may obtain the tolerable $e_b$ of the three-state protocol from the figure or by substituting the approximate relation given in Eq. (28) into the key-generation-rate formula given in Eq. (29). Using the latter method, we obtain a lower bound of $e_b=0.0425$, which is

substantially lower than the one-way lower bound of BB84 ($e_b$=0.110 [6]). The two-way lower bound of BB84 corresponds to the point where $e_b=\alpha$ on the efficient BB84 curve in Fig. 2 and is equal to 19.9%. This is higher than the two-way upper bound of the three-state protocol at $e_b=\alpha$ =14.6%. Thus, the BB84 protocol strictly tolerates a higher QBER than the three-state protocol does.

### B. Coherent source and imperfect threshold detectors

In the previous section, we derived the upper bounds on the phase error rate of the three-state protocol with the assumption of a single-photon source. Nevertheless, we can easily establish security when a phase-randomized weak coherent light source and imperfect threshold detectors are used by applying the decoy-state method [29–38]. In essence, the bit error rates of the single-photon emissions, $e_b$ and $\alpha$, can be upper bounded by the decoy-state method. The phase error rate of the single-photon emissions, $e_p$, can then be upper bounded either by using the approximate bound in Eq. (26) or by solving the problem in Eq. (24). We can further utilize the result of Ref. [8], which proves the security of BB84 with an imperfect source, to find the key generation rate of the three-state protocol on the sifted key to be

$$R \leqslant -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_p)], \qquad (30)$$

where the subscript $\mu$ denotes the mean photon number for the signal states, $Q_\mu$ is the gain[2] of the signal states, $E_\mu$ is the QBER of the signal states, $Q_1$ and $e_p$ are the gains and the phase error rates of the single-photon states, $f(x)$ is the error correction efficiency as a function of error rate, and $H_2(x)$ is the binary entropy function.

Figure 3 compares the performance of the three-state protocol and the BB84 protocol by using the decoy-state method of Ref. [30]. The simulation parameters used are from the Gobby-Yuan-Shields (GYS) experiment [51], and we have used $f(E_\mu)$=1.22. Here, the phase error rate of the single-photon emissions, $e_p$, is upper bounded by solving the problem in Eq. (24). As shown in Fig. 3, the BB84 protocol is better than the three-state protocol in both the key generation rate and the maximal secure distance. Also, the slopes of both curves can be observed to be approximately the same at short and medium distances. The difference in the key generation rates for the BB84 protocol and the three-state protocol can be determined from Eq. (30). Note that for the BB84 protocol, $e_p=e_b$, while for the three-state protocol, $e_p \approx 5e_b$ (since we have $e_p=\alpha$ in this model of the QKD setup). Thus, when the mean photon numbers $\mu$ for both protocols are the same; the difference in the key generation rates is simply $Q_1[H_2(5e_b)-H_2(e_b)]$. On the other hand, when the mean photon numbers are different as in Fig. 3 where the optimal $\mu$ is always used, the difference in the key generation rates has to be calculated directly using Eq. (30).

[2]The gain of a particular state (e.g., the signal state or the single-photon state) is the probability that Alice transmits that state and Bob's result is conclusive.

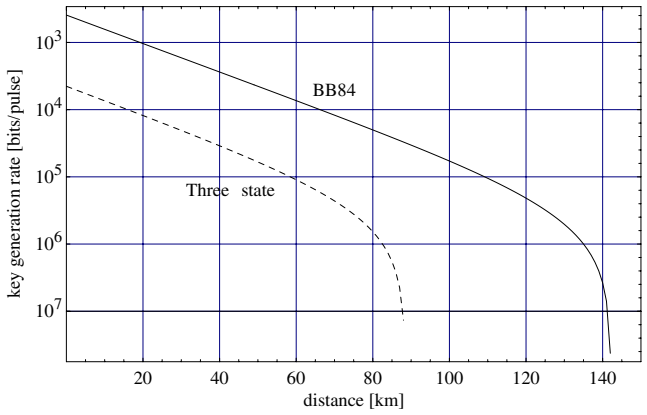


FIG. 3. (Color online) Comparison between the three-state protocol and the BB84 protocol using the decoy-state method of Ref. [30]. The two key-generation-rate curves are computed from Eq. (30). The simulation parameters used are from the Gobby-Yuan-Shields (GYS) experiment [51], and we have used $f(E_\mu)$=1.22. The optimal mean photon numbers $\mu$ for both curves are used at all distances. The maximal secure distance is 88.5 km for the three-state protocol and 142.2 km for BB84.

## V. CONCLUDING REMARKS

In this paper, we considered a three-state protocol and proved its security. Specifically, we showed how the phase error rate of the data bits is upper bounded using the bit error rates observed in the check bits. This protocol is very similar to the BB84 protocol, sharing the same three qubit states. Essentially, we showed that, by removing one state from the BB84 protocol and thus destroying the rotational symmetry, the protocol is still secure. This three-state protocol is interesting in itself since it can be easily implemented in some frequency-based QKD systems [21–23]. The result of this work is that these QKD schemes are in fact secure against the most general attacks allowed in quantum mechanics.

We compared the three-state protocol with the BB84 protocol both for the single-photon source case and the coherent source case. Specifically, for the single-photon source case, we showed that the BB84 protocol can strictly tolerate higher bit error rates than the three-state protocol. For the coherent-source case, the achievable key generation rate and maximal secure distance of the BB84 protocol are both larger than that of the three-state protocol, when the decoy-state method of Ref. [30] is used. In essence, the three-state protocol is inferior to the BB84 protocol; however, the three-state protocol does have its own merit of being easily implementable in some systems.

We may consider some variations of the three-state protocol. In the three-state protocol we analyzed, Alice sends states in the $Z$ and $X$ bases with equal probabilities. This gives rise to Bob using the same basis as Alice with a probability of 1/2, and thus half of the qubit pairs are discarded. Although not done in this paper, one may improve on this inefficiency in basis mismatch by applying the idea of efficient BB84 [50]. In the asymptotic limit, Alice and Bob use the same basis with probability approaching 1.

In the analysis we provided, we upper bound the phase error rate of the $Z$ basis states by using the average bit error

rate of the two $Z$ basis states and the bit error rate of the $|+\rangle$ state. On the other hand, it is possible to perform a more refined analysis by considering the three bit error rates separately, one for each of the states $|0_z\rangle$, $|1_z\rangle$, and $|+\rangle$. Although not addressed in this paper, such an analysis can be done in a similar manner as in this paper. In addition, one may consider a three-state protocol where the check state is not the $|+\rangle$ state, but some other state that is an unequal superposition of the $|0_z\rangle$ and $|1_z\rangle$ states, or a four-state protocol involving the same three states as our three-state protocol plus a state not on the $X-Z$ plane of the Bloch sphere [e.g., $(|0_z\rangle + i|1_z\rangle)/\sqrt{2}$]. In this case, it would be interesting to apply the same approach to analyze the security of these protocols.

*Note added*. After the first posting of our paper on the arXiv e-print server, we learned from Norbert Lütkenhaus about the existence of an independent proof of the security of the three-state protocol based on a different approach by the Geneva group. Recently, such an independent proof has appeared in Appendix A of Ref. [52].

## ACKNOWLEDGMENTS

We thank Gilles Brassard, Jim Harrington, Norbert Lütkenhaus, Bing Qi, and Renato Renner for helpful discussions. Financial support from CIAR, NSERC, CIPI, PREA, CRC program, CFI, OIT, OGSST, the Walter Sumner Memorial, and the University of Toronto is gratefully acknowledged. H.K.L. thanks the Perimeter Institute for support where this research is completed. This research was supported by the Perimeter Institute for Theoretical Physics. Research at Perimeter Institute is supported in part by the Government of Canada through NSERC and by the Province of Ontario through MEDT.

## APPENDIX: SUFFICIENCY OF USING ONE SET $\{a_I, a_X, a_Y, a_Z\}$

In this section, we show that it is sufficient to consider using only one set of $\{a_I, a_X, a_Y, a_Z\}$ in the problem in Eq. (11). The idea is to construct a new set $\{a_I, a_X, a_Y, a_Z\}$ from two existing sets $\{a_I^{(s)}, a_X^{(s)}, a_Y^{(s)}, a_Z^{(s)}\}$, where $s=1,2$, such that

$$|a_\beta|^2 = |a_\beta^{(1)}|^2 + |a_\beta^{(2)}|^2, \quad \beta = I,X,Y,Z, \tag{A1}$$

$$|ia_Y - a_Z|^2 = |ia_Y^{(1)} - a_Z^{(1)}|^2 + |ia_Y^{(2)} - a_Z^{(2)}|^2, \tag{A2}$$

$$|a_I + a_X|^2 = |a_I^{(1)} + a_X^{(1)}|^2 + |a_I^{(2)} + a_X^{(2)}|^2 \tag{A3}$$

are satisfied, meaning that the values of $\{e_b, \alpha, e_p\}$ [cf. Eqs. (11)–(13)] are preserved when the new set is used instead of the two existing ones. Note that condition (A1) already gives the magnitudes of the new $a_\beta$'s. Thus, only the phases of them remain to be found. Let us consider terms with $a_I$ and $a_X$ (the case for $a_Y$ and $a_Z$ are exactly the same). First note that we can express $|a_I+a_X|^2=|a_I|^2+|a_X|^2+2c|a_I||a_X|$, where $|c|\leqslant 1$ is a function of the phase difference between $a_I$ and $a_X$ and is what we need to determine next. Once we have found $c$, we can construct the new set by letting $a_X=|a_X|$ and $a_I = \exp(i \arccos c)|a_I|$.

To find $c$, we write condition (A3) as

$$c|a_I||a_X| = c^{(1)}|a_I^{(1)}||a_X^{(1)}| + c^{(2)}|a_I^{(2)}||a_X^{(2)}|, \tag{A4}$$

where condition (A1) has been used to eliminate the square terms. From this, we can readily get

$$c = \frac{c^{(1)}|a_I^{(1)}||a_X^{(1)}| + c^{(2)}|a_I^{(2)}||a_X^{(2)}|}{\sqrt{|a_I^{(1)}|^2 + |a_I^{(2)}|^2}\sqrt{|a_X^{(1)}|^2 + |a_X^{(2)}|^2}}, \tag{A5}$$

where we have again used condition (A1). All that is left to do is to verify that $|c|\leqslant 1$ as follows:

$$|c| \leqslant \frac{|a_I^{(1)}||a_X^{(1)}| + |a_I^{(2)}||a_X^{(2)}|}{\sqrt{|a_I^{(1)}|^2 + |a_I^{(2)}|^2}\sqrt{|a_X^{(1)}|^2 + |a_X^{(2)}|^2}} \tag{A6}$$

$$= \frac{1 + g_I g_X}{\sqrt{1+g_I^2}\sqrt{1+g_X^2}}, \tag{A7}$$

where the first inequality follows from the fact that $|c^{(1)}| \leqslant 1$ and $|c^{(2)}|\leqslant 1$, and we have used the definitions $g_I \triangleq |a_I^{(2)}|/|a_I^{(1)}|$ and $g_X \triangleq |a_X^{(2)}|/|a_X^{(1)}|$. Now, it is easy to show that the right-hand side of Eq. (A7) is less than or equal to 1. For the special case that $|a_I^{(1)}|=0$ and/or $|a_X^{(1)}|=0$, the same conclusion of $|c|\leqslant 1$ can be trivially seen.

The construction of the new $a_Y$ and $a_Z$ is similar to the above (which is for $a_I$ and $a_X$), by using conditions (A1) and (A2).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] D. Mayers, J. ACM **48**, 351 (2001), preliminary version in D. Mayers, *Advances in Crytology Proceedings of Crypto 96*, Vol. 1109 of *Lecture Notes in Computer Science*, edited by N. Koblitz (Springer-Verlag, New York, 1996), pp. 343–357.
[4] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.
[5] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] H. Inamori, N. Lükenhaus, and D. Mayers, e-print quant-ph/0107017.
[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[9] M. Koashi, e-print quant-ph/0505108.
[10] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[11] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[12] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[13] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
[14] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
[15] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, Phys. Rev. A **73**, 012337 (2006).
[16] S. Phoenix, S. Barnett, and A. Chefles, J. Mod. Opt. **47**, 507 (2000).
[17] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).
[18] M. Koashi, e-print quant-ph/0507154.
[19] D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, e-print quant-ph/0604198.
[20] J. W. Harrington (private communication).
[21] S. N. Molotkov and S. S. Nazin, J. Exp. Theor. Phys. Lett. **63**, 924 (1996).
[22] S. N. Molotkov, J. Exp. Theor. Phys. **87**, 288 (1998).
[23] B.-S. Shi, Y.-K. Jiang, and G.-C. Guo, Appl. Phys. B: Lasers Opt. **70**, 415 (2000).
[24] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
[25] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **66**, 062304 (2002).
[26] W. Tittel and G. Weihs, Quantum Inf. Comput. **1**, 3 (2001).
[27] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, e-print quant-ph/0411022.
[28] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[29] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[30] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[31] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[32] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[33] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[34] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print quant-ph/0503002.
[35] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[36] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2006* (IEEE Press, New York, 2006), pp. 2094–2098.
[37] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, e-print quant-ph/0607129.
[38] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, J. E. Nordholt, A. E. Lita, and S. W. Nam, e-print quant-ph/0607186.
[39] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[40] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[41] R. Renner, e-print quant-ph/0512258.
[42] R. Koenig and R. Renner, J. Math. Phys. **46**, 122108 (2005).
[43] M. Christandl, R. Koenig, G. Mitchison, and R. Renner, e-print quant-ph/0602130.
[44] C. D'Cruz, T. J. Osborne, and R. Schack, e-print quant-ph/0606139.
[45] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[46] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[47] J.-C. Boileau (private communication).
[48] C.-H. F. Fung *et al.* (unpublished).
[49] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).
[50] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[51] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[52] C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, e-print quant-ph/0609090.