

Unconditional Security of a Three State Quantum Key Distribution Protocol

J.-C. Boileau,¹ K. Tamaki,² J. Batuwantudawe,¹ R. Laflamme,^{1,2} and J. M. Renes^{3,4}

¹*Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*

²*Perimeter Institute for Theoretical Physics, 35 King Street North, Waterloo, Ontario, Canada N2J 2W9*

³*Department of Physics and Astronomy, University of New Mexico, Albuquerque, New Mexico 87131-1156, USA*

⁴*IAKS, Arbeitsgruppe Quantum Computing, Universität Karlsruhe, Am Fasanengarten 5, D-76131 Karlsruhe, Germany*

(Received 17 November 2004; published 31 January 2005)

Quantum key distribution (QKD) protocols are cryptographic techniques with security based only on the laws of quantum mechanics. Two prominent QKD schemes are the Bennett-Brassard 1984 and Bennett 1992 protocols that use four and two quantum states, respectively. In 2000, Phoenix *et al.* proposed a new family of three-state protocols that offers advantages over the previous schemes. Until now, an error rate threshold for security of the symmetric trine spherical code QKD protocol has been shown only for the trivial intercept-resend eavesdropping strategy. In this Letter, we prove the unconditional security of the trine spherical code QKD protocol, demonstrating its security up to a bit error rate of 9.81%. We also discuss how this proof applies to a version of the trine spherical code QKD protocol where the error rate is evaluated from the number of inconclusive events.

DOI: 10.1103/PhysRevLett.94.040503

PACS numbers: 03.67.Dd

Quantum key distribution (QKD) protocols permit two separated parties, say Alice and Bob, to construct a secret shared string of bits that may be used for cryptography. The first QKD protocol, called BB84, was invented by Bennett and Brassard in 1984 [1]. It requires Alice to randomly produce four different states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ and send them through a quantum channel to Bob who measures them randomly in the $\{|0\rangle, |1\rangle\}$ basis or in its conjugate basis $\{|+\rangle, |-\rangle\}$. The unconditional security of this protocol was first shown by Mayers in 1996 [2]. A simpler QKD protocol, B92, was proposed by Bennett in 1992 [3]. It requires Alice to produce only two nonorthogonal states, say $|\psi_1\rangle$ and $|\psi_2\rangle$, and Bob to perform the measurement described by the POVM (positive operator-valued measure) $\{\alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|, \mathbb{1} - \alpha|\bar{\psi}_1\rangle\langle\bar{\psi}_1| - \alpha|\bar{\psi}_2\rangle\langle\bar{\psi}_2|\}$, where $|\bar{\psi}_1\rangle$ and $|\bar{\psi}_2\rangle$ are orthogonal to $|\psi_1\rangle$ and $|\psi_2\rangle$, respectively, and α equals $\frac{1}{1+|\langle\psi_1|\psi_2\rangle|}$ to optimize the probability of a conclusive result to occur. Recent results by Tamaki *et al.* showed that B92 is secure for small noise, and the security threshold depends on qubit losses [4].

Phoenix *et al.* [5] postulated that the addition of a third state to the B92 protocol could considerably enhance its security and would be optimal if the three quantum states form an equilateral triangle on the X - Z plane in the Bloch sphere. We call this particular case the trine spherical code QKD protocol or the Phoenix-Barnett-Chefles 2000 (PBC00) protocol. PBC00 is similar to B92, except that Alice randomly chooses two of three states for a basis instead of using two fixed states. From Eve's point of view, the state sent by Alice is a maximally mixed state, unlike in B92. This feature is similar to BB84, in which the choice of encoding basis by Alice corresponds to a random rotation (the identity or the Hadamard transformation). In PBC00, the choice of encoding basis by Alice also corresponds to a rotation—by 120° , 240° , or none at all.

Intuitively, we could expect to find a security threshold for PBC00 that is independent of qubit losses and that is close to the one of BB84. As we will explain in detail, our security proof also applies to a slightly modified version of the PBC00 protocol proposed by Renes [6] that we refer to as R04. In this protocol, the error rate is estimated from the number of inconclusive events, and all conclusive results can be used as data bits instead of wasting some as test bits. This also simplifies the classical communication between Alice and Bob because they do not need to randomly select a set of test bits and broadcast them.

Up to now, the high error rate threshold for the security of the PBC00 protocol has been shown only in the special case of the intercept-resend attack [6]. In this Letter, we give a proof of the unconditional security of the PBC00 and R04 protocols. Assuming one-way classical communication, we show that these protocols are secure up to a bit error rate of 9.81%. In order to establish security, we first propose a QKD scheme based on an entanglement distillation protocol (EDP) [7]. This protocol uses a Calderbank, Shor, and Steane (CSS) code [8], a technique first used by Shor and Preskill in their security proof for BB84 [9]. Before running an EDP-based on CSS codes, Alice and Bob perform state rotations followed by Bob's local filtering (LF) operation [10]. The local filtering operation correlates the phase and bit error rates, as in the security proof of B92 [4]. Because of the state rotation by Alice and Bob, we achieve phase error estimation from bit error estimation. We also explain how the security of R04 follows from that of PBC00.

The PBC00 protocol involves three states $|\psi_1\rangle \equiv \frac{1}{2}|0_x\rangle + \frac{\sqrt{3}}{2}|1_x\rangle$, $|\psi_2\rangle \equiv \frac{1}{2}|0_x\rangle - \frac{\sqrt{3}}{2}|1_x\rangle$, and $|\psi_3\rangle \equiv |0_x\rangle$, where $\{|0_x\rangle, |1_x\rangle\}$ is a basis state (X basis) of a qubit state. The Z basis is defined by $\{|j_z\rangle \equiv [|0_x\rangle + (-1)^j|1_x\rangle]/\sqrt{2}\}$

($j = 0, 1$), and we also define states $|\bar{\psi}_1\rangle = \frac{\sqrt{3}}{2}|0_x\rangle - \frac{1}{2}|1_x\rangle$, $|\bar{\psi}_2\rangle = \frac{\sqrt{3}}{2}|0_x\rangle + \frac{1}{2}|1_x\rangle$, and $|\bar{\psi}_3\rangle = |1_x\rangle$ that are orthogonal to $|\psi_1\rangle$, $|\psi_2\rangle$, and $|\psi_3\rangle$, respectively. The protocol proceeds as follows.

PBC00.—(1.1) Alice creates a large trit string r and a large bit string b of the same length. For each r_i , the i th trit value of the trit string r , she chooses the set $\{|\psi_1\rangle, |\psi_2\rangle\}$ (if $r_i = 0$), $\{|\psi_2\rangle, |\psi_3\rangle\}$ (if $r_i = 1$), and $\{|\psi_3\rangle, |\psi_1\rangle\}$ (if $r_i = 2$). If the i th bit value b_i is 0, she prepares the first state of the chosen pair. If the bit is 1, she prepares the second state. Alice sends all prepared qubits to Bob.

(1.2) Bob performs a measurement described by the POVM $\{\frac{2}{3}|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \frac{2}{3}|\bar{\psi}_2\rangle\langle\bar{\psi}_2|, \frac{2}{3}|\bar{\psi}_3\rangle\langle\bar{\psi}_3|\}$. He publicly announces when all his measurements are done, and Alice in turn announces the trit string r .

(1.3) Bob regards the i th measurement outcome $|\bar{\psi}_1\rangle$ (if $r_i = 0$), $|\bar{\psi}_2\rangle$ (if $r_i = 1$), and $|\bar{\psi}_3\rangle$ (if $r_i = 2$) as the bit value 0. Similarly, he regards $|\bar{\psi}_2\rangle$ (if $r_i = 0$), $|\bar{\psi}_3\rangle$ (if $r_i = 1$), and $|\bar{\psi}_1\rangle$ (if $r_i = 2$) as the bit value 1. All other events are regarded as inconclusive. Bob announces whether his measurement outcome is inconclusive or not. Alice and Bob keep all data where Bob's outcome is conclusive, discarding the rest.

(1.4) Alice randomly chooses half of the remaining events as test bits in order to estimate the bit error rate on the code bits, and announces her selection to Bob. They compare the values of their test bits, aborting the protocol if the error rate is too high.

(1.5) By public discussion, they run classical error correction and privacy amplification protocols to share a secure secret key.

In order to prove the security of PBC00, we relate this protocol to a secure QKD based on an EDP initiated by state rotations and a LF, followed by error correction using CSS codes [9]. The LF is designed so that it probabilistically distills the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}} \times (|0_z\rangle|0_z\rangle + |1_z\rangle|1_z\rangle)$ if the filtering succeeds. Thus, the successful local filtering operation can be written by a Kraus operator $F = |0_x\rangle\langle 0_x| + \frac{1}{\sqrt{3}}|1_x\rangle\langle 1_x|$. For later convenience, we define $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle|0_z\rangle - |1_z\rangle|1_z\rangle)$, $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle|1_z\rangle \pm |1_z\rangle|0_z\rangle)$, and $R_y(2b\pi/3)$ as a $2b\pi/3$ rotation around the Y axis in the Bloch sphere. The following is the secure QKD based on an entanglement distillation protocol that is reduced to PBC00.

QKD based on EDP.—(2.1) Alice creates many pairs of qubits in the state $|\phi\rangle = \frac{1}{\sqrt{2}}(|0_z\rangle_A|\psi_1\rangle_B + |1_z\rangle_A|\psi_2\rangle_B)$, and randomly chooses a large trit string r whose length equals the number of prepared qubit pairs. She applies $R_y(2r_i\pi/3)$ on the second qubit of every pair and sends them to Bob.

(2.2) Upon receiving the i th signal state, Bob determines whether the signal is in a qubit state or not, which physically corresponds to detecting a photon or not. If it is, he declares this publicly to Alice, who in turn declares the trit

value r_i . Bob applies $R_y(-2r_i\pi/3)$ on that qubit state followed by the filtering operation. In cases where the filtering operation does not succeed or Bob receives a state that is not a qubit state, he publicly tells Alice to discard her corresponding qubits.

(2.3) Alice randomly chooses half of the remaining states as test bits and the other half as code bits, and announces her selection to Bob. For the test bits, Alice and Bob each measure their halves in the Z basis. By public discussion, they determine the number of bit errors. If the number of errors in the test bits is too high, they abort the protocol.

(2.4) By public discussion, Alice and Bob agree on an appropriate CSS code and run the EDP based on the CSS code to distill nearly perfect Bell states from the remaining qubit pairs (code pairs).

(2.5) Alice and Bob each measure the Bell pairs in the Z basis to obtain a shared secret key.

First, we reduce this EDP-based protocol into the PBC00 protocol. The reduction can be made in the manner of Shor and Preskill [9]. Their reduction technique implies that, in the context of QKD, the EDP-based on CSS codes requires Alice to perform only Z -basis measurements immediately after she has prepared the state $|\phi\rangle$ and Bob to perform only Z -basis measurements immediately after he has performed the filtering operation. The Z -basis measurement, together with Alice's rotation, is equivalent to the situation where Alice randomly sends $|\psi_1\rangle$, $|\psi_2\rangle$, or $|\psi_3\rangle$ to Bob. On Bob's side, the rotation followed by the filtering operation and Z -basis measurement is described by the following POVM:

$$\begin{aligned} &R_y(2r_i\pi/3)F^\dagger|0_z\rangle\langle 0_z|FR_y(-2r_i\pi/3), \\ &R_y(2r_i\pi/3)F^\dagger|1_z\rangle\langle 1_z|FR_y(-2r_i\pi/3), \\ &R_y(2r_i\pi/3)(\mathbb{1} - F^\dagger F)R_y(-2r_i\pi/3), \end{aligned} \quad (1)$$

which are equivalent as a set to the POVM $\{\frac{2}{3}|\bar{\psi}_1\rangle\langle\bar{\psi}_1|, \frac{2}{3}|\bar{\psi}_2\rangle\langle\bar{\psi}_2|, \frac{2}{3}|\bar{\psi}_3\rangle\langle\bar{\psi}_3|\}$, regardless of the trit value r_i . Note that failing the filtering operation is equivalent to Bob measuring $|\bar{\psi}_j\rangle$ when Alice encoded in the $\{|\psi_{j+1}\rangle, |\psi_{j+2}\rangle\}$ basis in the PBC00 protocol. This completes the reduction.

The equivalence of the two schemes allows us to use the EDP-based protocol to prove the security of PBC00. Security follows by employing a result of Shor and Preskill. They showed that if the estimations of bit and phase error rates on the code pairs are bounded, except for a failure probability that becomes exponentially small as N increases, then Eve's mutual information on the secret key also becomes exponentially small as N increases. Here, N is the number of impure qubit code pairs. Since a large number of test bits yields an exponentially reliable estimation of the bit error rate on the code pairs, we have to show only how to estimate the phase error rate from the bit error rate on the code pairs in our protocol. In the case of BB84, it is trivial to deduce that the phase error rate must equal the

bit error rate since the protocol can be interpreted as Alice and Bob measuring all the time in the bit basis, but half the time the bit errors are inverted with the phase errors. In the case of the three-state protocol, the phase error rate is five quarters of the bit error rate. However, the lack of symmetry caused by the filtering operation makes this more difficult to prove.

To make the estimation of the phase error rate, we appeal to Azuma's inequality [11]. For a brief explanation of this inequality, consider N random, but dependent, events. Let $\{p^{(l)}\}_{l=1,\dots,N}$ be the set of probabilities of having a head in coin flipping for each event. Note that $p^{(l)}$ may depend on the results of the $l-1$ previous events. Azuma's inequality tells us that if we perform all the N coin flips and if we have n_{head} head events, then the probability that the difference between n_{head}/N and $\frac{1}{N}\sum_{l=1}^N p^{(l)}$ is larger than some arbitrary small quantity drops exponentially as N increases.

Proof of our claim.—Definition: Suppose we have a series of events F_0, F_1, \dots . Let X_0, X_1, \dots be random variables. The sequence is a martingale iff the expectation of X_{i+1} conditional to events F_i, F_{i-1}, \dots, F_0 is equal to X_i for all i .

Consider the case of N coin tosses, where the probability of getting heads for each coin may be correlated in any way. Consider a series of events F_0, F_1, \dots . Let h_i be the number of heads from the events F_i, F_{i-1}, \dots, F_0 . Let X_i be $h_i - \sum_{j=1}^i p^{(j)}$ where $p^{(j)}$ is the probability of obtaining a head on the j th coin conditional on events $F_{j-1}, F_{j-2}, \dots, F_0$. The expectation of X_{i+1} conditional on events F_i, F_{i-1}, \dots, F_0 is $h_i - \sum_{j=1}^i p^{(j)}$ plus the expectation of obtaining a head on the $i+1$ coin, minus $p^{(i+1)}$. Since the expectation of obtaining a head on the $i+1$ coin minus $p^{(i+1)}$ is zero, the sequence X_0, X_1, \dots is a martingale.

Special case of Azuma's inequality: Let X_0, X_1, \dots be a martingale sequence such that for each k , $|X_k - X_{k-1}| \leq 1$. Then, for all $N \geq 0$ and any $\lambda \geq 0$,

$$\text{Pr}[|X_N - X_0| \geq \lambda] \leq 2e^{-\lambda^2/2N}.$$

In the case of coin flipping introduced above, the condition $|X_k - X_{k-1}| \leq 1$ is obviously satisfied. If we let $\lambda = N\epsilon$, then Azuma's inequality implies that

$$\text{Pr}\left[\left|\frac{h_N - \sum_{j=1}^N p^{(j)}}{N}\right| \geq \epsilon\right] \leq 2e^{-N\epsilon^2/2},$$

which proves our claim that the probability that the average number of heads differs from $\sum_{j=1}^{N-1} p^{(j)}/N$ by more than an arbitrarily small quantity, ϵ , drops exponentially as N increases. ■

For the phase error estimations, we define $\{p_{\text{bit}}^{(l)}\}_{l=1,\dots,N}$ and $\{p_{\text{phase}}^{(l)}\}_{l=1,\dots,N}$ as the sets of probabilities that Alice and Bob detect a bit error and a phase error, respectively, on the l th qubit pair after they have done the same measurements

on the $l-1$ previous pairs. Let e_{bit} and e_{phase} be, respectively, the bit and phase error rates that Alice and Bob would have obtained if they had performed bit and phase error measurements on the code pairs. Azuma's inequality tells us that if $Cp_{\text{bit}}^{(l)} = p_{\text{phase}}^{(l)}$ is satisfied for all l and a particular value of C , then we have the exponentially reliable equality $Ce_{\text{bit}} = e_{\text{phase}}$. Since e_{bit} gets exponentially closer to the bit error rate on the test bits, e_{err} , we need to find only a value for C .

Before we try to obtain C , we must assume that Eve can do any coherent attack on all the qubits sent by Alice and that she can use all the ancillary qubits she wants. We write a general equation for the state of the l th test pair depending on Eve's action. We must be careful to take into account that Alice and Bob's measurement outcomes on the previous $l-1$ test pairs might affect the measurement outcome for the l th test pair. Every qubit pair that has passed the filtering operation has undergone Alice's rotation, Eve's global operation, and Bob's rotation followed by the filtering operations. The reduced density operator of the l th qubit can be written as $\rho^{(l)} = \frac{1}{3}\sum_{b=0,1,2} |\phi_b^{(l)}\rangle\langle\phi_b^{(l)}|$, where $|\phi_b^{(l)}\rangle = \mathbb{1}_A \otimes [FR_y(-2b\pi/3)\hat{E}^{(l)}R_y(2b\pi/3)]_B|\phi\rangle$, $|\phi\rangle$ is the state created by Alice in step (2.1) before she applies a rotation, and $\hat{E}^{(l)}$ represents Eve's action restricted to the l th test pair. For simplicity, we suppose that Eve's action can be written in the form of a single matrix $\hat{E}^{(l)}$ that needs not be unitary. As it will soon be obvious, our final result still holds in the most general case, where Eve's action on the l th pair is represented by a superoperator satisfying $\sum_i \hat{E}_i^{(l)\dagger} \hat{E}_i^{(l)} \leq \mathbb{1}$. Note that $\hat{E}^{(l)}$ may depend on Eve or Alice and Bob's measurement outcome obtained from the previous $l-1$ test pairs. Also note that we summed over the different values of b , since r was selected randomly and independently of the other operations done by Alice, Eve, or Bob.

The probability of measuring a bit error on the l th test pair is $p_{\text{bit}}^{(l)} = \frac{1}{\zeta^{(l)}}(\langle\Psi^+|\rho^{(l)}|\Psi^+\rangle + \langle\Psi^-|\rho^{(l)}|\Psi^-\rangle)$ and the probability of measuring a phase error is $p_{\text{phase}}^{(l)} = \frac{1}{\zeta^{(l)}}(\langle\Phi^-|\rho^{(l)}|\Phi^-\rangle + \langle\Psi^-|\rho^{(l)}|\Psi^-\rangle)$, where $\zeta^{(l)} = (\langle\Phi^+|\rho^{(l)}|\Phi^+\rangle + \langle\Phi^-|\rho^{(l)}|\Phi^-\rangle) + (\langle\Psi^+|\rho^{(l)}|\Psi^+\rangle + \langle\Psi^-|\rho^{(l)}|\Psi^-\rangle)$ is the probability that the filtering operation succeeds on that qubit. Let us suppose that c_{11}, c_{12}, c_{13} , and c_{22} are the elements of $\hat{E}^{(l)}$ in the X basis where the c_{ij} 's are any complex numbers. Then, we easily obtain that $\frac{5}{4}p_{\text{bit}}^{(l)} = p_{\text{phase}}^{(l)}$. Thus, we have $C = \frac{5}{4}$, and by the previous argument, we conclude that the phase error rate on the code pairs, e_{phase} , asymptotically approaches $\frac{5}{4}e_{\text{bit}}$. This implies that from the measured bit error rate on the test pairs (e_{err}), Alice and Bob can not only get an estimate of the bit error rate on the code pairs (e_{bit}), but can also deduce the phase error rate on them (e_{phase}). If Eve's action is represented by a general superoperator, then the above result still holds by

linearity. Note that this argument is valid for any eavesdropping allowed by quantum mechanics because we allow $\{p_{\text{bit}}^{(l)}\}_{l=1,\dots,N}$ and $\{p_{\text{bit}}^{(l)}\}_{l=1,\dots,N}$ to be arbitrary, including any correlations, and because the $\hat{E}^{(l)}$'s are also arbitrary. Thus, our estimation is applicable to any attack, including coherent attacks.

Since we have the bit and phase error rates, we can calculate the secret key rate. The asymptotically achievable key generation rate for bit error rate e_{bit} and phase error rate e_{phase} is given by $p_{\text{conc}}[1 - h(e_{\text{bit}}) - h(e_{\text{phase}})]$, where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy [8], and p_{conc} is the probability of conclusive events. In our case, the key generation rate is given by $p_{\text{conc}}[1 - h(e_{\text{err}}) - h(\frac{3}{4}e_{\text{err}})]$. From this we find that the PBC00 protocol is secure up to $e_{\text{err}} \approx 9.81\%$, for which the key generation rate reaches 0. Contrary to the phase error estimation of B92 over the lossy and noisy channel [4], this threshold is independent of the qubit losses because, in the previous analysis, we considered only the qubits that survived the filtering operation.

In order to compare the security performance of the three-state protocol with the one of B92, BB84 and the six-state protocol (which is similar the BB84 except that Alice and Bob encode and measure in the X , the Z , and also the Y bases), we assume that Eve simulates a depolarizing channel where a qubit state ρ evolves as $(1-p)\rho + \frac{p}{3}\sum_{a=x,y,z}\sigma_a\rho\sigma_a$. Here, σ_a is the Pauli operator for a component. It is known that B92, BB84, and the six-state protocol are secure up to $p \approx 3.4\%$ [4], $p \approx 16.5\%$ [9], and $p \approx 19.1\%$ [12], respectively, while the three-state protocol is secure up to $p \approx 15.2\%$.

The above security proof also applies to the R04 protocol [6]. It is similar to the PBC00 protocol, except that the rate of inconclusive events is used to estimate the bit error rate in conclusive events, instead of using test bits in step (1.5). In the following, we explain how that is possible. As a first step, we make a clear distinction between inconclusive results caused by qubit losses and those caused by qubits that have failed the filtering operation. From now on, inconclusive events exclude the qubits lost in the channel. In PBC00, Alice randomly chooses which basis she uses before sending the state. Without threatening the security, we can modify the protocol so that she sends a random state $|\psi_j\rangle$ and waits until Bob has received it before choosing a basis. For each state, Alice can randomly pick between two bases. The one that she chooses determines which result from Bob's POVM is inconclusive and which one induces a "good" conclusive result (by good, we mean not an error). For Eve, there is no way to differentiate between the one that is inconclusive and the one that induces a good conclusive result. This implies that the number of good conclusive results approximately equals the number of inconclusive results. Define I as the fraction of inconclusive results left after discarding the lost qubits. Then, $(1 - e_{\text{bit}})(1 - I)$ is close to I , where e_{bit} represent the

error rate on all the conclusive events. More precisely, the probability that e_{bit} and $\frac{1-2I}{1-I}$ are different by more than an arbitrary quantity goes exponentially small as the number of received qubits increases. Consequently, Alice and Bob can measure the error rate of the conclusive results by counting the number of inconclusive results. Note that the fraction of conclusive results is $p_{\text{conc}} = \frac{1}{2-e_{\text{bit}}} \geq \frac{1}{2}$.

In this Letter, we have proven the unconditional security of the PBC00 and R04 protocols, the latter offering the ability to estimate the bit error rate without sacrificing test bits. Using one-way classical communication, we found an error rate threshold of 9.81%. As in the case of BB84, two-way classical communication could increase the threshold [13]. We believe that Azuma's inequality, used in our security proof, might be useful in other QKD protocol security proofs. Finally, we note that the security proof in this Letter could likely be modified to show the unconditional security of the tetrahedron spherical code recently proposed by Renes [6] or of a new three-state QKD protocol robust against collective noise [14].

The authors thank Daniel Gottesman, Hoi-Kwong Lo, and Ashwin Nayak for helpful discussions. J.C.B. and R.L. acknowledge support from NSERC and R.L. from ARDA. J.M.R. acknowledges the support of ONR Grant No. N00014-00-1-0578 and BMBF Project No. 01/BB01B.

-
- [1] 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.
 - [2] D. Mayers, in *Advances in Cryptology: Proceedings of Crypto'96*, Lecture Notes in Computer Science Vol. 1109 (Springer-Verlag, Berlin, 1996), p. 343.
 - [3] C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).
 - [4] K. Tamaki, M. Koashi, and N. Imoto, *Phys. Rev. Lett.* **90**, 167904 (2003); K. Tamaki and N. Lütkenhaus, *Phys. Rev. A* **69**, 032316 (2004).
 - [5] S. Phoenix, S. Barnett, and A. Chefles, *J. Mod. Opt.* **47**, 507 (2000).
 - [6] J. M. Renes, *Phys. Rev. A* **70**, 052314 (2004).
 - [7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996); H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).
 - [8] A. R. Calderbank and P. W. Shor, *Phys. Rev. A* **54**, 1098 (1996); A. M. Steane, *Proc. R. Soc. London A* **452**, 2551 (1996).
 - [9] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [10] N. Gisin, *Phys. Lett. A* **210**, 151 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997).
 - [11] K. Azuma, *Tôhoku Math. J.* **19**, 357 (1967).
 - [12] H.-K. Lo, *Quantum Inf. Comput.* **1**, 81 (2001).
 - [13] D. Gottesman and H.-K. Lo, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
 - [14] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, *Phys. Rev. Lett.* **92**, 017901 (2004).