Modified Bennett-Brassard 1984 quantum key distribution protocol with two-way classical communications

Kai Wen[1] and Gui Lu Long[1,2]
[1]*Key Laboratory For Quantum Information and Measurements and Department of Physics, Tsinghua University, Beijing 100084, China*
[2]*Key Laboratory for Atomic and Molecular NanoSciences, Tsinghua University, Beijing 100084, China*
(Received 19 April 2005; published 26 August 2005)

The quantum key distribution protocol without public announcement of bases is equipped with a two-way classical communication symmetric entanglement purification protocol. This modified key distribution protocol is unconditionally secure and has a higher tolerable error rate of 20%, which is higher than previous scheme without public announcement of bases.

DOI: 10.1103/PhysRevA.72.022336 PACS number(s): 03.67.Hk, 03.65.Ud, 03.67.Dd

I. INTRODUCTION

The quantum key distribution (QKD) is one of the most important and exciting fields in quantum information. Its basic idea is to make use of principles in quantum mechanics to detect whether there exists an eavesdropper Eve when two parties Alice and Bob use a quantum channel to perform the key distribution. In this way, the security is much higher than that with only classical communications. The earliest QKD protocol was proposed by Bennett and Brassard in 1984 (BB84) [1]. It is a kind of prepare-and-measure QKD protocol, a protocol that Alice first prepares a sequence of single photons, and she sends them to Bob who measures each single photon immediately after receiving it. Such kinds of protocols are much more practical because they do not require quantum computation and quantum memory.

The security of QKD protocols is a basic problem in quantum information. The BB84 protocol has been proved to be secure when the channels are noiseless. However, it was only until recently that its unconditional security has been proved. Mayers [2] and Biham *et al.* [3] presented their proofs, but the proofs are rather complex. In Mayers' proof, the BB84 protocol is secure when the error rate of the channel is less than about 7%. Shor and Preskill [4] gave a much simpler proof which guarantees the unconditional security of the BB84 protocol if the error rate is less than about 11%. And then, Gottesman and Lo [5] brought two-way classical communications to the BB84 protocol and obtained a much higher tolerable error rate, 18.9%, which makes sure that the BB84 protocol with two-way classical communications is unconditionally secure. Recently, Chau has presented a secure QKD scheme making use of an adaptive privacy amplification procedure with two-way classical communications whenever the bit error rate is less than 20.0% [6].

It is known that the standard BB84 protocol will use only half of the transmitted qubits for the key distribution. In order to enhance the efficiency of the standard BB84 protocol, many variations have been proposed. The BB84 scheme without public announcement of basis (PAB) is just such a protocol [7]. In the eavesdropping detection process of the standard BB84 protocol, Alice announces her basis string in which the qubit string is prepared only after Bob has finished receiving and measuring the qubit string. This announcement step is called PAB. PAB guarantees that Alice and Bob select the same measurement basis. However, it also leads to waste of an average of one-half of the qubits. In the BB84 protocol without PAB, the communication parties do not need PAB; instead, they agree on a secret random measurement basis sequence before any steps of the standard BB84 protocol. Alice encodes qubits according to the prior basis sequence, and Bob uses the same basis sequence to measure the qubits when he receives them. In this way, none of the measurement results will be dropped as a result of Alice and Bob choosing different measuring bases. The BB84 scheme without PAB, therefore, is still a prepare-and-measure QKD. In the information processing of this protocol, Eve knows little about the secret prior basis sequence yet, so all attacking strategies that she can use are still the same as those in the standard BB84 protocol. As a result, the security of the BB84 scheme without PAB in noiseless channels can be derived easily from the proof of the noiseless security of the standard BB84 protocol.

In this paper, we concentrate on the security of the BB84 scheme without PAB and its tolerable error rate. The protocol has been proved to be secure through noisy channels following Shor and Preskill's method [8] which obtains a tolerable error rate of 11%, the same as that of the standard BB84 protocol [4]. Recently, two-way classical communications were introduced in security proof and it increases the tolerable error rate of the standard BB84 protocol to 18.9% [5] and 20% [6], respectively. Inspired by this idea, we prove the security of the BB84 scheme without PAB with two-way classical communications. We first describe the notations in this paper in Sec. II. In Sec. III, we present a QKD protocol without PAB and with a two-way entanglement purification protocol (2-EPP) and prove its security. Then we use a theorem in Sec. IV to reduce the protocol into a prepare-and-measure protocol—that is, the BB84 scheme without PAB and with two-way classical communications—and give a detailed example in Sec. V to obtain its minimal tolerable error rate of 20%. We give a brief summary in Sec. VI.

II. NOTATIONS

The notations in this paper are mostly the same as those in the Gottesman-Lo paper [5]. A Pauli operator acting on n qubits is a n-dimensional tensor product of individual qubit operators that are of the following forms:

$$I,X=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},$$

$$Y=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\quad Z=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \tag{1}$$

where I is the identity. Note that X, Y, and Z operators are anticommutative with each other and all Pauli operators have only eigenvalues $+1$ and -1.

Bell bases are the four maximally entangled states

$$\Psi^{\pm}=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle),\quad \Phi^{\pm}=\frac{1}{\sqrt{2}}(|00\rangle\pm|11\rangle). \tag{2}$$

A *symmetric EPP* can be described with a set of operators $\{M_\mu\}$ plus unitary decoding operations $U_\mu\otimes(P_\mu U_\mu)$, where P_μ is a Pauli operator. Each M_μ is a particular measurement step of the protocol with index μ which denotes a measurement history sequence in which each bit is 0 or 1 based on the outcome of the corresponding measurement step. According to the history sequence μ, Alice and Bob should both choose the same operator M_μ to do the measurement and this is why the EPP is called symmetric. $U_\mu\otimes(P_\mu U_\mu)$ represents error correcting operations depending on μ after they obtain all error syndromes. Alice performs U_μ while Bob performs $P_\mu U_\mu$ operation.

In various symmetric EPP's, there exists a set of the EPP's in which all measurements M_μ are of eigenspaces of Pauli operators, the decoding operator U_μ is a Clifford group operator, and the error-correcting operator P_μ is a Pauli operator. These symmetric EPP's are called *stabilizer EPP's*. And if all measurements M_μ of a stabilizer EPP are either X-type (including only I and X operators) or Z-type (including only I and Z operators), and U_μ involves only controlled NOT operations, this stabilizer EPP is called a *Calderbank-Shor-Steane-like EPP* (CSS-like EPP). The CSS-like property comes from the idea of a CSS code which decouples the error correction of X and Z and guarantees the reduction in the Shor-Preskill proof of the BB84 protocol [4]. Below, all EPP's are CSS like unless noted explicitly. In CSS code, CSS (C_1,C_2) is constructed from two classical linear codes C_1 and C_2 that encode k_1 bit and k_2 bits of codewords into n-bit codewords, and $C_2\subset C_1$ and C_1 and $C_2^{\perp}$ both correct t errors.

In the EPP with one-way classical communications (1-EPP), Alice does not know the measurement results of Bob and cannot obtain the history sequence μ. Therefore, all the measurements and operations in 1-EPP are independent of μ. However, in the EPP with two-way classical communications (2-EPP), Bob can also tell Alice his measurement results through classical channels, so the communication parties can make use of the history sequence μ and choose a proper measurement operator according to the current history, and the final decoding and error-correcting operations also vary with the measurement results. In this way, the 2-EPP is supposed to tolerate a higher error rate than the 1-EPP, and we will show that introducing two-way classical communications indeed increases the tolerable error rate for the BB84 protocol without PAB.

III. QKD WITH 2-EPP WITHOUT PAB

In this section, we present a QKD protocol with 2-EPP without PAB, and prove its security through noisy channels.

Protocol 1: QKD with 2-EPP without PAB:

(1) Alice and Bob share a secret random $(2n/r)$ bit string and repeat it r times to form a basis sequence b.

(2) Alice prepares $2n$ EPR pairs in the state $(\Phi^+)^{\otimes 2n}$ and applies a Hadamard transformation to the second qubit of each EPR pair where the corresponding bit of the basis sequence b is 1.

(3) Alice sends the second half of each EPR pairs to Bob.

(4) Bob receives the qubits and publicly announces the reception.

(5) Alice randomly chooses n pairs of the $2n$ EPR pairs as check bits to check the interference of Eve.

(6) Alice broadcasts the positions of the check EPR pairs.

(7) Bob applies a Hadamard transformation to the qubits where the corresponding bit of the basis sequence b is 1.

(8) Alice and Bob both measure their own halves of the n check EPR pairs on the Z basis and publicly compare the results. If there are too many disagreements, they abort the protocol.

(9) Alice and Bob apply the 2-EPP to the remaining n EPR pairs and then share a state with high fidelity to $(\Phi^+)^m$.

(10) Alice and Bob measure the state in the Z basis to obtain a shared secret key.

In protocol 1, the idea of QKD without PAB is applied in steps 1, 2, and 7. Alice and Bob share a basis sequence b at the beginning. They can first distribute a smaller random sequence with bit length $2n/r$ by another QKD protocol or other methods, then repeat it r times. Although the basis sequence b is a repeat of a random string, if r is small and n is large enough, the information of the base sequence of Eve is still exponentially small for n and the effect of r is only to increase the information of the base sequence of Eve by multiplying polynomial of r. Therefore, we can affirm that Eve knows very little about the basis sequence.

Knowing that Eve knows very little about b, we can follow the method of Gottesman and Lo [5] to derive the unconditional security of protocol 1. First, protocol 1 is based on a stabilizer EPP; hence, the quantum channel is equivalent to a Pauli channel. Furthermore, because all operators in protocol 1 commute with each other, we can apply classical probability analysis. Calculating the probability of the success of error correcting, because Eve knows little about the basis sequence, we find that the fidelity of the state shared by Alice and Bob after the EPP to $(\Phi^+)^{\otimes m}$ is $1-2^{-s}$ for a large factor s [4]. By lemma 1 and lemma 2 in [9], Eve's mutual information with the final key is less than $2^{-c}+2^{O(-2s)}$ where $c=s-\log_2(2m+s+1/\ln 2)$. As a result, Eve's information about the final key is exponentially small and the unconditional security of protocol 1 is proved.

IV. BB84 PROTOCOL WITH TWO-WAY CLASSICAL COMMUNICATIONS WITHOUT PAB

Protocol 1 is based on the EPP which requires quantum computers to process. In this section, we will reduce protocol 1 to a prepare-and-measure protocol—that is, the BB84 pro-

tocol with two-way classical communications without PAB (2-BB84 scheme without PAB). The equivalent reduction of protocol 1 is based on the main theorem of Gottesman and Lo [5]. We revise it in a more simple way and apply it to protocol 1 as the following.

Theorem 1 (revised main theorem in [5]). Suppose a 2-EPP is CSS like and also satisfies the following conditions:

(1) If M_μ is X-type operators for a specific step with μ, for the following step with μ' ($\mu'=\mu 0$ or $\mu 1$), the choice of $M_{\mu'}$ is independent of the measurement result of M_μ—that is, $M_{\mu 0}=M_{\mu 1}$.

(2) The final decoding operations U_μ can depend arbitrarily on the outcome of the measured Z-type operators, but cannot depend on the outcomes of measured X-type operators at all. The correction operation P_μ can depend on the outcome of X-type operators, but only by factors of Z.

Then protocol 1 can be converted to a prepare-and-measure QKD without PAB scheme with the same security.

The first condition in theorem 1 is equivalent to the tree diagram representation of the first condition of the main theorem in [5]. If Alice and Bob drop the phase error, they do not know the exact result of the phase error. In order to continue the 2-EPP, they must choose the unique measurement operator in the next step despite the X-type measurement outcome. The existence of the two conditions guarantees this statement. And a CSS-like EPP makes that the corrections of bit-flip errors and phase-flip errors are separated. So Alice and Bob can perform only a bit-flip error correction and do not require quantum computers to correct phase-flip errors.

In detail, the first step is to throw away X-basis operations and measurements. The introduction of QKD without PAB in protocol 1 affects only in steps 1–7, before the error correction and privacy amplification. It only modifies the choice of base sequence, and when the EPP is proceeded, all particles are in the Z basis. Therefore, the transformation of a 2-EPP quantum circuit in [5] can be directly applied. After the transformation, Alice and Bob can obtain a classical circuit with measurements only in the Z basis.

The second step is to transform the protocol into a prepare-and-measure QKD. Following the same idea in [4], because all operations in protocol 1 commute with each other, it is not necessary for Alice to prepare and distribute EPR pairs and then measure them. Instead, Alice can measure them before distribution. In other words, Alice can just prepare a random binary string and encode it into qubits and send them to Bob. Also, Bob can measure the qubits in the basis according to the basis sequence immediately after he receives them, instead of using quantum memory to store the qubits. Thus, we can successfully transform protocol 1 into a prepare-and-measure QKD without PAB.

In the final step, in order to simplify the protocol, Alice and Bob can perform a 2-EPP to reduce the error rate of the qubits until both bit-flip and phase-flip errors are lower than the bound of the capacity of the 1-EPP. Then they can perform a 1-EPP to correct the remaining error and obtain the final secret key [5].

Consequently, we can conclude the content above into protocol 2 as the following.

Protocol 2: Secure BB84 scheme with two-way classical communications without PAB:

(1) Alice and Bob share a secret random $(2n/r)$ bit string and repeat it r times to form a basis sequence b.

(2) Alice prepares $2n$ random qubits and measures each qubit in Z basis of which the corresponding bit of b is 0 or in the X basis of which the corresponding bit of b is 1. So Alice obtains a random key and encodes it in the qubit string.

(3) Alice sends the qubit string to Bob.

(4) Bob receives these $2n$ qubit strings, measures it in the Z basis or X basis according to b, and then publicly acknowledges the receipt.

(5) Alice randomly chooses n qubits as check bits and announces their positions.

(6) Alice and Bob compare the measurement results of the check bits. If there are too many errors, they abort the protocol.

(7) Alice and Bob use a classical circuit transformed from the 2-EPP to do error correction until the error rates of both bit and phase are lower than the bound of the capacity of the BB84 protocol with one-way classical communications—for example, 11% in [4].

(8) Alice and Bob use the method in the BB84 protocol with one-way classical communications to perform final error correction and privacy amplification to obtain the key. For example, they can use the CSS code to correct errors and obtain the coset $\nu+C_2$ as the secret key [4].

According to theorem 1, protocol 2 is equivalent to protocol 1. Therefore protocol 2 is also unconditionally secure through noisy channels.

V. EXAMPLE OF A SECURE BB84 PROTOCOL WITH TWO-WAY CLASSICAL COMMUNICATIONS AND WITHOUT PAB

In Sec. III, we give the secure BB84 protocol with two-way classical communications without PAB—that is, protocol 2. However, protocol 2 is still a theoretic scheme and needs further study to exploit its capacity. In this section, a particular 2-EPP from [5] is presented and transformed to the classical circuit. We use this classical circuit in step 7 of protocol 2 so that we can estimate the lower bound of the tolerable error rate of protocol 2.

Although Theorem 1 guarantees the security of protocol 2, it is still necessary to find a practical 2-EPP that fulfills the theorem's conditions. Such a 2-EPP is presented in [5] induced from the classical error-correction theory. This 2-EPP contains alternating rounds of two major steps—that is, a bit-flip error-correction step ("B step") and phase-flip error-correction ("P step") step:

B step [5]: Alice and Bob randomly permute all the EPR pairs. Then they each measure their own local $Z\otimes Z$ in order to obtain the bit-flip error of the remaining output pair. If the results of Alice and Bob are different, they estimate that there is a bit flip on the remaining output pair and discard it. This step is similar to advantage distillation in classical communications by Maurer [10].

P step [5]: Alice and Bob randomly permute all the EPR pairs. Then they group them into sets of three, both measure X_1X_2 and X_1X_3 on each set. This step can be transformed into a circuit that first perform a Hadamard transformation on each qubit, two bilateral XOR transformations, measurement

of the last two EPR pairs, and a final Hadamard transform. If Alice and Bob disagree on one measurement, Bob estimates that the phase error was probably on the first two EPR pairs and does nothing; if both measurements disagree, Bob assumes the phase error was on the third EPR pair and corrects it by performing a Z gate. This step is induced from the three-qubit phase-flip error correcting code and will reduce the phase-flip error rate if the error rate is low enough.

The completed 2-EPP consists of alternating rounds of the two steps above. In each round, Alice and Bob first perform a B step to calculate bit-flip error syndromes. This is a Z-type measurement step. Then Alice and Bob perform a P step to calculate phase-flip error syndromes, which is an X-type measurement step. And the P step does not affect later operations. So the 2-EPP satisfies the conditions of theorem 1. After the P step, they estimate the error rate of the qubits by sacrificing some of them to measure. If the error rate is lower than the bound of the BB84 protocol with one-way classical communication—that is, about 11%—they use the Shor-Preskill method to obtain final key [4]; otherwise, they go on with another round of B and P steps.

By transforming the circuit of the 2-EPP according to theorem 1, we can get a more detailed protocol than protocol 2 as the following.

Protocol 3: secure BB84 protocol example with two-way classical communications without PAB:

(1) Alice and Bob share a secret random $(2n/r)$ bit string and repeat it r times to form a basis sequence b.

(2) Alice prepares $2n$ random qubits and measures each qubit in the Z basis in which the corresponding bit of b is 0 or in the X basis in which the corresponding bit of b is 1. So Alice obtains a random key and encodes it in the qubit string.

(3) Alice sends the qubit string to Bob.

(4) Bob receives these $2n$ qubit string, measures it in the Z basis or X according to b, and then publicly acknowledges the receipt.

(5) Alice randomly chooses n qubits as check bits and announces their positions.

(6) Alice and Bob compare the measurement results of the check bits. If there are too many errors, they abort the protocol.

(7) (B step) Alice and Bob randomly pair up their own bits. Alice publicly announces the parity (XOR) of the values of each pair of her own—that is, $x_{2i-1} \oplus x_{2i}$—and Bob also publicly announces the parity of his corresponding pair—that is, $y_{2i-1} \oplus y_{2i}$. If the parities agree, they keep one of the bits of the pair. Otherwise, they discard the whole pair.

(8) (P step) Alice and Bob randomly group the remaining bits in to sets of three and compute the parity of each set. They now regard those parities as their effective new bits in later steps.

(9) Alice and Bob sacrifice sufficient m of the new bit pairs to perform the refined data analysis publicly. They abort if the error rate is too large. And if the error rate is low enough, they go to the next step; otherwise, they return to step 7.

(10) Alice and Bob randomly permute their pairs and use the Shor-Preskill method [4] with one-way classical communications to perform final error correction and privacy amplification. In detail, it contains the following substeps:

(a) Alice and Bob select a proper CSS (C_1, C_2) code Q.

(b) Alice randomly choose a codeword u from classical linear code C_1 and announces $u+v$, where v is a remaining code bits.

(c) Bob subtracts $u+v$ from his code bits, $v+\epsilon$, and obtains $u+\epsilon$, and then corrects it to a codeword w in C_1.

(d) Because code C_2 in CSS code Q is a subgroup of F_2^n which is the binary vector space on n bits [11], and $u-w \in C_2$, Alice and Bob use the coset of $u+C_2$ as the final key.

Protocol 3 consists of detailed operations of each step, which can be studied further, for example, the tolerable error rate. Reviewing the discussion in this section, the introduction of the QKD without PAB does not affect the error correction and privacy amplification of protocol 3. Thus, we can estimate the tolerable error rate of our protocol without PAB directly from the same method in [5,6]. First, from [5], in the BB84 protocol, the 2-EPP by alternating B and P steps is successful provided that the bit error rate is lower than 17.9%. Hence, protocol 3 is secure with the same upper bound of error rate. However, Gottesman and Lo point out that alternating B and P steps is not optimal, and based on other arrangements of such two steps, the BB84 protocol can achieve higher tolerable error rate of 18.9% [5]. Moreover, by applying adaptive privacy amplification procedure with two-way classical communications in the Gottesman-Lo method, Chau obtain that a tolerable error rate of the BB84 scheme is 20.0% [6]. Such modifications in the error correcting and privacy amplification procedure can also be applied to our BB84 protocol with two-way classical communications and without PAB. In conclusion, our protocol is secure whenever the bit error rate is less than 20.0%, which is higher than the result of the BB84 protocol with only one-way classical communications and without PAB [8].

VI. CONCLUSIONS AND DISCUSSIONS

In this paper, we have proved the unconditional security of a simple modification of the standard BB84 protocol—the BB84 scheme without public announcement of bases—by applying two-way classical communications. In addition, we present a detailed protocol, protocol 3, and follow other 2-EPP procedures [5,6] to calculate a lower bound of the tolerable error rate of the protocol. The result of about 20.0% demonstrates the advantages of two-way classical communications over one-way classical communications without PAB whose tolerable error rate is about 11% [8]. Compared to the previous BB84 protocol sets, this protocol benefits from both two-way classical communications which tolerate a higher error rate and the technique without PAB which increases the key generation rate. As a result, it is much more efficient than previous protocols and can be widely used in future quantum communications.

ACKNOWLEDGMENTS

This work was supported by the National Fundamental Research Program Grant No. 001CB309308, China National Natural Science Foundation Grant Nos. 10325521 and 60433050, the Hang-Tian Science Fund, and the SRFDP program of Education Ministry of China.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computer, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[2] D. Mayers, in *Advances in Cryptology-Proceedings of Crypto '96* (Springer-Verlag, New York, 1996), p. 343.
[3] 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), p. 715.
[4] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] D. Gottesman and H.-K. Lo, e-print quant-ph/0105121.
[6] H. F. Chau, e-print quant-ph/0205060.
[7] W. Y. Hwang, I. G. Koh, and Y. D. Han, Phys. Lett. A **244**, 489 (1998).
[8] W.-Y. Hwang, X.-B. Wang, K. Matsumoto, J. Kim, and H.-W. Lee, Phys. Rev. A **67**, 012302 (2003).
[9] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[10] U. M. Maurer, in *Advances in Cryptology—Proceedings of Crypto'92* (Springer-Verlag, New York, 1993), Vol. 740, p. 461.
[11] 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).