Semiquantum-key distribution using less than four quantum states

Xiangfu Zou,[1,2] Daowen Qiu,[1,3,*] Lvzhou Li,[1] Lihua Wu,[1] and Lvjun Li[1]
[1]*Department of Computer Science, Zhongshan University, Guangzhou 510275, China*
[2]*Department of Mathematics and Physics, Wuyi University, Jiangmen 529020, China*
[3]*SQIG-Instituto de Telecomunicações, IST, TULisbon, Av. Rovisco Pais 1049-001, Lisbon, Portugal*

(Received 17 June 2008; published 12 May 2009)

Recently Boyer *et al.* [Phys. Rev. Lett. **99**, 140501 (2007)] suggested the idea of semiquantum key distribution (SQKD) in which Bob is classical and they also proposed a semiquantum key distribution protocol (BKM2007). To discuss the security of the BKM2007 protocol, they proved that their protocol is completely robust. This means that nonzero information acquired by Eve on the information string implies the nonzero probability that the legitimate participants can find errors on the bits tested by this protocol. The BKM2007 protocol uses four quantum states to distribute a secret key. In this paper, we simplify their protocol by using less than four quantum states. In detail, we present five different SQKD protocols in which Alice sends three quantum states, two quantum states, and one quantum state, respectively. Also, we prove that all the five protocols are completely robust. In particular, we invent two completely robust SQKD protocols in which Alice sends only one quantum state. Alice uses a register in one SQKD protocol, but she does not use any register in the other. The information bit proportion of the SQKD protocol in which Alice sends only one quantum state but uses a register is the double as that in the BKM2007 protocol. Furthermore, the information bit rate of the SQKD protocol in which Alice sends only one quantum state and does not use any register is not lower than that of the BKM2007 protocol.

DOI: 10.1103/PhysRevA.79.052312 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Key distribution technique is regarding two parties (Alice and Bob) to acquire a random bit sequence (i.e., key) with a high level of confidence that the others cannot know it or obtain significant partial information about it [1–3]. In 1984, Bennett and Brassard [1] invented quantum key distribution (QKD) to provide a new key distribution technique which is called the Bennett-Brassard 1984 (BB84) protocol. QKD makes use of the subtle properties of quantum mechanics such as the quantum no-cloning theorem and the Heisenberg uncertainty principle. Then, Ekert [4] presented a QKD scheme based on the Einstein-Podolsky-Rosen (EPR) pairs [5] and Bell's inequality [6]. It turned out that the key in the BB84 protocol can be seen to arise from the properties of entanglement. Bennett *et al.* [7] simplified Ekert's protocol to a protocol without invoking Bell's inequality. In 1999, Lo and Chao [2] showed that the BB84 protocol for quantum key distribution over an arbitrarily long distance of a realistic noisy channel was unconditionally secure. This proof was based on fault-tolerant quantum computers and random testing of EPR pairs. Then, in 2000, Shor and Preskill [8] proved that the BB84 protocol for quantum key distribution is secure without fault-tolerant quantum computer and without sharing EPR pairs. The unconditional security of quantum cryptography has been further discussed in [9]. It is worth noting that unconditionally security is impossible for conventional cryptography whose security is often based on unproven computational complexity assumptions. Also, the security of quantum key distribution against the most general attacks by an eavesdropper with unlimited computation abilities has been proved in [10].

One important step in studying security is to prove the protocol being robust [3]. Robustness of a protocol means that any attempt of an eavesdropper to obtain information on the key necessarily induces some error which is detectable by the legitimate users. Bennett *et al.* [7] verified that the adversary learned nothing in their protocol if his tampering could escape detection, which implies that the protocol is robust. Later, Scarani *et al.* [11] proposed a QKD protocol and showed that it is robust against the number of photons splitting attacks.

In particular, Boyer *et al.* [3] divided robustness into three classes: completely robust, partly robust, and completely nonrobust. A protocol is said to be completely robust if nonzero information acquired by Eve on the *information string* (INFO string; The definition of INFO string will be given in Step 7 of SQKD Protocol 1) implies nonzero probability that the legitimate participants find errors on the bits tested by the protocol. A protocol is said to be partly robust if Eve can acquire some limited information on the INFO string without inducing any error on the bits tested by the protocol. A protocol is said to be completely nonrobust if Eve can acquire the INFO string without inducing any error on the bits tested by the protocol. It is clear that completely robust protocols are more secure than partly robust protocols. Partly robust protocols could still be secure, but completely nonrobust protocols are automatically proven insecure [3]. Indeed, Brassard *et al.* [12] pointed out that the BB84 protocol is completely robust when qubits are used by Alice and Bob, but it is only partly robust if photon pulses are used and sometimes two-photon pulses are sent. To discuss the security of the BKM2007 protocol, Boyer *et al.* [3] proved that their protocol is completely robust.

The question of what a "quantum" protocol should be, in order to achieve a significant advantage over all classical protocols, is of great interest [3]. To answer this question in

[*] issqdw@mail.sysu.edu.cn

the field of quantum cryptography, Boyer *et al.* [3] recently suggested the idea of semiquantum key distribution (SQKD) in which Bob was classical and they invented an SQKD protocol. For convenience, we call such a protocol BKM2007. Indeed, the BKM2007 protocol has been proved to be completely robust [3].

To distribute a secret key, Alice sends four quantum states in the BB84 [1] and BKM2007 protocols [3]. However, Bennett [13] presented a QKD protocol called the Bennet 1992 (B92) protocol in which Alice sent only two nonorthogonal quantum states. Though restrictions on Alice in the B92 protocol are more strict than that in the BB84 protocol, many researchers have proved that it is still unconditionally secure [14–16]. Phoenix *et al.* [17] presented a QKD protocol called the PBC00 protocol in which Alice sent three quantum states. Also, Boileau *et al.* [18] proved that the PBC00 protocol is unconditionally secure. In addition, Mor [19] suggested a very surprising QKD scheme by using only three orthogonal pure states.

It is natural to ask whether there exists a high-secure SQKD protocol in which Alice sends less than four quantum states. Especially, is there a completely robust SQKD protocol in which Alice sends only two quantum states? In this paper, we present five different SQKD protocols in which Alice sends less than four quantum states. Furthermore, we prove that all the five protocols are completely robust.

First, we construct a completely robust SQKD protocol in which Alice sends three quantum states. Though Alice sends less quantum states in the SQKD protocol than those in the BKM2007 protocol, the proportion of *information bits* (INFO bits) in our SQKD protocol is higher than that in the BKM2007 protocol.

Then, we present two completely robust SQKD protocols in which Alice sends only two quantum states. Alice uses an N-bit register in one SQKD protocol, but she does not use any register in the other. The INFO bit proportion of the SQKD protocol in which Alice uses a register is the same as that in the BKM2007 protocol. When Alice does not use any register in the other SQKD protocol, she must send double number of quantum bits to obtain the same number of INFO bits.

Finally, we present two completely robust SQKD protocols in which Alice sends only one quantum state. Similarly, Alice uses a register in one SQKD protocol, but she does not use any register in the other. The INFO bit proportion of the SQKD protocol in which Alice uses a register is the double of that in the BKM2007 protocol. In particular, the rate of INFO bit of the SQKD protocol in which Alice sends only one quantum state and does not use any register is not lower than that of the BKM2007 protocol.

The remainder of this paper is organized as follows. In Sec. II, we present some preliminaries about semiquantum key distribution. In Sec. III, we present an SQKD protocol in which Alice sends three quantum states and we prove that it is completely robust. In Sec. IV, we first point out that it is very difficult to construct an SQKD protocol in which Alice sends only two quantum states by a mock SQKD protocol; then, we suggest a technique to remedy the weakness of the above mock protocol by Alice using a register, and we construct an SQKD protocol in which Alice sends only two quantum states, and prove that the SQKD protocol is completely robust; finally, we propose another SQKD protocol in which Alice sends only two quantum states to reform the foregoing SQKD protocol by removing the use of quantum register, and we prove that it is also completely robust. In Sec. V, we invent two SQKD protocols in which Alice sends only one quantum state to improve the two SQKD protocols in Sec. IV. Furthermore, we show that they are completely robust. To conclude, we sum up our work in Sec. VI.

II. PRELIMINARIES

In this section, we briefly recall some notations and terminologies concerning SQKD. Other notations and terminologies which we do not interpret can be found in [3,20–22].

We call Bob classical if Bob can measure, prepare, and send quantum states only in the fixed orthogonal quantum basis set $\{|0\rangle,|1\rangle\}$ [3]. Similarly, we call the fixed computational basis $\{|0\rangle,|1\rangle\}$ classical.

The setting of SQKD is as follows [3]: (1) Alice and Bob have laboratories that are perfectly secure; (2) they use qubits for their quantum communication; (3) they have access to an unjammable public classical communication channel; (4) a quantum channel leads from Alice's laboratory to the outside world and back to her; (5) Bob can access a segment of the channel, and whenever a qubit passes through that segment Bob can either let it go undisturbed or measure the qubit and send a fresh qubit in the classical $|0\rangle$ and $|1\rangle$ basis.

Statement 1. The first three postulates are the same as those in QKD protocols; the fourth and the fifth postulates are added for the SQKD protocols. Though the fourth postulate cannot be absent in SQKD protocols, it can be found in some QKD experiments too [23]. So, the fifth postulate is the essential difference between SQKD and QKD.

Theorem 1. The BKM2007 SQKD protocol is completely robust [3].

For convenience, we use $|+\rangle$ and $|-\rangle$ to denote $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, respectively. Z basis and X basis stand for the bases $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$, respectively.

III. SQKD PROTOCOL IN WHICH ALICE SENDS ONLY THREE QUANTUM STATES

We follow the BKM2007 protocol's ideas of SQKD [3], but use only three of the four BB84 states [1], as in Ref. [19], to construct an SQKD protocol described in the following.

SQKD Protocol 1: Alice sends three quantum states

(1) Alice creates an $N=6n(1+\delta)$ random string $a \in \{0,1,2\}^N$, where n is the desired length of the INFO string, and $\delta>0$ is a fixed parameter. The ith bit of a is denoted by a_i. Then, she creates and sends the quantum states $|\phi_1\rangle \otimes|\phi_2\rangle\otimes\cdots\otimes|\phi_N\rangle$, where

$$|\phi_i\rangle = \begin{cases} |0\rangle, & \text{if } a_i = 0 \\ |1\rangle, & \text{if } a_i = 1, \\ |+\rangle, & \text{if } a_i = 2. \end{cases} \qquad i = 1, 2, \ldots, N$$

(2) When each qubit arriving, Bob chooses randomly either to reflect it (CTRL it) or to measure it in the Z basis and resend it in the same state he found (SIFT it). Bob sends the first qubit to Alice after receiving the last qubit, in the same order he received them (This amounts to Alice sending a qubit only after receiving the previous one and Bob resending a qubit immediately after receiving it [3]).

(3) Alice measures each qubit in the basis she sent it.

(4) Alice announces which states were $|+\rangle$'s and Bob announces which ones he chose to SIFT. It is expected that approximate $\frac{N}{3}$ Z-SIFT bits [Z-SIFT- bits denote the bits produced by the process that Alice sends quantum states in the Z basis (in some other protocols, only state $|0\rangle$ is sent) and Bob chooses to SIFT] form the sifted key. They abort the protocol if the number of Z-SIFT bits is less than $2n$; this happens with exponentially small probability.

(5) Alice checks the error rate on the CTRL bits (CTRL bits denote the bits produced by the process that Bob chooses to CTRL). If either the X error rate or the Z error rate is higher than some predefined threshold P_{CTRL}, she and Bob abort the protocol.

(6) Alice chooses at random n Z-SIFT bits to be TEST bits. She announces which are the chosen bits. Bob announces the value of these TEST bits. Alice checks the error rate on the TEST bits. If it is higher than some predefined threshold P_{TEST}, they abort the protocol.

(7) Alice and Bob select the first n remaining Z-SIFT bits to be used as INFO bits (INFO string).

(8) Alice announces error correction code (ECC) and privacy amplification (PA) data [3,20,24–26]; Alice and Bob use them to extract the m-bit final key from the n-bit INFO string.

In this paper, similar to Z-SIFT bits, Z-CTRL bits denote the bits produced by the process that Alice sends quantum states in Z basis (in some protocols, only state $|0\rangle$ is sent) and Bob chooses to CTRL. Similarly, X-SIFT (X-CTRL) bits denote the bits produced by the process that Alice sends quantum states in X basis (in fact, only the state $|+\rangle$ is sent in all our protocols) and Bob chooses to SIFT (CTRL).

Theorem 2. The SQKD Protocol 1 is completely robust.

Proof. Because the proof of complete robustness of the BKM2007 protocol [3] does not use the state $|-\rangle$ sent by Alice, it can be used to prove the complete robustness of SQKD Protocol 1. ■

Statement 2. Though Alice sends less quantum states in our SQKD Protocol 1 than those in the BKM2007 protocol, the proportion of INFO bits in SQKD Protocol 1 has been increased and the SQKD Protocol 1 is also completely robust.

IV. TWO SQKD PROTOCOLS IN WHICH ALICE SENDS ONLY TWO QUANTUM STATES

At first glance, it seems to be a simple work to constitute an SQKD protocol in which Alice sends only two quantum states. We first describe a mock protocol which is clearly insecure. The first four steps of the mock SQKD protocol, in which Alice sends only two quantum states, is described in the next section. Recall that Z-SIFT bit, Z-CTRL bit, X-SIFT bit, and X-CTRL bit are defined as in Sec. III.

Mock SQKD Protocol: Alice sends two quantum states

(1) Alice generates a random string $a \in \{0,1\}^N$, where N is a predefined integer number. Then, she creates and sends the qubits $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle$, where

$$|\phi_i\rangle = \begin{cases} |0\rangle, & \text{if } a_i = 0 \\ |+\rangle, & \text{if } a_i = 1 \end{cases} \qquad i = 1, 2, \ldots, N.$$

After Alice sends the first qubit, she sends a qubit only after receiving the previous one.

(2) Bob generates a random string $b \in \{0,1\}^N$. When the ith qubit arriving, he chooses to SIFT it if $b_i=1$ or CTRL it if $b_i=0$. Bob denotes the measure result by c_i if he SIFT's it, otherwise, $c_i=-1$.

(3) Alice measures each qubit in the basis she sent it.

(4) Bob announces all the stations i satisfying $c_i=1$. Alice chooses at random n instances i with $c_i=1$ to generate INFO bits which must satisfy $a_i=b_i$.

At first glance, this protocol may look like a nice way to transfer secret bits from Alice to classical Bob. However, it is completely nonrobust because all bits in the INFO string satisfy $a_i=b_i=1$.

Fortunately, we have found a technique to remedy the weakness of the above mock protocol. To conquer the defect of the mock protocol, the INFO string must include 0 and 1. We can achieve it if all the X-SIFT bits become the INFO bit. It is necessary to make Alice and Bob know all X-SIFT bits. If Alice measures all qubits in Z basis after Bob announces the SIFT instances, she can know all X-SIFT bits. Also, Bob can know all X-SIFT bits if he knows which one sent by Alice is quantum state $|0\rangle$. We give an SQKD protocol using only two quantum states in the following.

SQKD Protocol 2: Alice sends two quantum states

(1) Alice generates a random string $a \in \{0,1\}^N$, where $N = 8n(1+\delta)$, n is the desired length of the INFO string, and $\delta > 0$ is a fixed parameter. Alice creates and sends qubits $|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_N\rangle$, where

$$|\phi_i\rangle = \begin{cases} |0\rangle, & \text{if } a_i = 0 \\ |+\rangle, & \text{if } a_i = 1 \end{cases} \qquad i = 1, 2, \ldots, N.$$

After Alice sends the first qubit, she sends a qubit only after receiving the previous one.

(2) Bob generates a random string $b \in \{0,1\}^N$. When the ith qubit arriving, he chooses to CTRL it if $b_i=0$ or SIFT it if $b_i=1$.

(3) Alice uses an N-qubit register to save all qubits coming back from Bob.

(4) Bob announces b after Alice receives the last qubit. Alice checks the number of X-SIFT bits. They abort the protocol if the number of X-SIFT bits is less than $2n$. This case happens with exponentially small probability.

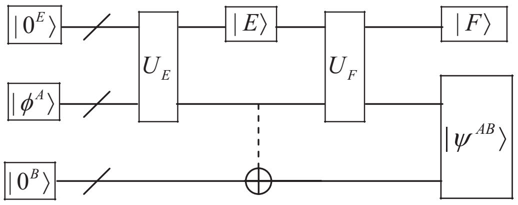

FIG. 1. The running procedure of SQKD Protocol 2.

(5) Alice measures each CTRL bit in the basis she sent it and measures each SIFT bit in the Z basis. Then, Alice checks the error rate on the CTRL bits. She and Bob abort the protocol if the error rate is higher than the predefined threshold P_t.

(6) Alice announces a. Alice and Bob check the error rate on the Z-SIFT bits. They abort the protocol if the error rate is higher than the predefined threshold P_t.

(7): Alice selects n measure results of X-SIFT bits to be TEST bits at random. Alice and Bob check the error rate on the TEST bits. They abort the protocol if the error rate is higher than P_t.

(8) Alice and Bob select the first n remaining measure results of X-SIFT bits to be used as INFO bits.

(9) Alice announces ECC and PA data; she and Bob use them to extract the m-bit final key from the n-bit INFO string.

The effect of Bob measuring a qubit in the Z basis and resending it in the same state he found is equal to the effect of Bob setting the qubit as a control bit through a CNOT gate and measuring the other qubit which is described in Fig. 1. It must be noticed that Bob's CNOT operation implements only on the stations satisfying $b_i=1$. We use $|0^E\rangle$ and $|0^B\rangle$ to denote Eve's and Bob's initial states, respectively; $|\phi^A\rangle=|\phi_1\rangle \otimes|\phi_2\rangle\otimes\cdots\otimes|\phi_N\rangle$ is Alice's sending state. Eve's attack may consist of two unitary operators U_E and U_F. U_E acts on the qubits $|\phi^A\rangle$ as they go from Alice to Bob and Eve's ancilla bits $|0^E\rangle$. And U_F acts on the qubits as they go back from Bob to Alice and Eve's ancilla bits after she uses the attack U_E. Any attack, where Eve would make U_F depending on a measurement made after applying U_E, can be implemented by unitary operators U_E and U_F with controlled gates. $|E\rangle$ and $|F\rangle$ denote Eve's states after she uses attacks U_E and U_F, respectively; $|\psi^{AB}\rangle$ is the final combining state of Alice and Bob.

In Fig. 1, we assume that the final combining state of Alice and Bob $|\psi^{AB}\rangle$ is not entangled with Eve's final state $|F\rangle$. In fact, Eve's final state $|F\rangle$ is independent of $|\psi^{AB}\rangle$ if the attack (U_E,U_F) induces no error on CTRL and TEST bits in SQKD Protocol 2, which will be justified in Lemma 1 and Lemma 2. If the attack (U_E,U_F) induces no error on CTRL and TEST bits, the final combining state of Alice and Bob $|\psi^{AB}\rangle$ is in the tensor product form $|\psi^{AB}\rangle=|\psi_1\rangle\otimes|\psi_2\rangle\otimes\cdots\otimes|\psi_N\rangle$ where

$$|\psi_i\rangle=\begin{cases} c_i|\phi_i\rangle|0\rangle, & \text{if } b_i=0 \\ c_i(x|00\rangle+y|11\rangle), & \text{if } b_i=1 \text{ and } |\phi_i\rangle=x|0\rangle+y|1\rangle, \end{cases} \tag{1}$$

and c_i is a complex number with $|c_i|=1$, $i=1,2,\ldots,N$.

Lemma 1. Alice's final state ρ'^A is a product state $\rho'^A=\rho_1'^A\otimes\rho_2'^A\otimes\cdots\otimes\rho_N'^A$ in SQKD Protocol 2. If the attack (U_E,U_F) induces no error on CTRL and TEST bits, then ρ'^A satisfies the following conditions:

(1) If $b_i=0$, then $\rho_i'^A=|\phi_i\rangle\langle\phi_i|$;

(2) If $b_i=1$, then Alice's ith final state $\rho_i'^A$ and Bob's ith final state $\rho_i'^B$ are entangled, and their combining state is

$$\rho_i'^{AB}=(x|00\rangle+y|11\rangle)(\bar{x}\langle 00|+\bar{y}\langle 11|), \text{ if } |\phi_i\rangle=x|0\rangle+y|1\rangle, \tag{2}$$

i.e.,

$$|\psi_i\rangle=c_i(x|00\rangle+y|11\rangle), \text{ if } |\phi_i\rangle=x|0\rangle+y|1\rangle, \tag{3}$$

where c_i is a complex number with $|c_i|=1$.

Proof. Because Alice sends a qubit only after receiving the previous one, the qubits she received are in the tensor product form, i.e., $\rho'^A=\rho_1'^A\otimes\rho_2'^A\otimes\cdots\otimes\rho_N'^A$.

(1) The case of $b_i=0$.

The ith bit is a CTRL bit. $\rho_i'^A\neq|\phi_i\rangle\langle\phi_i|$ can be detected by Alice as an error with some nonzero probability.

(2) The case of $b_i=1$.

The probability of the ith bit being a TEST bit is about $\frac{1}{2}$. Also, if $|\phi_i\rangle=x|0\rangle+y|1\rangle$, $\rho_i'^{AB}\neq(x|00\rangle+y|11\rangle)(\bar{x}\langle 00|+\bar{y}\langle 11|)$ can be detected by Alice and Bob as an error with some nonzero probability when the ith bit is a TEST bit. ■

By Lemma 1, we can know that the final combining state of Alice and Bob $|\psi^{AB}\rangle$ satisfies Eq. (1) if the attack (U_E,U_F) induces no error on CTRL and TEST bits in SQKD Protocol 2.

Lemma 2. If the attack (U_E,U_F) induces no error on CTRL and TEST bits in SQKD Protocol 2, then Eve's final state $|F\rangle$ is independent of the final combining state of Alice and Bob $|\psi^{AB}\rangle$.

Proof (By induction). Because Alice sends a qubit only after receiving the previous one after she sends the first one, Eve's attack can only act on one qubit every time. For convenience, we use $(U_E^{(i)},U_F^{(i)})$ to denote Eve's attack on the ith qubit. Eve does not know the value of a and b when she attacks, so Eve's attacks U_E and U_F are independent of a and b.

Basis step

We consider the effect of $(U_E^{(1)},U_F^{(1)})$ acting on the first qubit.

Case 1: $a_1=1$. By $a_1=1$, we know $|\phi_1\rangle=|+\rangle$. We denote the combining state of Eve and Alice by $x|\eta_0\rangle|0_A\rangle +y|\eta_1\rangle|1_A\rangle$ after the attack $U_E^{(1)}$ on the first qubit. Note that the effect of Bob measuring a qubit in the Z basis and resending it in the same state he found is equal to the effect of Bob setting the qubit as a control bit through a CNOT gate and measuring the other qubit. When $b_1=1$, we know that the combining state of Eve, Alice, and Bob is $x|\eta_0\rangle|00\rangle +y|\eta_1\rangle|11\rangle$ after Bob uses CNOT gate.

By the case $b_1=1$ in Lemma 1, we obtain

$$U_F(|\eta_0\rangle|00\rangle_{AB})=|\eta_0'\rangle|00\rangle_{AB} \tag{4}$$

and

$$U_F(|\eta_1\rangle|11\rangle_{AB}) = |\eta_1'\rangle|11\rangle_{AB}. \quad (5)$$

Therefore, according to the linearity of unitary operations, the combining state of Eve, Alice, and Bob is $x|\eta_0'\rangle|00\rangle + y|\eta_1'\rangle|11\rangle$ after the attack U_F. However, by the case $b_1=0$ in Lemma 1, the final combining state of Eve, Alice, and Bob is $|F_1\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}$.

Therefore,

$$x|\eta_0'\rangle|00\rangle + y|\eta_1'\rangle|11\rangle = |F_1\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (6)$$

Consequently,

$$|F_1\rangle = d_0|\eta_0'\rangle = d_1|\eta_1'\rangle, \quad (7)$$

where d_0 and d_1 are two complex numbers with $|d_0|=|d_1| =1$. By Eq. (7), we know that Eve's final state is independent of the final combining state of Alice and Bob when $a_1=1$.

Case 2: $a_1=0$. In this case, $|\phi_1\rangle=|0\rangle$. By Lemma 1, we can assume that

$$U_F^{(1)}U_E^{(1)}|0_E\rangle|00\rangle = |F_1'\rangle|00\rangle. \quad (8)$$

Note that, by the above case ($a_1=1$), we have

$$U_F^{(1)}U_E^{(1)}|0_E\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}} = |F_1\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (9)$$

By Eq. (8), Eq. (9), $|11\rangle=\sqrt{2}(\frac{|00\rangle+|11\rangle}{\sqrt{2}})-|00\rangle$, and the linearity of unitary operations, we have

$$U_F^{(1)}U_E^{(1)}|0_E\rangle|11\rangle = (|F_1\rangle - |F_1'\rangle)|00\rangle + |F_1\rangle|11\rangle. \quad (10)$$

Since $|0_E\rangle|00\rangle$ and $|0_E\rangle|11\rangle$ are orthogonal, by Eq. (8) and Eq. (10), $|F_1'\rangle|00\rangle$ and $(|F_1\rangle-|F_1'\rangle)|00\rangle+|F_1\rangle|11\rangle$ are also orthogonal. Hence, since $|F_1\rangle$ and $|F_1'\rangle$ are unit vectors, we obtain

$$|F_1'\rangle = |F_1\rangle.$$

From Case 1 ($a_1=1$) and Case 2 ($a_1=0$), we know that Eve's final state is independent of the final combining state of Alice and Bob despite the value of a_1. Thus, Eve is left with no information on the first qubit, and Eve's final state $|F_1\rangle$ and the combining state of Alice and Bob $|\psi_1\rangle$ are in tensor product form $|F_1\rangle|\psi_1\rangle$.

The Induction Step

Assume that Eve does not know any information on the first k qubits and the combining state of Eve, Alice, and Bob is $|F_1\rangle|\psi_1\rangle\otimes|F_2\rangle|\psi_2\rangle\otimes\cdots\otimes|F_k\rangle|\psi_k\rangle$ after Alice sends and receives the first k qubits.

Now, we consider the effect of $(U_E^{(k+1)},U_F^{(k+1)})$ acting on the $(k+1)$-th qubit. Because Eve has no information on the first k qubits, the effect of $(U_E^{(k+1)},U_F^{(k+1)})$ acting on the $(k+1)$-th qubit is completely similar to that of $(U_E^{(1)},U_F^{(1)})$ acting on the first one. Thereby, we can prove similarly that Eve's final state $|F_{k+1}\rangle$ is independent of the final combining state of Alice and Bob $|\psi_{k+1}\rangle$ despite the value of a_{k+1}.

Consequently, Eve does not know any information on the first $k+1$ qubits, and the combining state of Eve, Alice, and Bob is $|F_1\rangle|\psi_1\rangle\otimes|F_2\rangle|\psi_2\rangle\otimes\cdots\otimes|F_{k+1}\rangle|\psi_{k+1}\rangle$ after Alice sends and receives the first $k+1$ qubits.

Conclusion

By induction, we know that the final combining state of Eve, Alice, and Bob is $|F_1\rangle|\psi_1\rangle\otimes|F_2\rangle|\psi_2\rangle\otimes\cdots\otimes|F_N\rangle|\psi_N\rangle$, and Eve's final state $|F\rangle$ is independent of the final combining state of Alice and Bob $|\psi\rangle$. ■

Theorem 3. The SQKD Protocol 2 is completely robust: if any attack (U_E,U_F) inducing no error on TEST and CTRL bits, Eve is left with no information on the INFO string.

Proof. By Lemma 2, we can deduce easily that the SQKD Protocol 2 is completely robust. ■

In the SQKD Protocol 2, Alice uses registers for knowing all X-SIFT bits. Can we construct an SQKD protocol in which Alice sends only two quantum states and does not use any register? An SQKD protocol is described in the next section in which Alice sends only two quantum states without using any register.

SQKD Protocol 3: Alice sends two quantum states without any register

(1) Alice generates a random string $a\in\{0,1\}^N$, where $N =16n(1+\delta)$, n is the desired length of the INFO string, and $\delta>0$ is a fixed parameter. Alice creates and sends qubits

$$|\phi_i\rangle = \begin{cases} |0\rangle, & a_i=0 \\ |+\rangle, & a_i=1 \end{cases} \qquad i=1,2,\ldots,N.$$

After Alice sends the first qubit, she sends a qubit only after receiving the previous one.

(2) Bob generates a random string $b\in\{0,1\}^N$. When the ith qubit arriving, he chooses to CTRL it if $b_i=0$ or SIFT it if $b_i=1$.

(3) Alice generates a random string $c\in\{0,1\}^N$. She measures the ith bit in the Z basis if $c_i=0$ and measures the ith bit in the X basis if $c_i=1$.

For convenience, in the following, X-SIFT-Z (Z-SIFT-Z, Z-CTRL-Z) bits denote the X-SIFT (Z-SIFT, Z-CTRL) bits produced by the process that Alice measures in the Z basis. Similarly, X-CTRL-X bits denote the X-CTRL bits produced by the process that Alice measures in the X basis. It is expected that approximate $\frac{N}{8}$ X-SIFT-Z bits form the sifted key.

(4) Alice announces c and Bob announces b. They check the number of X-SIFT-Z bits. They abort the protocol if the number of X-SIFT-Z bits is less than $2n$.

(5) Alice checks the error rates on the Z-CTRL-Z, X-CTRL-X, and Z-SIFT-Z bits, respectively. She and Bob abort the protocol if any one is higher than the predefined threshold P_t.

(6) Alice chooses at random n measure results of X-SIFT-Z bits to be TEST bits. She and Bob check the error rate on the TEST bits. They abort the protocol if the error rate is higher than P_t.

(7) Alice and Bob select the first n remaining measure results of X-SIFT-Z bits to be used as INFO bits.

(8) Alice announces ECC and PA data; she and Bob use them to extract the m-bit final key from the n-bit INFO string.

Theorem 4. The SQKD Protocol 3 is completely robust.

Proof. It is similar to the proof of Theorem 3. ■

V. TWO SQKD PROTOCOLS IN WHICH ALICE SENDS ONLY ONE QUANTUM STATE

It is nature to think whether there are SQKD protocols in which Alice sends only one quantum state after constructing SQKD protocols in which Alice sends only two quantum states. By analyzing the proofs of Lemma 2 and Theorem 3, we find that the state $|0\rangle$ sent by Alice is not necessary. Therefore, we can construct an SQKD protocol in which Alice sends only one quantum state. The SQKD protocol in which Alice sends only one quantum state is described in the following.

SQKD Protocol 4: Alice sends one quantum state

(1) Alice creates and sends N qubits $|+\rangle^{\otimes N}$, where $N = 4n(1+\delta)$, n is the desired length of the INFO string, and $\delta > 0$ is a fixed parameter. After Alice sends the first qubit, she sends a qubit only after receiving the previous one.

(2) Bob generates a random string $b \in \{0,1\}^N$. When the ith qubit arriving, he chooses to CTRL it if $b_i = 0$ or SIFT it if $b_i = 1$.

(3) Alice uses an N-qubit register to save all qubits coming back from Bob. Bob announces b after Alice receives the last qubit. They abort the protocol if the number of SIFT bits is less than $2n$.

(4) Alice measures each CTRL bit in the X basis and measures each SIFT bit in the Z basis. Then, Alice checks the error rate on the CTRL bits. She and Bob abort the protocol if the error rate is higher than the predefined threshold P_t.

(5) Alice chooses at random n measure results of SIFT bits to be TEST bits. Alice and Bob check the error rate on the TEST bits. They abort the protocol if the error rate is higher than P_t.

(6) Alice and Bob select the first n remaining measure results of SIFT bits to be used as INFO bits.

(7) Alice announces ECC and PA data; she and Bob use them to extract the m-bit final key from the n-bit INFO string.

Lemma 3. If the attack (U_E, U_F) induces no error on CTRL and TEST bits in the SQKD Protocol 4, then Eve's final state $|F\rangle$ is independent of the final combining state of Alice and Bob $|\psi^{AB}\rangle$.

Proof. Observing the proof of Lemma 2, we find that it can be used to the proof of SQKD Protocol 4 if we omit the discussion of the state $|0\rangle$ sent by Alice. ■

Theorem 5. The SQKD Protocol 4 is completely robust.

Proof. It is straightforward by Lemma 3. ■

In SQKD Protocol 4, Alice uses registers for knowing all X-SIFT bits. However, in SQKD Protocol 3, Alice does not use registers. Can we construct an SQKD protocol in which Alice sends only one quantum state and does not use any register? An SQKD protocol in which Alice sends only one quantum state and does not use any register is described in the following.

SQKD Protocol 5: Alice sends only one quantum state without register

(1) Alice creates and sends N qubits $|+\rangle^{\otimes N}$, where $N = 8n(1+\delta)$, n is the desired length of the INFO string, and $\delta > 0$ is a fixed parameter. After Alice sends the first qubit, she sends a qubit only after receiving the previous one.

(2) Bob generates a random string $b \in \{0,1\}^N$. When the ith qubit arriving, he chooses to CTRL it if $b_i = 0$ or SIFT it if $b_i = 1$.

(3) Alice generates a random string $c \in \{0,1\}^N$. She measures the ith bit in the Z basis if $c_i = 0$ and measures the ith bit in the X basis if $c_i = 1$.

For convenience, in the following, SIFT-Z (SIFT-X) bits denote the bits produced by the process that Bob chooses to SIFT and Alice measures in the Z basis (X basis). Similarly, CTRL-Z (CTRL-X) bits denote the bits produced by the process that Bob choose to CTRL and Alice measures in the Z basis (X basis). It is expected that approximate $\frac{N}{4}$ SIFT-Z bits form the sifted key.

(4) Alice announces c and Bob announces b. They check the number of SIFT-Z bits. They abort the protocol if the number of SIFT-Z bits is less than $2n$.

(5) Alice checks the error rate on the CTRL-X bits. She and Bob abort the protocol if the error rate is higher than the predefined threshold P_t.

(6) Alice chooses at random n measure results of SIFT-Z bits to be TEST bits. Alice and Bob check the error rate on the TEST bits. They abort the protocol if the error rate is higher than P_t.

(7) Alice and Bob select the first n remaining measure results of SIFT-X bits to be used as INFO bits.

(8) Alice announces ECC and PA data; she and Bob use them to extract the m-bit final key from the n-bit INFO string.

Theorem 6. The SQKD Protocol 5 is completely robust.

Proof. It is similar to the proof of Theorem 5. ■

VI. CONCLUSION

In this paper, we have simplified and improved the BKM2007 protocol investigated by Boyer *et al.* [3]. We have constructed five SQKD protocols in which Alice sends less than four quantum states. To study their security, we have proved that they are completely robust. Though Alice sends less quantum states in our SQKD Protocol 1 than that in the BKM2007 protocol, the proportion of INFO bits in SQKD Protocol 1 has been increased. Alice sends only two quantum states in SQKD Protocol 2 and SQKD Protocol 3. In addition, Alice sends only one quantum state in SQKD Protocol 4 and SQKD Protocol 5. It is worth noting that Alice does not use any register in SQKD Protocol 3 and SQKD Protocol 5. In particular, though the restrictions on Alice in SQKD Protocol 5 are stricter than those in the BKM2007 protocol, in which Alice sends only one quantum state and does not use any register, the rate of INFO bits of SQKD Protocol 5 is not lower than that of the BKM2007 protocol.

The BKM2007 protocol [3] and our SQKD protocols have been discussed in the idealized scenario. An interesting problem worthy of further consideration is what they are in the practical implementation. In the practical quantum key distribution, we should consider imperfect qubits sources, noisy channels, channel losses, and detection processes as in [2,12]. We would like to explore this question in future.

ACKNOWLEDGMENTS

We would like to thank the referees for their very helpful suggestions that greatly helped to improve the quality of this paper. This work is supported in part by the National Natural Science Foundation (Grants No. 90303024, No. 60573006, and No. 60873055), the Research Foundation for the Doctorial Program of Higher School of Ministry of Education (Grant No. 20050558015), and Program for New Century Excellent Talents in University (NCET) of China and D. Qiu was partially funded by project of SQIG at IT, and FCT and EU project QSec FEDER PTDC/EIA/67661/2006.

[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] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[3] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).

[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[5] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[6] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).

[7] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

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

[9] D. Mayers, J. ACM **48**, 351 (2001).

[10] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, J. Cryptology **19**, 381 (2006).

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

[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

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

[14] Q. Zhang and C. Tang, Phys. Rev. A **65**, 062301 (2002).

[15] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003).

[16] K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004).

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

[18] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, Phys. Rev. Lett. **94**, 040503 (2005).

[19] T. Mor, Phys. Rev. Lett. **80**, 3137 (1998).

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[21] H.-K. Lo and Y. Zhao, *Quantum Cryptography, in Encyclopedia of Complexity and System Science* (Springer, New York, 2009); see also e-print arXiv:0803.2507.

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

[23] D. S. Bethune and W. P. Risk, IEEE J. Quantum Electron. **36**, 340 (2000).

[24] K. Khoo and S. Heng, in *Procedings of 2004 IEEE International Symposium on Information Theory* (IEEE, Chicago, 2004), p. 205.

[25] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[26] C. H. Bennett, G. Brassard, C. Crkpeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).