Semiquantum key distribution without invoking the classical party's measurement capability

X. Zou* D. Qiu† S. Zhang‡ P. Mateus§

Abstract

In the existing *semiquantum key distribution* (SQKD) protocols, the both parties must measure qubits in some bases. In this paper, we show that the classical party's measurement capability is not necessary by constructing an SQKD protocol without invoking the classical Alice's measurement capability. In particular, we prove the proposed SQKD protocol is completely robust against joint attacks. Compared with the existing SQKD protocols, the number of the quantum states sent by Alice and Bob is decreased.

Keywords: Quantum key distribution Semiquantum key distribution Complete robustness Joint attack Measurement capability

1 Introduction

Quantum key distribution (QKD) technique is an essential ingredient in quantum cryptography. In 1984, Bennett and Brassard [1] first suggested a protocol using quantum technique to distribute key, which is called the Bennett-Brassard 1984 protocol (BB84). After that, many QKD protocols were proposed [2, 3]. Furthermore, these QKD protocols were proved to be unconditionally secure [4, 5]. In conventional cryptography, only the

*School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China and Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, China

†Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China and The Guangdong Key Laboratory of Information Security Technology, Sun Yat-sen University, Guangzhou 510006, China

‡Department of Computer Science and Engineering, The Chinese University of Hong Kong, Hong Kong, China

§SQIG–Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa, Av. Rovisco Pais, 1049-001, Lisbon, Portugal

one-time pads encryption is unconditional security. But, the one-time pads encryption needs an encryption key which is as long as the message. By combining QKD technique with one-time pad, we can obtain unconditional secure encryption methods.

It is of great interest that using as few as possible "quantum resource" achieves a significant advantage over all classical protocols [6]. In the field of quantum cryptography, Boyer *et al.* [6] proposed the idea of *semiquantum key distribution* (SQKD) in which one participant is classical and they constructed an SQKD protocol (BKM2007). To discuss the security of BKM2007, Boyer *et al.* [6] proved that their protocol is completely robust. In BKM2007 [6], a person is called classical if he can measure, prepare and send quantum states only in the fixed orthogonal quantum basis $\{|0\rangle, |1\rangle\}$.

Because the SQKD is conceptually novel and interesting, this work has been further discussed by many scholars. Tan *et al.* [7] presented an attack on a practical implementation of SQKD. However, Boyer *et al.* [8] argued that it can resist the attack by Bob using a wave length filter. Boyer *et al.* [9] gave a strengthened proof for the complete robustness of the measure-resend SQKD protocol in Ref. [6], and presented a completely robust randomization-based SQKD protocol. In Ref. [9], both the measure-resend SQKD protocol and the randomization-based SQKD protocol were proved to be completely robust against joint attacks. In the randomization-based SQKD protocol [9], the classical Bob can measure, prepare and send qubits only in the fixed orthogonal quantum basis $\{|0\rangle, |1\rangle\}$, and reorder the qubits by using different delay lines. Lu and Cai [10] presented a QKD protocol with classical Alice and pointed out that quantum is necessary in QKD for security reasons, but both Alice and Bob may be classical. Zou *et al.* [11] proposed five SQKD protocols and proved that all of them are completely robust. In particular, two completely robust SQKD protocols were suggested in which Alice sends only one quantum state. In many follow-up research articles, the SQKD protocols in Ref. [11] have been called QKD protocols with classical Alice. Robustness proofs of these QKD protocols [11] have been improved in Refs. [12–14]. Boyer and Mor [15] proved that QKD with classical Alice [11] is still robust when photon losses and even multi-photon states are taken into account. Zhang *et al.* [16] presented an SQKD protocol to distribute secure key bits among one quantum party and numerous classical parties who have no quantum capacity, and proved that the protocol is completely robust. Wang *et al.* [17] presented a randomization-based SQKD protocol by using maximally entangled states in which quantum Alice shares a secret key with classical Bob. Recently, Yu *et al.* [18] presented an authenticated semiquantum key distribution protocols without using authen-

ticated classical channels. Krawec [19] showed that, for single-state SQKD protocols, we need only consider a restricted attack operation by Eve. Furthermore, he described a single-state protocol that permits "reflections" to carry information and used the results concerning restricted attacks to show its robustness. Yang *et al.* [20] gave a delay-photon Trojan-horse attack on BKM2007 protocol and its improvement, and further presented a possible improvement.

Note that, some applications of SQKD have been researched [21–24]. Li *et al.* [21] proposed two semiquantum secret sharing protocols using maximally entangled Greenberger-Horne-Zeilinger states. Wang *et al.* [22] presented a semiquantum secret sharing protocol by using two-particle entangled states in which quantum Alice shares a secret key with two classical parties, Bob and Charlie. Recently, Li and Qiu *et al.* [23] gave a semiquantum secret sharing protocol without using any entangled state shared. Zou and Qiu [24] constructed a three-step semi-quantum secure direct communication protocol in which the sender Alice is classical.

SQKD protocols can be carried out easily because the classical party needs only classical abilities. This means that the classical party only needs to use very simple quantum devices (the preparation, measurement, and emission devices can work only with the fixed quantum basis $\{|0\rangle, |1\rangle\}$). Similarly, further restricting the ability of the classical party is also a very interesting problem.

Note that, in the measure-resend SQKD protocol [6], the classical party can measure, prepare and send quantum states only with the fixed orthogonal quantum basis $\{|0\rangle, |1\rangle\}$. In addition, the classical party adds the ability of reordering qubits in the randomization-based SQKD protocol [9]. In other SQKD protocols [10, 11, 16–19], the abilities of the classical party are limited as that in Refs. [6, 9]. Therefore, in existing SQKD protocols [6, 9–11, 16–19], the classical party must measure qubits in the classical basis $\{|0\rangle, |1\rangle\}$.

In this paper, we will further restrict the abilities of the classical party. We will construct an SQKD protocol without invoking the classical party Alice's measurement capability, and also prove it to be completely robust against quantum joint attacks. This shows that the measurement capability of the classical party is not necessary in semiquantum key distribution. In other words, to implement the proposed SQKD protocol, the classical party does not need any quantum measuring device.

The remainder of this paper is organized as follows. First, in Section 2, we present some preliminaries about SQKD. Then, in Section 3, we construct an SQKD protocol without invoking the classical party's measure-

ment capability, and point out its implementation complexity is decreased. Furthermore, in Section 4, we prove the proposed SQKD protocol to be completely robust against joint attacks. Finally, we make a conclusion in Section 5.

2 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 [6, 9, 11, 25].

2.1 The setting of semiquantum key distribution

As everyone knows, if a person is restricted to use only the quantum states in the fixed computational basis $\{|0\rangle, |1\rangle\}$ (no any unitary operation), he/she can only get classical computing power. Thereby, we call the fixed computational basis $\{|0\rangle, |1\rangle\}$ classical. If all parties of a QKD protocol were limited to perform only the operations: (1) measure the qubit in the classical $\{|0\rangle, |1\rangle\}$ basis, (2) prepare a (fresh) qubit in the classical basis and send it, (3) reorder the qubits (by using different delay lines, for instance), or do nothing, they would always be working with qubits in the classical basis and could never obtain any quantum superposition of the computational-basis states; the qubits can then be considered "classical bits"; the resulting protocol would then be equivalent to an old-fashion classical protocol, and therefore, the operations themselves shall here be considered classical. We term this kind of protocol, in which one or more participants are limited to perform only the operations (1)–(3) or do nothing, as "QKD protocol with classical party" or semiquantum key distribution (SQKD) [9].

In the *measure-resend* SQKD protocol [6, 9], a quantum channel leads from the quantum Alice's lab to the outside world and back to her lab. The classical Bob in the protocol [6] can access a segment of the channel, and whenever a qubit passes through that segment Bob can either let it go undisturbed or (1) measure the qubit in the classical $\{|0\rangle, |1\rangle\}$ basis and (2) prepare a (fresh) qubit in the classical basis and send it.

In the *randomization-based* SQKD protocol [9], there is also a quantum channel leading from the quantum Alice's lab to the outside world and back to her lab. The classical Bob can also access a segment of the channel, and whenever a qubit passes through that segment he can either let it go undisturbed or (1) measure the qubit in the classical $\{|0\rangle, |1\rangle\}$ basis; (3) reorder the qubits.

Similarly, in the other SQKD protocols [10, 11, 16–19], the classical party needs to measure some quantum states in the classical $\{|0\rangle, |1\rangle\}$ basis.

In this paper, we follow the ideas of the SQKD protocols [6, 9–11, 16–19], but remove the classical party's measurement capability, to set the setting of SQKD as follows: (1) the classical Alice and the quantum Bob have labs 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 Bob's lab to the outside world and back to his lab, (5) the classical Alice can access a segment of the channel, and whenever the qubits passes through that segment Alice can prepare some new qubits in the classical basis $\{|0\rangle, |1\rangle\}$, reorder all qubits including the incoming qubits and the preparing ones, and send them back to Bob.

Note that, the fifth postulate does not include the classical party's measurement capability.

Statement 1 [11].—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 can not be absent in SQKD protocols, it can be found in some QKD experiments too [26–28]. So, the fifth postulate is the essential difference between SQKD and QKD.

2.2 Robustness

One important step in studying security is to prove the protocol being robust [6, 9, 11]. 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.* [3] 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.* [29] proposed a QKD protocol and showed that it is robust against the number of photons splitting attacks.

In particular, Boyer *et al.* [6] divided robustness into three classes: completely robust, partly robust, and completely nonrobust. A protocol is called completely robust if nonzero information acquired by Eve on the information string (INFO string) implies nonzero probability that the legitimate participants find errors on the bits tested by the protocol. A protocol is called 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 called 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 securer than partly robust protocols. Partly

robust protocols could still be secure, but completely nonrobust protocols are automatically proven insecure [6]. Indeed, Brassard *et al.* [30] pointed out that BB84 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 BKM2007, Boyer *et al.* [6] proved that their protocol is completely robust. Similarly, the other SQKD protocols [9–11, 16–19] are showed to be completely robust.

3 An SQKD protocol without the classical Alice's measuring

We employ the ideas of the SQKD protocols [6, 9–11, 16–19], but remove the classical party's measurement capability, to construct an SQKD protocol in which Alice is classical and Bob is quantum. Let n be the desired length of the INFO string. The proposed SQKD protocol depends on a parameter δ with $\delta > 0$. For convenience, we use $|+\rangle$ and $|-\rangle$ to denote $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, respectively; Z basis and X basis stand for the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, respectively. The proposed SQKD protocol, in which Alice does not need to measure any quantum state, is described in the following.

SQKD Protocol: Alice does not need to measure

(1) Quantum Bob sends $N = \lceil 4n(1+\delta) \rceil$ qubits, which are randomly selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, to classical Alice.

(2) When the qubits arrive, Alice selects M ($M \geq N$) qubits randomly in the set $\{|0\rangle, |1\rangle\}$, and randomly reorders all qubits including that received from Bob and that inserted by her. Then, she sends the first $2N$ qubits $|\psi\rangle$ to Bob. For convenience, in $|\psi\rangle$, we call the qubits received from Bob *CTRL qubits* and the qubits inserted by Alice *SIFT qubits*.

Note that, in this step, Alice only uses preparing, sending, intercepting, and reordering operations but measuring operation.

(3) Bob measures each qubit randomly with Z basis or X basis.

(4) Alice publishes the order of the qubit string $|\psi\rangle$ by the classical channel and Bob announces publicly the positions which he measured with Z

basis. Z-SIFT bits denote the bits produced by Bob using Z basis to measure the SIFT qubits. It is expected that there are approximate $\frac{N}{2}$ Z-SIFT bits which form the sifted key. They abort the protocol if the number of Z-SIFT bits is less than $2n$.

(5) Bob checks the error rate on the CTRL qubits. In this case, Bob's measurement results must be the same as he sent because Alice does not perform any other operation on it except the ordering. If the error rate is higher than some predefined threshold P_{CTRL}, Alice and Bob abort the protocol.

(6) Bob chooses at random n Z-SIFT bits to be TEST bits, and announces what are the chosen bits and the value of these TEST bits by the classical channel. Bob's measurement results must be the states sent by Alice. 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 publicly the error correction code (ECC) and privacy amplification data [6, 31–33]; Alice and Bob use them to extract the m-bit final key from the n-bit INFO string.

The essential difference between the proposed SQKD protocol and the prior SQKD protocols [6, 9–11, 16, 17] is that the classical party does not measure any quantum state in the proposed SQKD protocol. In addition, to share n INFO bit by the proposed SQKD protocol, the number of the quantum states sent by Alice and Bob is decreased. In the proposed SQKD, the quantum Bob needs to send only half quantum states as usual, because the classical Alice does not need to measure quantum states. Compared with the SQKD protocol in which Alice sends only one kind of quantum state and does not use quantum register in Ref. [11], the number of the quantum states sent by the quantum party is decreased 50% and the total number of the quantum states sent by two parties is decreased 25%. Note that, the rate of information bits of the SQKD protocol, in which Alice sends only one kind of quantum state and does not use quantum register in Ref. [11], is not lower than that of the BKM2007 protocol [6]. The whole communications traffic of the proposed SQKD protocol is just as that of the randomization-based SQKD protocol. As the discussion in Ref. [11], Alice and Bob can decrease

the numbers of the sent quantum states in the proposed SQKD protocol 50% if Bob uses a quantum register.

4 The robustness proof of the proposed SQKD protocol

One important step in studying security is to prove the protocol being robust [6]. Robustness of a protocol means that any attempt of an eavesdropper to obtain any information on the key necessarily induces some error which is detectable by the legitimate users. For example, Bennett *et al.* [3] showed that the adversary learned nothing in their protocol if his tampering could escape detection. Scarani *et al.* [29] proved that their QKD protocol is robust against the number of photons splitting attacks. In particular, Boyer *et al.* [6] divided robustness into three classes: completely robust, partly robust, and completely nonrobust. A QKD or SQKD protocol is called completely robust if nonzero information acquired by an eavesdropper on the INFO string implies nonzero probability that the legitimate participants can find errors on the TEST bits. To discuss the security, Boyer *et al.* [6, 9] proved their SQKD protocols are completely robust. Also, we will show the proposed SQKD protocol is completely robust against joint attacks [25, 34]. The last step of the proposed SQKD protocol must be excluded from the definition of robustness or else no protocol would ever be robust unless the ECC is degenerate and unable to correct any error [8].

Gisin *et al.* [25] divided the eavesdropping strategies on quantum cryptography into three classes: individual attack, collective attack, and joint attacks. In the individual attack, the attacker Eve attaches independent probes to each qubit and measures her probes one after the other. The individual attack is also called the incoherent attack. In general, we call the collective attack and the joint attack coherent attacks. The coherent attacks are first suggested and discussed by Biham and Mor [34]. In the collective attack, the attacker Eve attaches one probe per qubit, as in individual attacks, but can measure several probes coherently. The most general attacks are called joint attacks in which Eve attaches several probes coherently and measures several probes coherently. It is clear that the joint attack is not less efficient than the individual attack and the collective attack.

We use $|A\rangle = |A_1\rangle \otimes |A_2\rangle \otimes \cdots \otimes |A_M\rangle$ with $|A_i\rangle \in \{|0\rangle, |1\rangle\}$, $|B\rangle = |B_1\rangle \otimes |B_2\rangle \otimes \cdots \otimes |B_N\rangle$ with $|B_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to denote Alice's and Bob's initial states, respectively. And, the $2N$ qubits string $|E\rangle$ denotes the attacker Eve's initial state. Without loss of generality, we can suppose

$|E_i\rangle = |0\rangle$, $i = 1, 2, \ldots, 2N$.

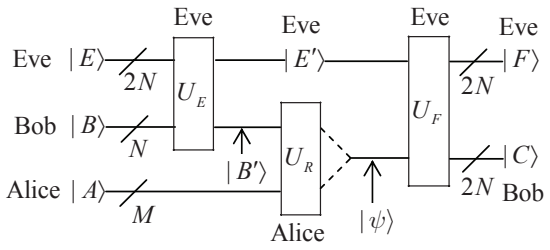

Figure 1: The running procedure and the attacks of the proposed SQKD protocol.

Because the proposed SQKD protocol is a two-way communication protocol, Eve's most general attacks can be described by two unitary operators U_E and U_F as in Fig. 1. $|E'\rangle$ and $|F\rangle$ denote Eve's states after she uses attacks U_E and U_F, respectively. And, $|B'\rangle$ and $|C\rangle$ denote the state Alice received after the attack U_E and the Bob's final state after the attack U_F, respectively. U_E acts on the qubits $|B\rangle$ as they go from Bob to Alice and Eve's ancillary bits $|E\rangle$. And, U_F acts on $|E'\rangle$ and $|\psi\rangle$ where $|\psi\rangle$ is the first $2N$ qubits Alice obtained by reordering $|A\rangle$ and $|B'\rangle$. As pointed out in Ref. [6], the shared probe allows Eve to make the attack on the returning qubits depend on the knowledge acquired by U_E (if Eve does not take advantage of that fact, then the "shared probe" can simply be the composite system comprised of two independent probes). Any attack where Eve would make U_F depend on a measurement made after applying U_E can be implemented by unitaries U_E and U_F with controlled gates.

Note that, Eve does not know the order of the qubit string $|\psi\rangle$ which Alice sends to Bob before Alice announces it publicly. By tracing through the execution of the protocol, one can determine that the global state of the Eve-Bob-Alice system before the measurements is

$$[U_F \otimes I_{2^{M-N}}][I_E \otimes U_R][U_E \otimes I_A](|E\rangle|B\rangle|A\rangle), \tag{1}$$

where U_R denotes the reordering operation applied by Alice.

In Fig. 1, we assume that the Eve's final state $|F\rangle$ is not entangled with Bob's final state $|C\rangle$. In fact, Eve's final state $|F\rangle$ is independent of $|C\rangle$ if the attack (U_E, U_F) induces no error on Alice's and Bob's test in the proposed SQKD protocol. This will be justified in Lemma 1.

Lemma 4.1 *If the attack (U_E, U_F) induces no error on the test of CTRL and SIFT qubits in the proposed SQKD protocol, then $|C\rangle$ satisfies the followings:*

(1) If $|C_i\rangle$ is a CTRL qubit and the ith particle of $|\psi\rangle$ is Bob's jth particle, then $|C_i\rangle = c|B_j\rangle$, i.e., Bob's ith final state is his initial state $|B_j\rangle$ (ignore the global factor c);

(2) If $|C_i\rangle$ is a SIFT qubit and $|\psi_i\rangle$ is Alice's jth initial qubit, then $|C_i\rangle = c'|A_j\rangle$, i.e., Bob's ith final state is Alice's jth initial state $|A_j\rangle$ (ignore the global factor c');

(3) The final global state of the Eve-Bob-Alice system is $|F\rangle|C\rangle$ and $|C\rangle$ the first $2N$-qubit-string of $U_R(|B\rangle|A\rangle)$ (ignore some global factor).

Proof: (1) In this case, $|C_i\rangle$ is a CTRL qubit. It is in $\frac{1}{2}$ probability that Bob measures the qubit with X basis. When the ith particle of $|\psi\rangle$ is Bob's jth particle, Bob's final quantum state $|C_i\rangle \neq c|B_j\rangle$ can be detected by Bob as an error with some non-zero probability in Step (5). Thereby $|C_i\rangle = c|B_j\rangle$.

(2) $|C_i\rangle$ is a SIFT qubit. It is in $\frac{1}{2}$ probability that Bob measures the qubit in Z basis. The probability of the Z-SIFT bit being a TEST bit is about $\frac{1}{2}$. Also, $|C_i\rangle \neq c'|A_j\rangle$ can be detected by Alice and Bob as an error with some non-zero probability in Step (6). Therefore $|C_i\rangle = c'|A_j\rangle$.

(3) By the conclusions (1) and (2) above, the final global state of the Eve-Bob system is $|F\rangle|C\rangle$ and $|C\rangle$ the first $2N$-qubit-string of $U_R(|B\rangle|A\rangle)$ (ignore some global factor). QED

Lemma 4.2 *Let $|B\rangle$ satisfy $|B_i\rangle \in \{|0\rangle, |1\rangle\}$, for any $i = 1, 2, \ldots, N$. If the attack (U_E, U_F) induces no error on the test of CTRL and SIFT qubits in the proposed SQKD protocol, then the global state of the Eve-Alice system after the attack U_E is $|E'\rangle \otimes |B'\rangle$ and $|B'\rangle = |B\rangle$.*

Proof: To show the combined state of $|E'\rangle$ and $|B'\rangle$ is a product state $|E'\rangle \otimes |B'\rangle$, we only need to show all qubits in $|B'\rangle$ and $|E'\rangle$ are formed into product states.

After Eve applies the attack U_E on $|B\rangle$, the combined state of Eve-Bob system changes to

$$U_E(|E\rangle|B\rangle) = \sum_{S\in\{0,1\}^N} a_S|\eta_S\rangle|S\rangle. \tag{2}$$

Now, we consider the ith particle sent by Bob being the state $|0\rangle$, for any $i \in \{1, 2, \ldots, N\}$. Since we only focus on the ith qubit, we trace out the other qubits sent by Bob on Eq. (2) and get

$$U_E(|E\rangle|0\rangle) = a|\eta_0\rangle|0\rangle + b|\eta_1\rangle|1\rangle. \tag{3}$$

After the attack U_F acts on them (trace out the other particles sent by Bob and Alice), we get

$$U_F U_E(|E\rangle|0\rangle) = aU_F(|\eta_0\rangle|0\rangle) + bU_F(|\eta_1\rangle|1\rangle). \tag{4}$$

When the qubit sent by Bob is a CTRL qubit, the measurement result must be $|0\rangle$. Accordingly, there is some $|\zeta\rangle$ such that

$$U_F U_E(|E\rangle|0\rangle) = |\zeta\rangle|0\rangle. \tag{5}$$

Now we consider Alice intercepts Bob's particle and sent a particle in the state $|0\rangle$ in Step (2). The global state of Eve-Alice system changes to $a|\eta_0\rangle|0\rangle|0\rangle + b|\eta_1\rangle|0\rangle|1\rangle$ where the first particle is held by Eve, the second particle inserted and sent by Alice, and the third particle sent by bob and intercepted by Alice. After Eve applies the attack U_F, the global final state of Eve-Bob-Alice system (trace out the other particles held by Bob and Alice) changes to

$$\begin{aligned}&[U_F \otimes I_2](a|\eta_0\rangle|0\rangle|0\rangle + b|\eta_1\rangle|0\rangle|1\rangle)\\ &\qquad = aU_F(|\eta_0\rangle|0\rangle)|0\rangle + bU_F(|\eta_1\rangle|0\rangle)|1\rangle.\end{aligned} \tag{6}$$

The measurement result of the second particle must be the state $|0\rangle$ sent by Alice. Therefore,

$$U_F(|\eta_0\rangle|0\rangle) = |\eta_0'\rangle|0\rangle \tag{7}$$

and

$$U_F(|\eta_1\rangle|0\rangle) = |\eta_1'\rangle|0\rangle. \tag{8}$$

Similarly, when Alice intercepts Bob's particle and sent a particle being the state $|1\rangle$ in Step (2), the global state of Eve-Alice system changes to $a|\eta_0\rangle|1\rangle|0\rangle + b|\eta_1\rangle|1\rangle|1\rangle$ where the first particle is held by Eve, the second particle inserted and sent by Alice, and the third particle sent by Bob and intercepted by Alice. After Eve applies the attack U_F, the global final state of Eve-Bob-Alice system (trace out the other particles held by Bob and Alice) evolves into

$$\begin{aligned}&[U_F \otimes I_2](a|\eta_0\rangle|1\rangle|0\rangle + b|\eta_1\rangle|1\rangle|1\rangle)\\ &\qquad = aU_F(|\eta_0\rangle|1\rangle)|0\rangle + bU_F(|\eta_1\rangle|1\rangle)|1\rangle.\end{aligned} \tag{9}$$

The measurement result of the second particle must be the state $|1\rangle$ sent by Alice. Therefore,

$$U_F(|\eta_0\rangle|1\rangle) = |\eta_0''\rangle|1\rangle \tag{10}$$

and

$$U_F(|\eta_1\rangle|1\rangle) = |\eta_1''\rangle|1\rangle. \tag{11}$$

Combining Eqs. (7) and (11), we obtain

$$\begin{aligned} U_F U_E(|E\rangle|0\rangle) &= aU_F(|\eta_0\rangle|0\rangle) + bU_F(|\eta_1\rangle|1\rangle) && (12)\\ &= a|\eta_0'\rangle|0\rangle + b|\eta_1''\rangle|1\rangle. && (13) \end{aligned}$$

Contrasting Eq. (13) with Eq. (5), we get $b = 0$. Accordingly,

$$U_E(|E\rangle|0\rangle) = a|\eta_0\rangle|0\rangle. \tag{14}$$

Similarly, when Bob sends the ith particle in the state $|1\rangle$, for any $i \in \{1, 2, \ldots, N\}$, we can trace out the other particles sent by Bob and get

$$U_E(|E\rangle|1\rangle) = b|\eta_1\rangle|1\rangle. \tag{15}$$

Combining Eqs. (14) and (15), every qubit in $|B'\rangle$ is the same state in $|B\rangle$ and it composes a product state with $|E'\rangle$. Thereby, the combined state of $|E'\rangle$ and $|B'\rangle$ is a product state $|E'\rangle \otimes |B'\rangle$ and $|B'\rangle = |B\rangle$. QED

One can no longer expect the Eve-Alice system after the attack U_E on $|E'\rangle \otimes |B\rangle$, for any B with $|B_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

Example 4.3 *Let* $\Theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$, $U_E = I_{2N} \otimes \Theta^{\otimes N}$ *and* $U_F = I_{2N} \otimes (\Theta^\dagger)^{\otimes 2N}$. *Then, the Eve-Alice system after the attack* U_E *is not* $|E'\rangle \otimes |B\rangle$ *and the attack* (U_E, U_F) *induces no error on the test of CTRL and SIFT qubits in the proposed SQKD protocol.*

Lemma 4.4 *Bob sends* $|B\rangle$ *or* $|\hat{B}\rangle$ *in Step 1 with* $|B_i\rangle, |\hat{B}_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, *for any* $i = 1, 2, \ldots, N$; *Alice inserts any state* $|A\rangle \in \{|0\rangle, |1\rangle\}^M$ *and uses any ordering operation* U_R *in Step 2. Let* $|F\rangle$ *and* $|\hat{F}\rangle$ *denote Eve's final state after she attacks on* $(U_R, |B\rangle, |A\rangle)$ *and* $(U_R, |\hat{B}\rangle, |A\rangle)$, *respectively. If the attack* (U_E, U_F) *induces no error on the test of CTRL and SIFT qubits in the proposed SQKD protocol, then* $|F\rangle = |\hat{F}\rangle$.

Proof: To show this conclusion, by the linearity of the unitary operators, we only need to show Eve's final states after she attacks on $(U_R, |S\rangle, |A\rangle)$ and $(U_R, |\hat{S}\rangle, |A\rangle)$ are equal, for any $S, \hat{S} \in \{0, 1\}^N$.

For any $S, \hat{S} \in \{0, 1\}^N$ with $H(S \oplus \hat{S}) = l \geq 1$, there exists a chain

$$S = S^{(0)}, S^{(1)}, \ldots, S^{(l)} = \hat{S} \tag{16}$$

satisfying $H(S^{(i-1)} \oplus S^{(i)}) = 1$, for any $i = 1, 2, \ldots, l$. Therefore, to show Eve gets the same information after applying the attack (U_E, U_F) on $(U_R, |S\rangle, |A\rangle)$ and $(U_R, |\hat{S}\rangle, |A\rangle)$ for any two $S, \hat{S} \in \{0,1\}^N$, we only need to show Eve gets the same information after applying the attack (U_E, U_F) on $(U_R, |S\rangle, |A\rangle)$ and $(U_R, |\hat{S}\rangle, |A\rangle)$ with $H(S \oplus \hat{S}) = 1$.

For any two $S, \hat{S} \in \{0,1\}^N$ with $H(S \oplus \hat{S}) = 1$, let $|F\rangle$ and $|\hat{F}\rangle$ denote Eve's final states after she attacks on $(U_R, |S\rangle, |A\rangle)$ and $(U_R, |\hat{S}\rangle, |A\rangle)$, respectively. By Lemma 2, we can suppose

$$U_E(|E\rangle|S\rangle) = |E'\rangle|S\rangle \tag{17}$$

and

$$U_E(|E\rangle|\hat{S}\rangle) = |\hat{E}'\rangle|\hat{S}\rangle. \tag{18}$$

Since $H(S \oplus \hat{S}) = 1$, there exists a $k \in \{1, 2, \ldots, N\}$ such that $S_k = 0$, $\hat{S}_k = 1$ and $S_i = \hat{S}_i$, for any $i = 1, 2, \ldots, N$ with $i \neq k$. Let $|\tilde{S}\rangle$ satisfy $|\tilde{S}_k\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\tilde{S}_i\rangle = |S_i\rangle$, for any $i = 1, 2, \ldots, N$ with $i \neq k$. Then $|\tilde{S}\rangle = \frac{1}{\sqrt{2}}(|S\rangle + |\hat{S}\rangle)$. After U_E attacks on $|\tilde{S}\rangle$, the combined state of Eve-Alice system is

$$U_E(|E\rangle|\tilde{S}\rangle) = \frac{1}{\sqrt{2}}(|E'\rangle|S\rangle + |\hat{E}'\rangle|\hat{S}\rangle). \tag{19}$$

For any reordering operator U_R,

$$\begin{aligned}
&[U_F \otimes I_{M-N}][I_E \otimes U_R][U_E \otimes I_A](|E\rangle|\tilde{S}\rangle|A\rangle) \\
&= \frac{1}{\sqrt{2}}[U_F \otimes I_{M-N}][I_E \otimes U_R](|E'\rangle|S\rangle|A\rangle + |\hat{E}'\rangle|\hat{S}\rangle|A\rangle) &(20)\\
&= \frac{1}{\sqrt{2}}[U_F \otimes I_{M-N}][|E'\rangle U_R(|S\rangle|A\rangle) + |\hat{E}'\rangle U_R(|\hat{S}\rangle|A\rangle)] &(21)\\
&= \frac{1}{\sqrt{2}}[|F\rangle U_R(|S\rangle|A\rangle) + |\hat{F}\rangle U_R(|\hat{S}\rangle|A\rangle)]. &(22)
\end{aligned}$$

Since we are interested in the kth qubit in Alice's and Bob's hands, we trace out the other qubits in Alice's and Bob's hands on Eq. (22), and get

$$\begin{aligned}
&[U_F \otimes I_{M-N}][I_E \otimes U_R][U_E \otimes I_A](|E\rangle|\tilde{S}\rangle|A\rangle) \\
&\quad = \frac{1}{\sqrt{2}}(|F\rangle|0\rangle + |\hat{F}\rangle|1\rangle) &(23)\\
&\quad = \frac{1}{2}[(|F\rangle + |\hat{F}\rangle)|+\rangle + (|F\rangle - |\hat{F}\rangle)|-\rangle]. &(24)
\end{aligned}$$

When this qubit in Bob's hands is a CTRL qubit, the measurement result must be the state $|+\rangle$ as he sent. Accordingly,

$$|F\rangle = |\hat{F}\rangle. \tag{25}$$

By Eq. (25), we have finished the proof. QED

Lemma 4.5 *Let $C, \hat{C} \in \{0,1\}^{2N}$, where $|C\rangle$ and $|\hat{C}\rangle$ are two Bob's final states. If the attack (U_E, U_F) induces no error on the test of CTRL and SIFT qubits in the proposed SQKD protocol, Eve obtains the same information on $|C\rangle$ and $|\hat{C}\rangle$ by the attack (U_E, U_F).*

Proof: *Case 1*: $H(C \oplus \hat{C}) = 1$. In this case, there exists $k \in \{1, 2, \ldots, 2N\}$ such that $C_k \neq \hat{C}_k$ and $C_i = \hat{C}_i$ for any $i \in \{1, 2, \ldots, 2N\}$ but $i \neq k$. Note that, Eve does not know the order of the qubits which Alice sends to Bob before Alice announces it publicly. This means that Eve can not discriminate which qubit is CTRL qubit or SIFT qubit when she applies the attack U_F. Thereby, the attack U_F is independent of U_R. Accordingly, we only need to show the two cases using the same ordering operation U_R. When the kth qubits in $|C\rangle$ and $|\hat{C}\rangle$ are CTRL qubits, the conclusion is straightforward by Lemma 3. So, we only need to show the conclusion when the kth qubits in $|C\rangle$ and $|\hat{C}\rangle$ are SIFT qubits.

By Lemma 1, we can suppose the finial global states of Eve-Bob-Aice system are $|F\rangle|C\rangle$ and $|\hat{F}\rangle|\hat{C}\rangle$ after the attack (U_E, U_F) acts on $|C\rangle$ and $|\hat{C}\rangle$, respectively. To prove that Eve obtains the same information on $|C\rangle$ and $|\hat{C}\rangle$, we only need to prove $|F\rangle = |\hat{F}\rangle$.

Without loss of generality, we suppose $C_k = 0, \hat{C}_k = 1$. We use $|\tilde{C}\rangle$ denoting a $2N$-qubit string such that $|\tilde{C}_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\tilde{C}_i\rangle = |C_i\rangle = |\hat{C}_i\rangle$ for any $i \in \{1, 2, \ldots, 2N\}$ but $i \neq k$. It is clear that $|\tilde{C}\rangle = \frac{1}{\sqrt{2}}(|C\rangle + |\hat{C}\rangle)$. By Lemma 1, we can use $|\tilde{F}\rangle|\tilde{C}\rangle$ denoting the finial global state of Eve-Bob system after the attack U_F on $|\tilde{C}\rangle$.

By Lemma 1 and Lemma 2, Alice must send $|C\rangle$, $|\hat{C}\rangle$, and $|\tilde{C}\rangle$ in Step 2 if Bob's final state is $|C\rangle$, $|\hat{C}\rangle$, and $|\tilde{C}\rangle$, respectively. We consider the scenario: (1) Bob's initial state is the same as $|B\rangle$; (2) The kth qubit in $|\psi\rangle$ corresponding to $|\tilde{C}\rangle$ is a CTRL qubit but corresponding to $|C\rangle$ or $|\hat{C}\rangle$ a SIFT qubit; (3) Alice uses the same operation (CTRL or SIFT) on the ith ($i \neq k$) qubit in $|\psi\rangle$ whenever corresponding to $|C\rangle$, $|\hat{C}\rangle$, or $|\tilde{C}\rangle$. It is clear that we always can choose the same as $|B\rangle$, suitable $|A\rangle$'s, and suitable ordering operations such that Bob gets the final states $|C\rangle$, $|\hat{C}\rangle$, and $|\tilde{C}\rangle$.

Because Bob's initial state is the same as $|B\rangle$, Eve's state is the same as $|E'\rangle$ after the attack U_E. By the supposition,

$$U_F(|E'\rangle|C\rangle) = |F\rangle|C\rangle \tag{26}$$

and

$$U_F(|E'\rangle|\hat{C}\rangle) = |\hat{F}\rangle|C\rangle. \tag{27}$$

By the linearity of U_F,

$$U_F(|E'\rangle|\tilde{C}\rangle) = \frac{1}{\sqrt{2}}U_F(|E'\rangle|C\rangle + |E'\rangle|\hat{C}\rangle) \tag{28}$$

$$= \frac{1}{\sqrt{2}}(|F\rangle|C\rangle + |\hat{F}\rangle|\hat{C}\rangle). \tag{29}$$

Therefore,

$$|\tilde{F}\rangle|\tilde{C}\rangle = \frac{1}{\sqrt{2}}|F\rangle|C\rangle + \frac{1}{\sqrt{2}}|\hat{F}\rangle|\hat{C}\rangle. \tag{30}$$

Since we are interested only in the kth qubit in Alice's and Bob's hands, we trace out all the other qubits in Alice's and Bob's hands in Eq. (30) and get the state

$$|\tilde{F}\rangle|+\rangle = \frac{1}{\sqrt{2}}|F\rangle|0\rangle + \frac{1}{\sqrt{2}}|\hat{F}\rangle|1\rangle \tag{31}$$

$$= \frac{1}{2}|F\rangle(|+\rangle + |-\rangle) + \frac{1}{2}|\hat{F}\rangle(|+\rangle - |-\rangle) \tag{32}$$

$$= (\frac{1}{2}|F\rangle + \frac{1}{2}|\hat{F}\rangle)|+\rangle + (\frac{1}{2}|F\rangle - \frac{1}{2}|\hat{F}\rangle)|-\rangle. \tag{33}$$

Accordingly,

$$\begin{cases} \frac{1}{2}|F\rangle + \frac{1}{2}|\hat{F}\rangle &= c|\tilde{F}\rangle; \\ \frac{1}{2}|F\rangle &= \frac{1}{2}|\hat{F}\rangle). \end{cases} \tag{34}$$

Solving Eqs. (34), we obtain

$$|F\rangle = |\hat{F}\rangle = \frac{c}{2}|\tilde{F}\rangle. \tag{35}$$

Ignoring the global factors,

$$|F\rangle = |\hat{F}\rangle = |\tilde{F}\rangle. \tag{36}$$

By Eq. (36), we have finished the proof of Case 1.

Case 2: $H(C \oplus \hat{C}) = l > 1$. In this case, we can construct a chain

$$|C\rangle = |C^{(0)}\rangle, |C^{(1)}\rangle, \ldots, |C^{(l)}\rangle = |\hat{C}\rangle \tag{37}$$

satisfying $H(C^{(i-1)} \oplus C^{(i)}) = 1$, $i = 1, 2, \ldots, l$. By the discussion above, Eve obtains the same information on $|C^{(i-1)}\rangle$ and $|C^{(i)}\rangle$, for any $i = 1, 2, \ldots, l$. Therefore, Eve obtains the same information on $|C\rangle$ and $|\hat{C}\rangle$. QED

Theorem 4.1 *The proposed SQKD protocol without invoking the classical party's measurement capability is completely robust: if any attack (U_E, U_F) inducing no error on SIFT and CTRL qubits, Eve is left with no information on the INFO string.*

Proof: It is straightforward by Lemmas 3 and 4. QED

Remark 4.6 *The proposed SQKD protocol is different from the randomization-based SQKD Protocol proposed by Boyer* et al. *[9]. In the proposed SQKD protocol, Eve can not get the Hamming weight of the INFO string if her attack on the proposed SQKD protocol introduces no error on CTRL and SIFT qubits because the number of CTRL qubits sent by Alice is not always equal to N.*

Remark 4.7 *If there is not any attack, it can be proved as the SQKD protocols [6, 9, 11] that the probability of aborting the proposed SQKD protocol is exponentially small with n, for any fixed $\delta > 0$.*

Remark 4.8 *If the proposed SQKD protocol was implemented by single photons, the classical Alice should use a wave-length-filter, as discussed in Ref. [8], to resist the Trojan horse attack suggested in Ref. [7]. Furthermore, to resist the delay-photon Trojan-horse attack [20], the classical Alice needs to use a photon number splitter.*

5 Conclusion

In this paper, we constructed an SQKD protocol without invoking the classical Alice's measurement capability. Furthermore, we proved that the proposed SQKD protocol is completely robust against joint attacks. The proposed SQKD protocol has the following properties: (1) The classical party Alice does not need the measurement capability; (2) Compared with the existing SQKD protocols, the number of the quantum states sent by Alice and Bob is decreased; (3) It is completely robust against joint attacks.

The proposed protocol shows that the classical party's measurement capability is not necessary in the SQKD. Thereby, the classical party does not need any quantum measuring device. Accordingly, the proposed SQKD protocol can be used in the scenario that Alice carries only a simple quantum preparation device (the emission device can prepare only the quantum states $|0\rangle$ and $|1\rangle$) and does not carry any quantum measuring device on her business trip.

There are many experiments based on the two-way quantum communication to show the security and the feasibility of QKD protocols [26–28]. Therefore, we believe that the experiment about SQKD is feasible. However, all the existing researches on the SQKD [6, 9–11, 16–19] focused only on their theoretics. Experimental proof for the security and the feasibility of the SQKD protocols must be a very interesting question needing to explore in future.

acknowledgements

The authors are grateful to the referees for invaluable suggestions that help us improve the quality of the paper. This work is supported in part by the National Natural Science Foundation (Nos. 61272058, 61073054), the Natural Science Foundation of Guangdong Province of China (Nos. S2012040007324, 10251027501000004), the Specialized Research Fund for the Doctoral Program of Higher Education of China (No. 20100171110042), the Science and Technology Project of Jiangmen City of China (No. [2011]131), and the Foundation of Graduate Education Reform of Wuyi University (No. YJS-JGXM-14-02), the FCT PEst-OE/EEI/LA0008/2013 project namely through the IT internal project CVQuantum.

References

[1] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, Bangalore India (1984)

[2] Ekert, A.K.: Quantum cryptography based on Bell's theorem. Physical Review Letters **67**(6), 661–663 (1991)

[3] Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Physical Review Letters **68**(5), 557–559 (1992)

[4] Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050 (1999)

[5] Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Physical Review Letters **85**(2), 441–444 (2000)

[6] Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Physical Review Letters **99**(14), 140501 (2007)

[7] Tan, Y.G., Lu, H., Cai, Q.Y.: Comment on "Quantum key distribution with classical Bob". Physical Review Letters **102**(9), 098901 (2009)

[8] Boyer, M., Kenigsberg, D., Mor, T.: Boyer, Kenigsberg, and Mor Reply. Physical Review Letters **102**(9), 098902 (2009)

[9] Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Physical Review A **79**(3), 032341 (2009)

[10] Lu, H., Cai, Q.Y.: Quantum key distribution with classical Alice. International Journal of Quantum Information **6**(6), 1195–1202 (2008)

[11] Zou, X., Qiu, D., Li, L., Wu, L., Li, L.: Semiquantum-key distribution using less than four quantum states. Physical Review A **79**(5), 052312 (2009)

[12] Boyer, M., Mor, T.: Comment on "Semiquantum-key distribution using less than four quantum states". Physical Review A **83**(4), 046301 (2011)

[13] Zou, X., Qiu, D.: Reply to "Comment on 'Semiquantum-key distribution using less than four quantum states' ". Physical Review A **83**(4), 046302 (2011)

[14] Miyadera, T.: Relation between information and disturbance in quantum key distribution protocol with classical Alice. International Journal of Quantum Information **9**(06), 1427–1435 (2011)

[15] Boyer, M., Mor, T.: On the robustness of (photonic) quantum key distribution with classical Alice. arXiv:1012.2418 (2010)

[16] Zhang, X.Z., Gong, W.G., Tan, Y.G., Ren, Z.Z., Guo, X.T.: Quantum key distribution series network protocol with M-classical Bobs. Chinese Physics B **18**, 2143–2148 (2009)

[17] Wang, J., Zhang, S., Zhang, Q., Tang, C.J.: Semiquantum key distribution using entangled states. Chinese Physics Letters **28**, 100301 (2011)

[18] Yu, K.F., Yang, C.W., Liao, C.H., Hwang, T.: Authenticated semiquantum key distribution protocol using Bell states. Quantum Information Processing **13**(6), 1457–1465 (2014)

[19] Krawec, W.O.: Restricted attacks on semi-quantum key distribution protocols. Quantum Information Processing **13**(11), 2417–2436 (2014)

[20] Yang, Y.G., Sun, S.J., Zhao, Q.Q.: Trojan-horse attacks on quantum key distribution with classical Bob. Quantum Information Processing **14**(2), 681–686 (2015)

[21] Li, Q., Chan, W.H., Long, D.Y.: Semiquantum secret sharing using entangled states. Physical Review A **82**(2), 022303 (2010)

[22] Wang, J., Zhang, S., Zhang, Q., Tang, C.J.: Semiquantum secret sharing using two-particle entangled state. International Journal of Quantum Information **10**(05), 1250050 (2012)

[23] Li, L., Qiu, D., Mateus, P.: Quantum secret sharing with classical Bobs. Journal of Physics A: Mathematical and Theoretical **46**(4), 045304 (2013)

[24] Zou, X., Qiu, D.: Three-step semiquantum secure direct communication protocol. Science China Physics, Mechanics & Astronomy **57**(9), 1696–1702 (2014)

[25] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Reviews of Modern Physics **74**(1), 145–195 (2002)

[26] Bethune, D.S., Risk, W.P.: An autocompensating fiber-optic quantum cryptography system basedon polarization splitting of light. IEEE Journal of Quantum Electronics **36**(3), 340–347 (2000)

[27] Cere, A., Lucamarini, M., Di Giuseppe, G., Tombesi, P.: Experimental test of two-way quantum key distribution in the presence of controlled noise. Physical review letters **96**(20), 200501 (2006)

[28] Pirandola, S., Mancini, S., Lloyd, S., Braunstein, S.L.: Continuous-variable quantum cryptography using two-way quantum communication. Nature Physics **4**(9), 726–730 (2008)

[29] Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters **92**(5), 057901 (2004)

[30] Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Limitations on practical quantum cryptography. Physical Review Letters **85**(6), 1330–1333 (2000)

[31] Deutsch, D., Ekert, A., Jozsa, R., Macchiavello, C., Popescu, S., Sanpera, A.: Quantum privacy amplification and the security of quantum cryptography over noisy channels. Physical Review Letters **77**(13), 2818–2821 (1996)

[32] Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Transactions on Information Theory **41**(6), 1915–1923 (1995)

[33] Khoo, K., Heng, S.H.: Universal hash functions over $GF(2^n)$. In: Proceedings of IEEE International Symposium on Information Theory, p. 205. IEEE, Chicago (2004)

[34] Biham, E., Mor, T.: Security of quantum cryptography against collective attacks. Physical Review Letters **78**(11), 2256 (1997)