Quantum secret sharing with classical Bobs

Lvzhou Li[a], Daowen Qiu[a,b], Paulo Mateus[b]

[a] Department of Computer Science, Sun Yat-sen University,
Guangzhou 510006, People's Republic of China

[b] SQIG–Instituto de Telecomunicações,
Departamento de Matemática, IST, Universidade Técnica de Lisboa,
Av. Rovisco Pais 1049-001, Lisbon, Portugal

December 11, 2012

Abstract

Boyer, Kenigsberg, and Mor [Phys.Rev.Lett.99, 140501(2007)] proposed a novel idea of semi-quantum key distribution where a key can be securely distributed between Alice who can perform any quantum operation and Bob who is classical. Extending the idea of "semi-quantum" to other tasks of quantum information processing is of interest and worth considering. In this article, we consider the issue of semi-quantum secret sharing where a quantum participant Alice can share a secret key with two classical participants Bobs. After analyzing the existing protocol, we propose a new protocol of semi-quantum secret sharing. Our protocol is more realistic, since it utilizes product states instead of entangled states. We prove that any attempt of an adversary to obtain information necessarily induces some errors that the legitimate users could notice.

1 Introduction

In the past two decades, quantum information processing (QIP) has attracted wide attention from the academic community. Roughly speaking, QIP is to process information using quantum systems (qubits), instead of classical systems (bits). Quantum mechanics has been showed to provide novel features to information processing, and has lead to many striking results such as teleportation, Shor's factoring algorithm, quantum cryptography and so on. In most of the QIP tasks that show advantage over classical ones, superposition of quantum states and entanglement play a key role. For example, entanglement is necessary for teleportation, and Shor's factoring algorithm makes use of superposition of quantum states.

Quantum key distribution (QKD) is a central problem in quantum cryptography. In a QKD protocol, the conventional setting is as follows: Alice and Bob have labs that are perfectly secure, they use qubits for their quantum communication, and they have access to an unjammable public classical communication channel. Then Alice and Bob choose to perform some quantum operations on the transmitted qubits, so that a random bit string is shared between them which is used as the key.

Recently, Boyer, Kenigsberg, and Mor [1] proposed the concept of semi-quantum key distribution (SQKD) where a key can be distributed between Alice who has full quantum power and Bob who is classical. In this SQKD protocol, a quantum channel leads from Alice's lab to the outside world and back to her lab. Bob can access a segment of the channel, and whenever a qubit passes through that segment Bob can choose to: (1) either let it go undisturbed, (2) or measure the qubit in the computational basis $\{|0\rangle, |1\rangle\}$ and then resend it in the state he found. A participant like Bob who is limited to perform operations (1) and (2) is said to be *classical*. It can be seen that if all parties were limited to perform only operations (1) and (2), the protocol would then be equivalent to a full classical one. In Ref. [1], it was showed that a semi-quantum protocol using less quantum properties than a pure quantum protocol still has an absolute advantage over classical protocols.

Indeed, it is of great interest to understand how to accomplish a QIP task using quantum properties as less as possible, but still keeping the advantage over classical ones. The idea of "semi-quantum" probably provides an approach to this problem. While Boyer, Kenigsberg, and Mor [1] have successfully incorporated the idea of "semi-quantum" into QKD, it is natural to ask: can we extend "semi-quantum" to other important QIP protocols? Recently, Li et al.[2] have extended this idea to quantum secret sharing [3], another important aspect of quantum cryptography.

Secret sharing addresses the problem where Alice wants to send a secret message to Bob and Charlie so that Bob and Charlie can collaborate to recover the message, but none alone can. There are classical solutions to this problem [4], but for addressing the problem of eavesdropping, classical secret sharing should be used in conjunction with other techniques such as encryption. Interestingly, Hillery, Buzek, and Berthiaume [3] in 1999 proposed a protocol based on quantum mechanics that can simultaneously achieve secret sharing and eavesdropping detection in an economical way. Such procedures that use quantum properties to achieve secret sharing are generally called *quantum secret sharing* (QSS).

After the seminal work [3], much work has been devoted to the study of quantum secret sharing (e.g. [2, 5, 6, 7, 8, 9, 10]). Note that in quantum secret sharing, the message to be shared can be either classical bits or quantum states. In this paper, we focus on sharing of classical messages, but it is worth pointing out that there are also many papers considering sharing of quantum states (e.g. [3, 11, 12, 13, 14]). Especially, unified approaches to secret sharing of both classical and quantum messages employing graph states were developed in [15, 16].

As mentioned before, Li et al. [2] have recently extended the idea of "semi-quantum" to quantum secret sharing, and proposed a protocol of semi-quantum secret sharing (SQSS) where a quantum participant, Alice, can share a secret key with two classical participants. However, one can observe that in the protocol in [2], there are two points going against its experimental implementation: (a) firstly, three-particle entangled states are needed in the protocol, which in fact play a crucial role; (b) secondly, Alice needs to perform joint measurements on three qubits. As we know, multipartite entangled states are generally difficult to prepare, and joint measurements are more difficult to implement than single-qubit measurements.

Taking all the above into account, in this paper we attempt to design a new SQSS protocol which uses product states. Also, in the new protocol, the communication parties need only to perform single-qubit measurements. Besides the above considerations concerning the experimental implementation, we are also motivated from the theoretical point of view to propose an SQSS protocol that does not require entanglement. Theoretically speaking, it is of great significance to discuss whether entanglement is necessary for a QIP task. For example, Ref. [17] discussed whether entanglement is necessary for quantum computation, and Ref. [18, 19] showed that entanglement is not necessary for distinguishing unitary operations.

The remainder of this paper is organized as follows. In Section 2 we first have a brief review on the SQSS protocol proposed by Li et al. [2], and then extend it to multiparty cases. In Section 3 we give a new SQSS protocol that uses product states. In Section 4 the security analysis of the proposed protocol is presented. Finally, a conclusion is made in Section 5.

2 On the existing SQSS protocol

In this section, we start by giving a brief review on the SQSS protocol proposed in [2], and then extend it to the multiparty case from which we obtain a deeper understanding on the role that entangled states played in the existing protocol.

2.1 A review on the existing SQSS protocol

Suppose that Alice wants to share a secret key with Bob and Charlie so that they can collaborate to recover the secret message, but none alone can. Since the protocol is semi-quantum, it is required that Alice has full power of quantum, but Bob and Charlie are classical. The main steps are as follows:
1. Alice first prepares a sufficient number of three-particle entangled states, of which each entangled state is in the following form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}} + |1\rangle\frac{|01\rangle + |10\rangle}{\sqrt{2}}). \tag{1}$$

After that, Alice sends the second and the third particle of each entangled state to Bob and Charlie, respectively, and keeps the remaining for herself.

2. Upon receiving each qubit, Bob randomly determines either to measure the qubit using the basis $\{|0\rangle, |1\rangle\}$ and resend the state he found, or to reflect it back to Alice without disturbance. Charlie does similarly.

3. Alice temporarily restores these qubits from Bob and Charlie, and announces by a public classical channel that she has received all the qubits. After that, Bob and Charlie declare which qubits they have measured.

4. Alice chooses to perform different operations on the qubits at his end, depending on Bob and Charlie's choices. If both Bob and Charlie choose to measure the qubits using the basis $\{|0\rangle, |1\rangle\}$, then Alice also measures his own qubit in the basis, and then uses this measurement result as a secret key bit. Note that, by denoting r_A, r_B, r_C the measurement result of Alice, Bob and Charlie, respectively, the following condition holds

$$r_A = r_B \oplus r_C. \tag{2}$$

Therefore, Bob and Charlie can only recover Alice's secret key if they collaborate. If either Bob or Charlie choose to reflect their qubit, then Alice can take advantage of this choice to detect eavesdropping. For example, if both Bob and Charlie choose to reflect the qubits back to Alice, then Alice measures all the three qubits at her end using a basis which includes the state given in Eq. (1). Thus, if Alice measured a state different from the state given in Eq. (1), she can ascertain that an eavesdropper has been interfering with the quantum channel.

The steps described above are the main steps of the SQSS protocol proposed in [2]. The efficiency of this protocol is 25%, that is, only one quarter of the qubits are used to produce the shared secret. Note that in the above protocol the entangled state $|\psi\rangle$ plays a crucial role. In addition, Alice needs to perform a joint measurement on three qubits in order to check for eavesdropping and noise.

2.2 Extending the existing SQSS protocol to multiparty cases

Next, we extend the SQSS protocol given in Section 2.1 to the multiparty case. In fact, such extension is not straightforward from Ref. [2].

In order to construct a multiparty SQSS protocol, we first introduce the following multi-particle entangled state

$$|\psi\rangle_n = \frac{1}{(\sqrt{2})^{n+1}}\Big[\bigotimes_{j=1}^{n}(|0\rangle + |1\rangle) + \bigotimes_{j=1}^{n}(|0\rangle - |1\rangle)\Big]. \tag{3}$$

The above state satisfies this property: it has a uniform superposition on the basis states $\{|c_1 c_1 \cdots c_n\rangle\}$ where c_i is 0 or 1 and the total number of 1's is even. For instance, when $n = 2$, we have

$$|\psi\rangle_2 = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{4}$$

When $n = 3$, we have

$$\begin{aligned} |\psi\rangle_3 &= \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle) && (5)\\ &= \frac{1}{\sqrt{2}}(|0\rangle\frac{|00\rangle + |11\rangle}{\sqrt{2}} + |1\rangle\frac{|01\rangle + |10\rangle}{\sqrt{2}}) && (6) \end{aligned}$$

which is the state given in Eq. (1). When $n = 4$, we have

$$\begin{aligned}|\psi\rangle_4 &= \frac{1}{\sqrt{2}}|0\rangle\frac{(|000\rangle + |011\rangle + |101\rangle + |110\rangle)}{2} \\ &+ \frac{1}{\sqrt{2}}|1\rangle\frac{(|001\rangle + |010\rangle + |100\rangle + |111\rangle)}{2}\end{aligned} \tag{7}$$

In fact, by using the state $|\psi\rangle_n$, Alice can share a secret key with $n-1$ classical Bobs as follows. (1) Alice prepares a sufficient number of states like $|\psi\rangle_n$, keeps the first qubit of each state for herself and sends the second to the n-th particle to the $n-1$ Bobs. (2) Each Bob chooses either to reflect the received qubit without disturbance or to measure it, using the basis $\{|0\rangle, |1\rangle\}$, and resend the state he found. (3) The remainder steps are similar those in the protocol presented in Section 2.1.

If Alice and all Bobs measure their own qubits using the basis $\{|0\rangle, |1\rangle\}$, then their measurement results have the following correlation:

$$r_A = r_{B_1} \oplus r_{B_2} \oplus \cdots \oplus r_{B_{n-1}} \tag{8}$$

where r_A denotes the result of Alice's measurement, and r_{B_i} denotes the result of the measurement performed by the i-th Bob. Thus, Alice can use her measurement results as the shared secret key.

Note that if Alice wants share a secret key with n Bobs, the efficiency of this protocol is $1/2^n$, and therefore, decreases exponentially with the number n. So for a large number of parties the protocol is definitely impractical. For this reason, it is relevant to find a semi-quantum multiparty scheme whose efficiency does not decrease exponentially with the number of parties. To be honest, our main purpose for presenting here such scheme is to offer an insight into the role that the entanglement played in the protocol proposed in [2], instead of to propose a perfect semi-quantum multiparty scheme.

In addition, there are also other factors going against the experimental implementation of the protocol: (i) the above protocol requires multipartite entangled states, and (ii) in the error checking steps Alice needs to do joint measurements on several qubits. In the next section we propose a SQSS protocol that does not require entangled states and joint measurements.

3 The description of our SQSS protocol without entanglement

Suppose that Alice wants to share a secret key with Bob and Charlie, so that they can collaborate to recover the secret message, but none alone can. We are going to design a semi-quantum protocol for this task. The term "semi-quantum" means that Alice has full quantum power, but Bob and Charlie are restricted to the following two operations: (1) either to measure the qubit using the basis $\{|0\rangle, |1\rangle\}$ and resend it in the found state (briefly referred to as MEASURE), (2) or to reflect the qubit back to Alice without disturbance (briefly referred to as REFLECT). For simplicity, we refer to the basis $\{|0\rangle, |1\rangle\}$ as Z basis, and the basis $\{|+\rangle, |-\rangle\}$ as X basis, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Now, our protocol is described as follows:

Step 1. Alice prepares N two-qubit product states, each pair of which is in the state:

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_B \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)_C. \tag{9}$$

We denote the ordered N two-qubit states by $\{[\mathrm{P}_1(B),\mathrm{P}_1(C)], [\mathrm{P}_2(B),\mathrm{P}_2(C)], \cdots, [\mathrm{P}_N(B),\mathrm{P}_N(C)]\}$, where the subscript indicates the order of each state in the sequence, and B, C represent the two particles of each state. Alice sends particles B and C of each pair to Bob and Charlie, respectively.

Step 2. When each particle arrives, Bob chooses randomly either to MEASURE, or to REFLECT. Charlie does similarly.

Step 3. Alice temporarily restores the received particles in quantum memory and informs Bob and Charlie that she has received particles B and C. After that, Bob and Charlie publish which particles they have chosen to MEASURE and which ones they have chosen to REFLECT.

Step 4. Alice performs one of the four operations on each received particle depending on Bob's and Charlie's choices, as illustrated in Table 1. In Table 1, ACTION 1 means measuring both particles B and C in Z basis, ACTION 2 means measuring particle B in Z basis and particle C in X basis, ACTION 3 means measuring particle B in X basis and particle C in Z basis, and ACTION 4 means measuring both particles B and C in X basis. Suppose that the four cases in Table 1 occur with the same probability. Then Alice can use cases (2,3,4) to detect eavesdropping and use case (1) to share the secret key. We provide more details in the following discussion.

Case	Bob	Charlie	Alice
(1)	MEASURE	MEASURE	ACTION 1
(2)	MEASURE	REFLECT	ACTION 2
(3)	REFLECT	MEASURE	ACTION 3
(4)	REFLECT	REFLECT	ACTION 4

Table 1: Participants' actions on the qubits in each position.

(i) If both Bob and Charlie choose to MEASURE, Alice can obtain both their measurement results by implementing ACTION1, and then she encodes her secret key as shown in Table 2. If we denote respectively r_B, r_C the measurement results of Bob and Charlie, and denote s_K the secret bit, then Alice encodes s_K as

$$s_K \equiv r_B \oplus r_C. \tag{10}$$

Thus, Bob and Charlie can recover the secret bit only if they collaborate.

Bob's result	Charlie's result	Alice's result	Secret
0	0	00	0
0	1	01	1
1	0	10	1
1	1	11	0

Table 2: The communication parties' measurement results and the shared secret key.

(ii) If cases (2,3,4) in Table 1 occur, then Alice can use them to detect eavesdropping. For example, if Bob chooses to MEASURE and Charlie chooses to REFLECT, then the state received by Alice should be $|r\rangle_B|+\rangle_C$ where $|r\rangle = |0\rangle$ or $|r\rangle = |1\rangle$ and $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Thus, by performing ACTION2, Alice can check whether there exists an eavesdropper at the line between her and Charlie, since if there is no eavesdropping, Alice will always measure Charlie's qubit in state $|+\rangle$, otherwise Alice may measure the state $|-\rangle$. Similarly, if case (3) occurs, Alice can check whether there exists an eavesdropper at the line between her and Bob. If case (4) occurs, Alice can check whether there exists an eavesdropper at the line between her and Bob or at the line between her and Charlie. In the next section we provide more details concerning the security analysis.

Step 5. Alice checks the error rate in cases (2,3,4) given in Table 1. If the error rate in any case is higher than some predefined threshold value, the protocol aborts.

Step 6. Alice checks the error rate in case (1). She chooses randomly a sufficiently large subset from the measurement results in case (1) and announces which are the chosen particles. Bob and Charlie then publish their measurement results. Alice then compares the measurement results obtained by implementing ACTION1 with those published by Bob and Charlie. If the error rate is below some predefined threshold value, Alice uses the remaining measurement results to form the final secret string which can be recovered only when Bob and Charlie work together.

Remark 1: Note that after Hillery, Buzek, and Berthiaume [3] proposed the idea of quantum secret sharing (QSS) where entangled states played a key role, some QSS protocols such as the one in [8] using no entanglement were proposed. The protocol in [8] is essentially a combination of two parallel BB84 key distribution protocols. Similarly, our protocol can be regarded as a combination of two parallel semi-quantum key distribution protocols [20]. However, the detailed security analysis presented in the next section is not trivial.

The above protocol can be directly extended to multiparty cases as follows: Alice distributes a state $|+\rangle^{\otimes n}$ to n Bobs, who choose to measure in Z basis or to reflect, and then use the same idea as in the bipartite case. One can then find that the efficiency of this case is again $1/2^n$ as the extending protocol mentioned in Section 2.2. This probability decreases exponentially with the number n, which implies that such multiparty protocol is not suitable for a large number of parties. Whether there exists a semi-quantum multiparty protocol whose efficiency does not decreases with the number of parties is worthy of further consideration. As pointed out by an anonymous referee, a possible approach to mitigate the rapid decrease of the efficiency is to increase the MEASURE probability of Bob, Charlie etc. above 1/2 and adapt Steps 5 and 6 accordingly.

4 The security analysis of the proposed protocol

Before presenting a more general discussion of eavesdropping, we first consider a specific situation in order to show that it can be detected. Suppose that Bob is dishonest and he has managed to get Charlies's states as well as his own. Note that Bob's eavesdropping can impact on the information from Alice to Charlie and on the information from Charlie to Alice. In the specific situation, we assume that Bob's eavesdropping is only on the information from Alice to Charlie. He then may measure the two particles sent by Alice and send one to Charlie. His object is to discover Alice's secret key without any assistance from Charlie, and to do so in a way that can not be detected.

To decrease the probability of being detected by Alice, Bob can do as follows. (1) When he chooses to REFLECT his own particle, he does nothing on the particle from Alice to Charlie, which will not introduce any error. (2) When he chooses to measure his own particle in Z basis, he may choose to do nothing on Charlie's particle and thus he obtains no information about Alice's secret; also, Bob may choose to measure the particle in Z basis and then send the state he found to Charlie, from which Bob can obtain some information about Alice's secret key, but he has the risk of being detected by Alice. If Bob measures Charlie's qubits in the position where Charlie has chosen to MEASURE, then Bob can obtain Charlie's measurement results, and thus can use them to recover the secret key without introducing any error. But if Bob measures Charlie's qubits in the position where Charlie has chosen to REFLECT, then with half of the time Alice finds an error by measuring the qubits received from Charlie in X basis, since it holds that $|0\rangle = \frac{|+\rangle+|-\rangle}{\sqrt{2}}$ and $|1\rangle = \frac{|+\rangle-|-\rangle}{\sqrt{2}}$. Thus, in this case the probability of Bob introducing an error is 25%.

Notice that there are two cases of eavesdropping. The first is that one dishonest participant (Bob or Charlie) attempts to find Alice's secret without cooperating with the other party. The second is that a fourth eavesdropper Eve aims to find Alice's secret without being detected. Without loss of generality, we should only consider the case of one dishonest participant (Bob or Charlie), since the eavesdropper in this case can obtain more information than a fourth eavesdropper Eve.

Now let us look at a general situation. Suppose that an eavesdropper, Eve (who could be Bob or Charlie), attempts to attack the information between

Alice and Bob/Charlie. We show that Eve cannot obtain information on the secret bits without being detectable. Eve's most general attack is comprised of two unitary operators: U attacking qubits as they go from Alice to Bob and Charlie and V as they go back from Bob and Charlie to Alice, where without loss of generality, U and V are assumed to share a common probe space $\mathcal{H}_E$ (see Figure 1). Note that the shared probe allows Eve to make the attack on the returning qubits depend on knowledge acquired by U, and if Eve does not take advantage of that fact, the "shared probe" can simply be the composite system comprised of two independent probes, which has no influence on the following proof. As stated before, without loss of generality we need only consider the case that an insider, say Bob, wants to eavesdrop Alice's secret without cooperating with Charlie.

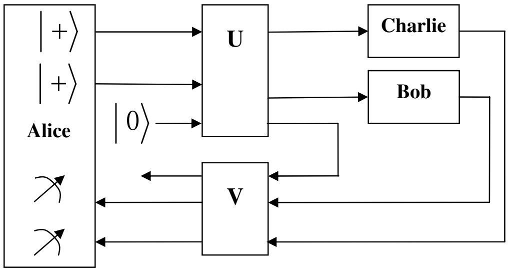

Figure 1: Eve attacks the qubits sent from Alice to Charlie/Bob and back to Alice with entangling unitary operators (U, V).

Theorem 1: Suppose that Bob performs attack (U, V) on the qubits sent from Alice to him and Charlie. Then, for this attack inducing no error in Steps 5 and 6, the final state of Bob's probe should be independent of Charlie's measurement result and therefore Bob gets no information on the secret key.

Proof: Denote the qubits sent from Alice to Bob and Charlie by B and C, respectively, and denote Bob's probe by E. Let us have a look at the evolution of the system $B + C + E$.

(1) Before Bob's attack, the state is $|+\rangle_B|+\rangle_C|0\rangle_E$.

(2) After Bob has performed U, the state evolves to

$$|\psi\rangle = |00\rangle_{BC}|E_{00}\rangle + |01\rangle_{BC}|E_{01}\rangle + |10\rangle_{BC}|E_{10}\rangle + |11\rangle_{BC}|E_{11}\rangle$$

where $|E_{ij}\rangle$ are un-normalized states of Eve's probe. In particular, if Eve does noting, then $|E_{ij}\rangle$'s equal to $\frac{1}{2}|0\rangle$.

(3) When Bob and Charlie receive the qubits sent from Alice, they choose either to measure or reflect the qubits. After that, Bob performs V. We want to prove that the state of E after V having been performed is independent of Charlie's final state.

(i) Firstly, for Bob not being detectable in Step 6, V must satisfy the following conditions:

$$V|x_1x_2\rangle_{BC}|E_{x_1x_2}\rangle = |x_1x_2\rangle_{BC}|F_{x_1x_2}\rangle, \tag{11}$$

where $x_1, x_2 \in \{0,1\}$, and the key point is that V can not change the state of $B+C$. Otherwise, Alice will detect this attack with a non-zero probability. For example, suppose that V changes $|00\rangle_{BC}|E_{00}\rangle$ to $|00\rangle_{BC}|F'_{00}\rangle + |01\rangle_{BC}|F'_{01}+\rangle|10\rangle_{BC}|F'_{10}\rangle + |11\rangle_{BC}|F'_{11}\rangle$. Then, while Bob and Charlie have measured their qubits in $|00\rangle$, Alice may observe an state not in $|00\rangle$ with probability $|||F'_{01}\rangle||^2 + |||F'_{10}\rangle||^2 + |||F'_{11}\rangle||^2$, and thus some errors will be induced in Step 6.

(ii) Secondly, we show that $|F_{00}\rangle = |F_{01}\rangle$ and $|F_{10}\rangle = |F_{11}\rangle$. Assume that Bob has chosen to measure his qubit and Charlie has chosen to reflect his qubit. After that, the state of $B+C+E$ is given in Table 3.

Bob's result	state of B+C+E
0	$\|00\rangle_{BC}\|E_{00}\rangle + \|01\rangle_{BC}\|E_{01}\rangle$
1	$\|10\rangle_{BC}\|E_{10}\rangle + \|11\rangle_{BC}\|E_{11}\rangle$

Table 3:

Assume that Bob measured 0. Then after performing V, the state is

$$|00\rangle_{BC}|F_{00}\rangle + |01\rangle_{BC}|F_{01}\rangle = |0\rangle_B(|0\rangle_C|F_{00}\rangle + |1\rangle_C|F_{01}\rangle)$$

Let $|\psi_0\rangle = |0\rangle_C|F_{00}\rangle + |1\rangle_C|F_{01}\rangle$. Replacing $|0\rangle$ by $\frac{|+\rangle+|-\rangle}{\sqrt{2}}$ and $|1\rangle$ by $\frac{|+\rangle-|-\rangle}{\sqrt{2}}$ gives

$$|\psi_0\rangle = \Big[|+\rangle_C\frac{|F_{00}\rangle + |F_{01}\rangle}{\sqrt{2}} + |-\rangle_C\frac{|F_{00}\rangle - |F_{01}\rangle}{\sqrt{2}}\Big]. \tag{12}$$

According to the protocol, for Bob inducing no error in Step 5, the probability of Alice measuring the qubit reflected by Charlie in the result $|-\rangle$ must be zero, and thus it must hold that

$$|F_{00}\rangle = |F_{01}\rangle. \tag{13}$$

Similarly, assuming Bob measured 1 necessarily leads to

$$|F_{10}\rangle = |F_{11}\rangle. \tag{14}$$

In summary, for Bob not inducing errors in Step 5, Eqs. (13, 14) must simultaneously hold, which means that the final state of Bob's probe is independent of Charlie's measurement result (but dependent on his own measurement result). Therefore, we have proved Theorem 1. □

Remark 2: (i) In the above proof, if the entangling attack (U, V) was performed by a fourth eavesdropper Eve, we can further show that $|F_{00}\rangle = |F_{01}\rangle = |F_{10}\rangle = |F_{11}\rangle$, which means that the state of Eve's probe is independent of Bob's and Charlie's measurement results. (ii) One can also consider the case that an eavesdropper first temporarily stores all the qubits sent from Alice to Bob and Charlie and then does a collective unitary operation U on them. When the qubits come back from Bob and Charlie to Alice, they can do another collective unitary operation V. The idea for proving this case is similar to the one we have presented, and thus we omit the details.

5 Conclusion

The idea of "semi-quantum" was first introduced by Boyer, Kenigsberg and Mor [1] to design a protocol of semi-quantum key distribution. In this paper, we have considered the issue of semi-quantum secret sharing (SQSS). By analyzing the existing SQSS protocol and extending it to multiparty cases, we have a deeper understanding on the role that entangled states played in the existing protocol. However, multipartite entangled states are generally difficult to prepare in practice. Therefore, in this paper we have proposed a new SQSS protocol using product states, where a quantum party, Alice, prepares a product state $|+\rangle|+\rangle$ of two qubits and then sends one to Bob and one to Charlie, and Bob and Charlie are classical, that is, Bob and Charlie choose either to reflect the received qubit without disturbance, or to measure the qubit in Z basis and then resend it in the found state. We have proven that any attempt of an adversary to obtain information necessarily induces some errors that the legitimate users could notice.

Note that in this paper we have only given a preliminary security analysis, and a deeper security analysis is required for the protocol to be feasible in practice. We hope this work will stimulate further discussion, and in the further study, one can consider to take a deep security analysis in the line of articles like [21] (we are grateful to one of anonymous referees for pointing out this reference to us).

Acknowledgements

This work is supported in part by the National Natural Science Foundation (Nos. 61272058, 61073054, 60873055, 61100001), the Natural Science Foundation of Guangdong Province of China (No. 10251027501000004), the Specialized Research Fund for the Doctoral Program of Higher Education of China (Nos. 20100171110042, 20100171120051), the Fundamental Research Funds for the Central Universities (Nos. 10lgzd12, 11lgpy36), the China Postdoctoral Science Foundation project (Nos. 20090460808, 201003375), and the project of SQIG at IT, funded by FCT and EU FEDER projects projects QSec PTDC/EIA/67661/2006, AMDSC UTAustin/MAT/0057/2008, NoE Euro-NF, and IT Project QuantTel, FCT project PTDC/EEA-TEL/103402/2008 QuantPrivTel.

References

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

[2] Q. Li, W. H. Chan, and D. Y. Long, Phys. Rev. A **82**, 022303 (2010).

[3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[4] B. Schneier, *Applied Cryptography* (John Wiley & Sons, New York, 1996), p. 70; J. Gruska, *Foundations of Computing* (International Thomson Computer Press, Boston, 1997), p. 504.

[5] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).

[6] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

[7] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).

[8] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).

[9] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).

[10] Z. J. Zhang, and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).

[11] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).

[12] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).

[13] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).

[14] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).

[15] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).

[16] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, Phys. Rev. A **82**, 062315 (2010).

[17] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor, Theor. Comput. Sci. 320, 15 (2004).

[18] L. Z. Li and D. W. Qiu, Phys. Rev. A **77**, 032337 (2008).

[19] R. Y. Duan, Y. Feng, and M. Ying, Phys. Rev. Lett. 98, 100503 (2007).

[20] X. Zou, D. Qiu, L. Li, L.Wu, and L. Li, Phys. Rev. A **79**, 052312 (2009); M. Boyer and T. Mor Phys. Rev. A **83**, 046301 (2011); X. Zou, D. Qiu, Phys. Rev. A **83**, 046302 (2011).

[21] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A 72, 012332 (2005); also at arXiv:quant-ph/0502064.