Semiquantum secret sharing using entangled states

Qin Li,[1,2,3] W. H. Chan,[3,*] and Dong-Yang Long[2]
[1]*College of Information Engineering, Xiangtan University, Xiangtan 411105, China*
[2]*Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China*
[3]*Department of Mathematics, Hong Kong Baptist University, Kowloon, Hong Kong, China*
(Received 6 June 2009; published 4 August 2010; publisher error corrected 19 October 2011)

Secret sharing is a procedure for sharing a secret among a number of participants such that only the qualified subsets of participants have the ability to reconstruct the secret. Even in the presence of eavesdropping, secret sharing can be achieved when all the members are quantum. So what happens if not all the members are quantum? In this paper, we propose two semiquantum secret sharing protocols by using maximally entangled Greenberger-Horne-Zeilinger-type states in which quantum Alice shares a secret with two classical parties, Bob and Charlie, in a way that both parties are sufficient to obtain the secret, but one of them cannot. The presented protocols are also shown to be secure against eavesdropping.

DOI: 10.1103/PhysRevA.82.022303 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

Suppose a service provider Alice wants to distribute some secret information among clients, Bob and Charlie, such that Bob and Charlie can obtain the secret information through their cooperation, while one of them cannot. Classical secret sharing has been proposed as a solution [1–3]. A simple example is that Alice prepares a binary bit string related to her secret message and generates a random string of the same length. She then applies bitwise XOR operations on these two strings and sends the resulting string to Bob and a copy of the random string to Charlie. Obviously, Bob and Charlie, by acting together, can access Alice's message, but one of them can obtain nothing about it.

Unfortunately, classical secret sharing cannot address the problem of eavesdropping if it is not used in conjunction with other techniques such as encryption. If an eavesdropper Eve (including one malicious participant of the Bob-Charlie pair) can control the communication channel and can obtain both of Alice's transmissions, then Alice's message becomes transparent for her. Fortunately, quantum secret sharing can achieve secret sharing and eavesdropping detection simultaneously. Hillery *et al.* showed how to implement a secret sharing scheme by using three-qubit entangled Greenberger-Horne-Zeilinger (GHZ) states [4] in the presence of an eavesdropper [5]. Karlsson *et al.* presented a secret sharing scheme based on two-qubit quantum entanglement such that only two members implementing together are able to obtain the information [6]. Gottesman showed that the size of each important share sometimes can be made half of the size of the secret if quantum states are used to share a classical secret [7]. The secret sharing protocol among n parties based on entanglement swapping of d-level cat states and Bell states was introduced by Karimipour *et al.* [8]. Guo and Guo proposed a secret sharing scheme that utilizes product states instead of entangled states so as to improve the efficiency up to 100% [9]. Xiao *et al.* generalized the scheme in Ref. [5] into any number of participants and gave two efficient quantum secret sharing schemes with the 100% asymptotical efficiency [10]. Zhang and Man considered a multiparty quantum secret sharing protocol of the classical secret based on entanglement swapping of Bell states [11]. There are also many quantum secret sharing protocols that consider sharing quantum information [5–7,12–20]. Especially, Markham and Sanders developed a unified approach to secret sharing of both classical and quantum secrets by employing graph state [20].

However, previous quantum secret sharing protocols require all the parties to have quantum capabilities. So, what happens if not all the parties are quantum? Actually, the situation that not all the participants can afford expensive quantum resources and quantum operations is more common in various applications. It is well known that semiquantum key distribution in which one party Alice is quantum and the other party Bob just owns classical capabilities is possible [21–23], so, it is interesting to ask whether semiquantum secret sharing (SQSS) (the specific definition is given afterward) is possible. The answer is affirmative.

In this paper, we consider the secret sharing protocol in which quantum Alice has to share a secret with classical Bob and classical Charlie such that the collaboration of Bob and Charlie can reconstruct the secret, while one of them cannot obtain anything about the secret. We say Alice is quantum as she is allowed to prepare general quantum states and to perform quantum operations on the qubits. We follow the descriptions about "classical" in Refs. [21–23]. An orthogonal basis such as the computational basis $\{|0\rangle,|1\rangle\}$ can be selected as a classical basis and can be replaced with the classical notations $\{0,1\}$. Bob and Charlie are restricted to performing four operations when they access a segment of the quantum channel: (1) measuring the qubits in the classical $\{0,1\}$ basis, (2) reordering the qubits (via different delay lines), (3) preparing (fresh) qubits in the classical basis, and (4) sending or returning the qubits without disturbance. If one can only apply those four operations on the qubits in the classical basis and cannot obtain any quantum superposition of the two states in the classical basis, such qubits can be regarded as classical bits, and the operations can be considered to be classical, since they are equivalent to the usual $\{0,1\}$ computation. The protocol of this kind is termed as SQSS. SQSS protocols can have two variants, *randomization-based* SQSS and *measure-resend* SQSS, in terms of the operations that classical participants are allowed to

*dchan@hkbu.edu.hk

implement. In a randomization-based SQSS protocol, classical participants are limited to perform operations (1), (2), and (4), while in a measure-resend SQSS protocol, classical participants are limited to perform operations (1), (3), and (4). In principle, an SQSS protocol is considered as secure if neither an eavesdropper nor a malicious participant can obtain any information about the secret. In the following sections, we utilize maximally entangled states of the GHZ type to construct a randomization-based SQSS protocol and a measure-resend SQSS protocol based on the semiquantum key distribution protocols [21–23], and we show that the proposed SQSS protocols are secure against eavesdropping.

II. THREE-QUBIT ENTANGLED STATES

In order to construct SQSS protocols, we introduce a three-qubit entangled state in the following form:

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

This state also can be rewritten as

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|++\rangle+|--\rangle}{\sqrt{2}} + |1\rangle\frac{|++\rangle-|--\rangle}{\sqrt{2}}\right)\\ &= \frac{|0\rangle+|1\rangle}{\sqrt{2}}\frac{|++\rangle}{\sqrt{2}} + \frac{|0\rangle-|1\rangle}{\sqrt{2}}\frac{|--\rangle}{\sqrt{2}}\\ &= \frac{|+++\rangle+|---\rangle}{\sqrt{2}}. \end{aligned} \quad (2)$$

Obviously, by implementing a Hadamard operation on each qubit of the state $|\psi\rangle$, respectively, $|\psi\rangle$ is transformed into the standard GHZ state,

$$|\mathrm{GHZ}\rangle = \frac{|000\rangle+|111\rangle}{\sqrt{2}}. \quad (3)$$

According to Ref. [24], if two three-qubit entangled states can be mutually transformed by local unitary operations, they must be equivalent. Hence, $|\psi\rangle$ is equivalent to the standard GHZ state, and it belongs to the GHZ type. Like the canonical GHZ state, it is also maximally entangled in several aspects [25]. For instance, it violates Bell inequality [26] maximally; it is maximally fragile, since only one qubit loss can disentangle it; by measuring a qubit, an Einstein-Podolsky-Rosen (EPR) state can be obtained from the other two qubits; the mutual information of measurement results can be maximal.

The GHZ-type state $|\psi\rangle$ is not only theoretically existent but also experimentally feasible. It can be obtained from the standard GHZ state by using Hadamard gates, and also can be generated in the following way. To gain $|\psi\rangle$, we may begin by preparing the state $|0\rangle$ and the Bell state $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, and then, we may apply the Hadamard gate to the first qubit, and finally we may apply the controlled-NOT gate to the first two qubits. The specific steps are illustrated by the quantum circuit shown in Fig. 1. Let us follow the states in the circuit to clearly see the process of generating $|\psi\rangle$. The input state of the circuit is

$$|\psi_0\rangle = |0\rangle\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}}. \quad (4)$$

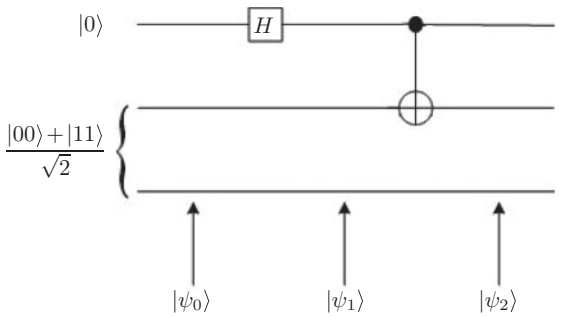

FIG. 1. Quantum circuit for generating $|\psi\rangle$.

After sending the first qubit through the Hadamard gate, we have

$$\begin{aligned}|\psi_1\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes\frac{|00\rangle+|11\rangle}{\sqrt{2}}\\ &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}} + |1\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right). \end{aligned} \quad (5)$$

Then, we send the first two qubits through the controlled-NOT gate to obtain

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}} + |1\rangle\frac{|10\rangle+|01\rangle}{\sqrt{2}}\right)\\ &= |\psi\rangle. \end{aligned} \quad (6)$$

Since the Hadamard gate and the controlled-NOT gate, which are fundamental quantum gates, can be experimentally feasible [27,28], the procedure presented here can lead to the possibility of generating $|\psi\rangle$.

Notice that full quantum secret sharing can be realized by using standard GHZ states [5]. Alice, Bob, and Charlie obtain a qubit from each GHZ state in the form of Eq. (3), and then, make random measurements in the x or y basis. Subsequently, they publicly announce which bases were used, but not the corresponding measurement results. By revealing a random subset of the outcomes, where their measurement bases coincided for verification, Alice can establish a secret string, which can be gained only when Bob and Charlie cooperate. We will show the usefulness of the GHZ-type state $|\psi\rangle$ for SQSS.

III. RANDOMIZATION-BASED SQSS PROTOCOL

In this section, we propose a randomization-based SQSS protocol in which quantum Alice and the other two classical parties, Bob and Charlie, share a secret string such that Bob and Charlie can recover the secret string only when they work together. Quantum Alice has the ability to prepare the maximally entangled GHZ-type state $|\psi\rangle$ and to perform some quantum operations such as Bell measurements and three-qubit join measurements. Classical parties, Bob and Charlie, are restricted to implementing three operations: (1) measuring the qubits in the classical basis, (2) reordering the qubits (via different delay lines), and (3) sending or returning the qubits without disturbance. All the participants can access a quantum channel and an authenticated public channel that is susceptible to eavesdropping. The detailed steps are given in the following.

(i) Alice creates a sufficiently long string of three-qubit entangled states in the form of Eq. (1). (Suppose N triplet states are in the string, and they are indexed from 1 to N.) After that, Alice sends the second and the third qubits of each entangled state to Bob and Charlie, and keeps the remainder for herself.

(ii) Upon receiving each qubit, Bob randomly determines, either to measure the qubit using the classical basis (we refer to this action as SHARE), or to reflect it back to Alice (we refer to this action as CHECK). Particularly, Bob reflects the qubits in a new order such that nobody else could distinguish which qubits are returned. Each measurement outcome is interpreted as a binary 0 or 1. Similarly, Charlie also randomly decides either to measure the qubits or to reflect the qubits in another order.

(iii) Alice temporarily restores the qubits reflected by Bob and Charlie in quantum registers according to their incoming sequences, and announces that she has received their reflected qubits in a public channel.

(iv) Bob and Charlie declare which qubits were reflected by them and the order in which their qubits were returned, respectively. Alice reordered the reflected qubits according to Bob's and Charlie's reports.

(v) For her own qubit in each position, Alice performs one of the four actions according to Bob's and Charlie's actions on the corresponding qubits, as illustrated in Table I.

It is supposed that the four cases in Table I, which appear in the same probability:

(1) Both Bob and Charlie choose to SHARE, then Alice can implement ACTION 1 to obtain a bit (we name this bit as the SHARE bit) that can be retrieved if Bob and Charlie use the XOR operation on their measurement outcomes;

(2) Bob chooses to SHARE, and Charlie chooses to CHECK, then Alice can perform ACTION 2 to check whether Bob's measurement outcome is right and the resulting two-qubit state is the correct Bell state;

(3) Bob chooses to CHECK, and Charlie chooses to SHARE, then Alice can utilize ACTION 3 to check if Charlie's measurement result is right and the resulting two-qubit state is the correct Bell state;

(4) Both Bob and Charlie choose to CHECK, then Alice can check whether the original three-qubit entangled state in the form of Eq. (1) is changed by carrying out ACTION 4.

TABLE I. Participants' actions on the qubits in each position.

Case	Bob	Charlie	Alice
(1)	SHARE	SHARE	ACTION 1[a]
(2)	SHARE	CHECK	ACTION 2[b]
(3)	CHECK	SHARE	ACTION 3[c]
(4)	CHECK	CHECK	ACTION 4[d]

[a]To measure her qubit in the classical basis.

[b]To combine her qubit with Charlie's reflected qubit and to perform a Bell measurement.

[c]To combine her qubit with Bob's reflected qubit and to perform a Bell measurement.

[d]To combine her qubit with the two reflected qubits and to perform an appropriate three-qubit join measurement.

For instance, let Bob randomly measure the qubits in $N/2$ positions (SHARE) and reflect the qubits in the other $N/2$ positions in a new order $l_B = l_1 l_2 \cdots l_{N/2}$ (CHECK), and Charlie performs the similar operations as Bob does and reflects the qubits in another order $m_C = m_1 m_2 \cdots m_{N/2}$. Suppose $N = 8$, $l_B = 4731$, and $m_C = 6427$. Then, the lists of the qubits measured by Bob and Charlie are indexed by their complements $\bar{l}_B = 2568$ and $\bar{m}_C = 1358$, respectively. Hence, Alice performs ACTION 1 in positions 5 and 8 and interprets the measurement outcomes as classical bits 0 or 1, and she performs ACTION 4 in positions 4 and 7. Alice also implements ACTION 2 in positions 2 and 6, and ACTION 3 in positions 1 and 3.

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

(vii) Alice requires Bob and Charlie to reveal a random subset (assume the size of the subset is about $N/8$) of the bits that are used to generate Alice's SHARE bits. Actually, this process is used to check the error rate in case (1). If the values of Bob's and Charlie's bits are the same (or opposite), then Alice's bit should be 0 (or 1) according to Eq. (1). From step v, we know that approximately $N/4$ positions are selected by both Bob and Charlie to SHARE. If the error rate on SHARE bits is not significant, the remaining $N/8$ SHARE bits of Alice form the final secret string, which can be recovered only when Bob and Charlie work together.

We show the preceding randomization-based SQSS protocol is secure against eavesdropping in two situations. The first is that one dishonest classical party Bob (or Charlie) attempts to find Alice's secret without cooperating with the other party in the recovery stage. The second is that an eavesdropper Eve (including malicious Bob or Charlie), who has quantum capabilities, is involved and aims to find Alice's secret without being detected.

We first suppose the dishonest classical party Bob can access both of Alice's transmissions. In some of the positions, Bob may measure the qubit using the classical basis and resend one of them in the state he found to Charlie. In terms of Eq. (1), if both of the measurement outcomes are the same (or the opposite), he learns that Alice's bit must be 0 (or 1). In the other positions, Bob may behave like an honest party and do nothing on Charlie's qubits. However, this cheating strategy can hardly succeed, since Bob does not know Charlie's choices. If Bob measures Charlie's qubit in the position where Charlie chooses to CHECK, he suffers a problem. According to the state $|\psi\rangle$ in Eq. (1), if Bob just measures his own qubit, then the two-qubit state, which results from combining Alice's qubit and Charlie's reflected qubit should be the Bell state, while, if Bob measures both qubits for himself and Charlie, then the two-qubit state, which results from combining Alice's qubit and Charlie's reflected qubit will be the product state; and, thus, Alice will find this abnormity with probability $1/2$ by using a Bell measurement. However, if Bob measures Charlie's qubit in the position where Charlie chooses to SHARE, his cheating will not be found. In each position, Charlie has a probability of $1/2$ for making either choice, so the probability that Bob escapes from being detected is $1/2 \times 1/2 + 1/2 = 3/4$. Assume that Bob has to measure both qubits in $l (l \leqslant N/4)$ positions to obtain the significant information of Alice's secret without the

aid of Charlie, then the probability that Bob goes undetected is $(3/4)^l$, which may be arbitrarily small by picking appropriate l and N.

Now, let us consider the second case in which Eve, who has quantum capabilities, is involved. Assume that Eve can obtain both of Alice's transmissions and tries to obtain Alice's secret. If Eve gets Bob's and Charlie's qubits of certain entangled states, she may measure the two qubits in the Bell basis and then resend the qubits in the states she found to Bob and Charlie, respectively. In terms of Eq. (1), if the measurement outcome is $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, Eve learns that Alice's bit should be 0; otherwise, she knows that Alice's bit should be 1. However, Eve's cheating is likely to be detected, since she does not know Bob's and Charlie's choices. If she measures the qubits in the position, where both Bob and Charlie choose to CHECK, then the three-qubit state, which results from combining Alice's qubit and the other two reflected qubits will be the product of one single state and a Bell state but not the same as the original state $|\psi\rangle$ in the form of Eq. (1); and, thus, Alice can discover this fraud with the probability $1/2$ by measuring it in an orthogonal basis of three qubits $\{|\phi_0\rangle,|\phi_1\rangle,\ldots,|\phi_7\rangle\}$, where

$$
\begin{aligned}
|\phi_0\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}+|1\rangle\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right),\\
|\phi_1\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}-|1\rangle\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right),\\
|\phi_2\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle-|11\rangle}{\sqrt{2}}+|1\rangle\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right),\\
|\phi_3\rangle &= \frac{1}{\sqrt{2}}\left(|0\rangle\frac{|00\rangle-|11\rangle}{\sqrt{2}}-|1\rangle\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right),\\
|\phi_4\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}+|0\rangle\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right),\\
|\phi_5\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle\frac{|00\rangle+|11\rangle}{\sqrt{2}}-|0\rangle\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right),\\
|\phi_6\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle\frac{|00\rangle-|11\rangle}{\sqrt{2}}+|0\rangle\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right),\\
|\phi_7\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle\frac{|00\rangle-|11\rangle}{\sqrt{2}}-|0\rangle\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right).
\end{aligned}
\tag{7}
$$

Similarly, if Eve measures the qubits either in the position, where Bob chooses to SHARE and Charlie chooses to CHECK, or in the position, where Bob selects to CHECK and Charlie selects to SHARE, she can also be detected with probability $1/2$ by implementing a Bell measurement. However, if Eve measures the qubits in the position where both Bob and Charlie choose to SHARE, she cannot be detected. In every position, as Bob and Charlie have a probability of $1/2$ for choosing to SHARE or to CHECK, the probability that Eve's cheating is undetected is $1/4\times 1/2\times 3+1/4=5/8$. Suppose there are $m(m\leqslant N/4)$ positions where Bob should measure the qubits in a Bell basis to learn the considerable information of the secret, then Bob's cheating goes undetected with probability $(5/8)^m$, which can be small enough by choosing suitable m and N. In addition, Eve also obtains nothing about Alice's secret information even if she manages to entangle an ancilla with each qubit of Bob (or Charlie). Suppose that, in a certain position, Eve has entangled an ancilla $|0\rangle$ with $|\psi\rangle$, and both Bob and Charlie measure their qubits, then the Alice-Eve system collapses to $|00\rangle$ or $|10\rangle$, which leaks no information to Eve about Alice's qubit. Note that dishonest Bob (or Charlie) who might be quantum can also implement the operations, which resemble the ones that can be done by Eve, and Alice is still able to detect the cheating in great probability by employing similar methods.

In addition, as Refs. [21–23] said that a protocol had better satisfy complete robustness, which means that, if Eve can obtain nonzero information about the secret string, then honest participants can detect errors through tests with nonzero probability. We show the proposed randomization-based SQSS protocol is completely robust informally. Assume quantum Eve (including dishonest Bob or Charlie) attempts to obtain Alice's secret. In some positions, when Eve wants to acquire the information of Alice's qubit by applying some operations on the other two qubits, then her act inevitably causes a disturbance to the state of the entire system. If at least one honest participant chooses to reflect his qubits in such positions, Alice could discover Eve's cheating through performing appropriate measurements. For example, if Bob and Charlie choose to reflect their qubits, then Alice may discover the three-qubit entangled state changed by using a joint measurement of three qubits shown in Eq. (7). Even if Eve might be dishonest Bob (Charlie), Alice is also likely to find the correlation between Alice's qubit and Charlie's (Bob's) qubit varied by implementing a Bell measurement if Charlie (Bob) reflects his qubit.

Particularly, notice that it is indispensable for Alice to announce that she has received all the reflected qubits in step iii. If Eve can learn which qubits were reflected by Bob and Charlie and in which order they were reflected before Alice receives the reflected qubits, she can obtain the secret string of Alice without producing errors by using the similar method to attack the mock protocol in Refs. [21–23]. For each incoming qubit of Bob, she entangles an ancilla $|0\rangle$ with it and implements a controlled-NOT operation on them (Bob's qubit as the control qubit and the ancilla qubit as the target qubit). Then, she holds all the qubits that Bob reflected until Bob publishes which qubits were reflected and in which order they were reflected. Next, she rearranges the reflected qubits in the same order as Alice sent them to Bob and performs another controlled-NOT operation on each returned qubit and the corresponding ancilla. After that, she resends the resulting qubits in the order that Bob declared to Alice. Finally, in the position where Bob chose to SHARE, she measures her ancilla and learns Bob's bit. For the qubits sent to Charlie, Eve does similar operations and learns Charlie's bits. In the position where both Bob and Charlie chose to SHARE, Eve can obtain the SHARE bit by implementing the XOR operation on their bits according to Eq. (1). Moreover, Eve goes undetected, since she introduces no errors.

IV. MEASURE-RESEND SQSS PROTOCOL

In the following, a measure-resend SQSS protocol is introduced. Quantum Alice can prepare the three-qubit GHZ-type state $|\psi\rangle$ and can perform certain quantum operations on the qubits. Classical parties, Bob and Charlie, are restricted to performing three operations: (1) measuring the qubits in

the classical basis; (2) preparing (fresh) qubits in the classical basis; (3) sending or returning the qubits without disturbance. This protocol is quite similar to the randomization-based SQSS protocol except that step ii and step iv are adapted to the different restrictions of classical participants, so the modified steps are given as follows:

(ii) When Bob (or Charlie) receives each qubit, he randomly determines, either to measure it in the classical basis and return it in the same state he found (SHARE) it, or to reflect it directly (CHECK).

(iv) Bob and Charlie declare the positions in which the qubits were measured (or reflected).

The proposed measure-resend SQSS protocol is secure against eavesdropping in a way similar to that in the randomization-based SQSS protocol. A dishonest classical party Bob (or Charlie) should not find Alice's secret without collaborating with the other party. Furthermore, the eavesdropper Eve (including malicious Bob or Charlie) who has quantum capabilities also should not be able to obtain Alice's secret without disturbance. Suppose classical Bob is dishonest, and he has controlled both of Alice's transmissions. In some of the positions, Bob measures both qubits in the classical basis and resends one of them to Charlie. However, if Charlie does not measure the qubits in such positions, the Alice-Charlie system should collapse to the Bell states but not to the product states, which might be discovered by Alice through implementing Bell measurements. Likewise, assume that quantum Eve (who could also be dishonest Bob or Charlie) has managed to obtain both Bob's and Charlie's qubits. In certain positions, Eve measures the two qubits in the Bell basis and then resends the qubits to Bob and Charlie, respectively. However, if at least one honest participant does not measure his qubits in such positions, Alice would be able to discover Eve's cheating through performing appropriate measurements. In addition, even if Eve manages to entangle an ancilla with each three-qubit entangled state $|\psi\rangle$, she also obtains nothing about Alice's bits, since the ancilla states are always left unchanged in the positions, where both Bob and Charlie measure their qubits.

In addition, the measure-resend SQSS protocol can also be completely robust, since, if quantum Eve wants to obtain the nonzero information of Alice's qubit by implementing operations on the other two qubits, disturbance may be introduced to the three-qubit entangled state or the correlation between Alice's qubit and the honest participant's qubit, and that can be detected by Alice with nonzero probability.

Note that it is still significant to demand Alice to publish that she has received all the reflected qubits in step iii of this protocol. If this requirement is lost, Eve can cheat successfully. For instance, Eve holds the reflected qubits from Bob and Charlie until they announce the positions in which the qubits were measured and resent (SHARE), or reflected directly (CHECK). Then, Eve measures the qubits that they measured and further resends them in the states she found, and reflects the qubits that they reflected without disturbance. In the position, where both Bob and Charlie measured their qubits, Eve learns Alice's bit must be 0 if her measurements are the same; otherwise, she learns that Alice's bit must be 1. In this case, Eve can escape from being detected, since she does not introduce disturbance anywhere.

V. CONCLUSION AND DISCUSSION

We have introduced a maximally entangled GHZ-type state and have shown that it can be produced by using the quantum circuit. Moreover, we have used such GHZ-type states to propose two SQSS protocols in which Alice has quantum capabilities, while the other two parties, Bob and Charlie, are limited to classical operations: measuring qubits in the classical basis, sending or reflecting qubits without disturbance, reordering some qubits, or preparing fresh qubits after measurements and resending them. The proposed protocols have also been shown to be secure against eavesdropping. Since the proposed SQSS protocols do not require all the participants to own quantum capabilities, the secret sharing can be achieved at a lower cost. Therefore, the applicability of secret sharing could be widen to the situation in which not all the participants can afford expensive quantum resources and quantum operations.

Nevertheless, we just consider the case that quantum Alice shares a secret with two classical parties, Bob and Charlie. An interesting question is: Can a general SQSS protocol in which quantum Alice shares a secret with several parties who may be quantum or classical be achieved? Additionally, we only show the robustness of the proposed SQSS protocols informally. So another interesting question is: How to give a formal proof of robustness for an SQSS protocol?

ACKNOWLEDGMENTS

We thank S. Muralidharan, L. Lin, J. Zhang, J. X. Li, Y. X. Long, and B. H. Wang for helpful discussions and suggestions. We also want to express our gratitude to anonymous referees for their valuable and constructive comments. This work was sponsored by the Faculty Research (Grant No. FRG2/08-09/070) Hong Kong Baptist University.

[1] G. R. Blakley, in *Proceedings of National Computer Conference* (AFIPS, New York, 1979), Vol. 48, p. 313.

[2] A. Shamir, Commun. ACM **22**, 612 (1979).

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

[4] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of Universe*, edited by M. Kaftos (Kluwer, Dordrecht, 1989); D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

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

[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[7] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[8] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).
[9] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).
[10] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).
[11] Z. J. Zhang and Z. X. Man, Phys. Rev. A **72**, 022303 (2005).
[12] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[13] S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000).
[14] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).
[15] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A **324**, 420 (2004).
[16] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[17] Z. J. Zhang, Y. Li, and Z. X. Man, Phys. Rev. A **71**, 044301 (2005).
[18] S. B. Zheng, Phys. Rev. A **74**, 054303 (2006).
[19] S. Muralidharan and P. K. Panigrahi, Phys. Rev. A **78**, 062333 (2008).
[20] D. Markham and B. C. Sanders, Phys. Rev. A **78**, 042309 (2008).
[21] M. Boyer, D. Kenigsberg, and T. Mor, in *Proceedings of the First International Conference on Quantum, Nano, and Micro Technologies* (IEEE, Washington DC, 2007), p. 10.
[22] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).
[23] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, Phys. Rev. A **79**, 032341 (2009).
[24] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[25] N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998).
[26] J. S. Bell, Physics **1**, 195 (1964).
[27] V. I. Kuvshinov and A. V. Kuzmin, Phys. Lett. A **341**, 450 (2005).
[28] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, Phys. Rev. Lett. **75**, 4714 (1995).