Quantum secret-sharing protocol based on Grover's algorithm

Li-Yi Hsu
Physics Division, National Center of Theoretical Sciences, Hsinchu, Taiwan, Republic of China
(Received 11 February 2003; published 18 August 2003)

A marked state can be found with certainty in the two-qubit case of Grover's algorithm. This property is included in the proposed quantum secret-sharing protocol. In the proposed scheme, the sender prepares some initial state in private and then performs a phase shift of the marked state as the sender's bit. Then, the sender sends these two qubits to each of the two receivers. Only when the sender broadcasts the initially prepared state and then the receivers perform the corresponding inversion operation about the average, is the sender's bit faithfully revealed. Moreover, the sender can detect deception using cheat-detecting states. The proposed quantum secret-sharing protocol is shown to be secure.

DOI: 10.1103/PhysRevA.68.022306 PACS number(s): 03.67.Hk

Secret sharing addresses the following problem: Alice in Taipei wants a confidential action to take place in Seattle. She wants two agents, Bob and Charlie, to carry it out for her. However, she knows the following: (1) one of the two agents—and at most one—may be dishonest, (2) as long as the two agents work together, the honest agent will prevent the dishonest one from sabotaging the action. Consequently, she cannot entrust the two agents with the faithful message. Instead, she encrypts her message in two pieces, neither of which contains any information individually. These two agents can determine Alice's message only when they combine their encrypted messages. Recently, some research has focused on quantum secret sharing because of its potential application in quantum information theory. Hillery *et al.* originally considered quantum secret sharing via three-particle and four-particle Greenberger-Horne-Zeilinger (GHZ) states [1]. Karlsson *et al.* considered quantum secret sharing using two-particle entanglement [2]. Cleve and coworkers investigated quantum (k,n) threshold scheme [3,4]. Furthermore, they considered the connection between quantum secret sharing and quantum error-correction code [3]. Recently, Karimipour *et al.* explored quantum secret sharing using the entanglement swapping of *d*-level generalized Bell states [5]. Very recently, Cabello discussed *N*-party quantum secret sharing [6].

This study proposes a one-to-two-party quantum secret-sharing protocol based on Grover's algorithm [8]. The basic idea that underlies the proposed protocol markedly differs from the ideas that underlie the protocols mentioned above. In this protocol, Alice prepares different Bell states. In addition, the sender and the honest agent do not analyze a portion of the sequence of measurement outcomes to discover possible cheating [1]. Under error-free conditions, the sender can find cheating immediately by observing a public message of receivers' discussion result. However, in some of the above protocols, Alice can encrypt only random bits owing to the intrinsic randomness in the quantum measurement or the entanglement swapping [1,5]. In the proposed protocol, Alice can encode the wanted bits with the help of the Grover's algorithm. Moreover, since even the three-qubit Grover's algorithm has been experimentally realized [7], our quantum secret-sharing protocol based on Grover's algorithm becomes highly practical for experimental realization. Finally, through Grover's algorithm, a (2,2) threshold scheme is established.

The original two-qubit Grover's algorithm is briefly reviewed in Ref. [8]. Suppose we want to find a marked state $|w\rangle$, where w can be 00, 01, 10, or 11. The initial state $|S_1\rangle=[(1/\sqrt{2})(|0\rangle+|1\rangle)]^{\otimes 2}$ is prepared. Then, two unitary transformations U_w and $-U_{S_1}$ are transformed in that order, where $U_x=1-2|x\rangle\langle x|$, yielding

$$-U_{S_1}U_w|S_1\rangle=|w\rangle; \tag{1}$$

that is, the marked state can be found with certainty. In the proposed protocol, the two-qubit Grover's algorithm with some other initial prepared state $|S_i\rangle$, is performed. Each qubit in $|S_i\rangle$ can be in one of the following four states: $(1/\sqrt{2})(|0\rangle+|1\rangle)$, $(1/\sqrt{2})(|0\rangle-|1\rangle)$, $(1/\sqrt{2})(|0\rangle+i|1\rangle)$, and $(1/\sqrt{2})(|0\rangle-i|1\rangle)$, denoted as $|+\rangle$, $|-\rangle$, $|+i\rangle$, and $|-i\rangle$ in Table I, respectively. For simplicity, $U_w|S_i\rangle$ is represented as $|S_i\rangle_w$. Interestingly,

$$-U_{S_j}|S_j\rangle_w=a|w\rangle \tag{2}$$

holds, where a is some phase term and w can be 00, 01, 10, or 11. In other words, in Grover's algorithm, even though some other $|S_i\rangle$ is prepared, the marked state can still be found with certainty. In the following discussion, $\mathfrak{S}$ is the set of these 16 initial preparations, as shown in Table I.

This paper divides $|S_j\rangle_w$ into two classes: the message states and the cheat-detecting states. Alice encodes the classical bits 0 and 1 as the marked states $|01\rangle$ and $|10\rangle$, respectively. That is, Alice encrypts her secret bit in the state $|S_j\rangle_w$, where w is either 01 or 10. She tries to detect any possible eavesdropping using the state $|S_j\rangle_w$, where w is either 00 or 11. The procedure of the secret-sharing protocol is as follows: (1) Alice randomly prepares some initial state $|S_i\rangle \in \mathfrak{S}$, for $i=1,\ldots,16$, and then performs U_w on $|S_i\rangle$. (2) Alice sends each of the receivers, Bob and Charlie, one of the qubits. Bob and Charlie are assumed to receive the first and the second qubits, respectively. (3) Alice has to confirm that each agent has actually received the qubit via classical communication. (4) Alice announces her initial state $|S_i\rangle$ in public. (5) Only when Bob and Charlie combine their qubits and perform $-U_{S_i}$ on these two qubits can they both determine the marked state $|w\rangle$ with certainty. (6) Bob and

TABLE I. The 16 outcomes of $-U_{S_j}|S_1\rangle_{10}$, where $j=1,\ldots,16$. Here $\xi=\exp(i\pi/4)$. Only when $j=1$, must the measurement outcome be the marked state $|10\rangle$. In addition, the probability of either perfect or antiperfect correlated measurement outcomes is $\frac{1}{2}$.

j	$\|S_j\rangle$	$-U_{S_j}\|S_1\rangle_{10}$	j	$\|S_j\rangle$	$-U_{S_j}\|S_1\rangle_{10}$
1	$\|+\rangle\|+\rangle$	$\|10\rangle$	9	$\|+\rangle\|+i\rangle$	$\frac{1}{\sqrt{2}}(\xi\|00\rangle-\xi^*\|10\rangle)$
2	$\|+\rangle\|-\rangle$	$-\|00\rangle$	10	$\|+\rangle\|-i\rangle$	$\frac{1}{\sqrt{2}}(\xi^*\|00\rangle-\xi\|10\rangle)$
3	$\|-\rangle\|+\rangle$	$-\|00\rangle$	11	$\|-\rangle\|+i\rangle$	$\frac{\xi}{\sqrt{2}}(\|11\rangle+\|01\rangle)$
4	$\|-\rangle\|-\rangle$	$-\|01\rangle$	12	$\|-\rangle\|-i\rangle$	$\frac{1}{\sqrt{2}}(\xi^*\|11\rangle+\xi\|01\rangle)$
5	$\|+i\rangle\|+i\rangle$	$-\|S_1\rangle_{10}$	13	$\|+i\rangle\|+\rangle$	$\frac{1}{\sqrt{2}}(\xi^*\|00\rangle-\xi\|10\rangle)$
6	$\|+i\rangle\|-i\rangle$	$-i\|S_1\rangle_{10}$	14	$\|+i\rangle\|-\rangle$	$\frac{1}{\sqrt{2}}(\xi^*\|00\rangle+\xi\|01\rangle)$
7	$\|-i\rangle\|+i\rangle$	$-i\|S_1\rangle_{10}$	15	$\|-i\rangle\|+\rangle$	$\frac{1}{\sqrt{2}}(\xi\|11\rangle-\xi^*\|10\rangle)$
8	$\|-i\rangle\|-i\rangle$	$-i\|S_1\rangle_{10}$	16	$\|-i\rangle\|-i\rangle$	$\frac{1}{\sqrt{2}}(\xi\|00\rangle+\xi^*\|01\rangle)$

Charlie discuss whether their outcomes are perfectly correlated (w is either 00 or 11) or anti-perfectly correlated (w is either 01 or 10). (7) If Bob and Charlie find that their outcomes are perfectly correlated, then each of them is required to inform Alice over a classical channel, respectively. A few notes regarding this protocol are important.

(1) In step 1, Alice has to prepare some $|S_i\rangle_w$. All $|S_i\rangle_w$ states are maximally entangled states. Hence, Alice can perform her preparation as follows. Alice can prepare the singlet state and then performs some necessary local operation on one of the two qubits. In this way, Alice can prepare any $|S_i\rangle_w$.

(2) The main point is that Alice does not broadcast her initial preparation until she makes sure that both receivers have received their respective qubits. Alice can expect that the honest receiver will convey the faithful message in public. Therefore, Alice knows whether the honest receiver has received a qubit. The dishonest receiver must also announce that he has also received a qubit. Otherwise, Alice will not announce her preparation. As a result, Alice's confirmation guarantees that the honest receiver receives a qubit. After Alice broadcasts the initial preparation, the honest receiver(s) can combine his qubit with the other qubit to perform $-U_{S_i}$. As previously mentioned, the honest receiver will prevent the dishonest one from causing any damage if they perform the collective operation $-U_{S_i}$ together. In other words, the dishonest receiver cannot perform any deception in the collective operation $-U_{S_i}$.

(3) After the operation $-U_{S_i}$ is performed, both receivers have to perform the respective local measurements in the computational basis. Suppose that both Bob and Charlie are honest. In this case, Bob and Charlie share the secret bit 0 (1) with Alice if their outcomes are 0 (1) and 1 (0), respectively. They do not need any further discussion on their outcomes after they have performed their own local measurements. However, one receiver may be dishonest. The dishonest one may access the secret bits without being aware of it. Therefore, the sender and the honest receiver must make every effort to detect any possible eavesdropping. A means of detecting eavesdropping is suggested here. Notably, Alice encrypts her one-bit information in two qubits; that is, the marked state is either $|01\rangle$ or $|10\rangle$, which are anti-perfectly correlated. As previously stated, $|S_i\rangle_w$, where w is either 00 or 11, are regarded as cheat-detecting states. Using cheat-detecting codes, Alice does not encrypt any secret information if the marked state is either $|00\rangle$ or $|11\rangle$. Rather, using cheat-detecting codes, the sender can detect the possible eavesdropping.

Alice can detect possible eavesdropping as follows. As in the proposal of Hillery *et al.*, Bob and Charlie must discuss whether their outcomes are perfectly or antiperfectly correlated. If the honest receiver finds that the outcomes are perfectly correlated, he concludes that either Alice has prepared the cheat-detecting state, or some eavesdropping has occurred. Therefore, in step 7, Bob and Charlie are required to tell Alice their perfectly correlated outcomes over a classical channel, respectively. In addition, the dishonest receiver can monitor but cannot alter the classical public messages. As a result, Alice can at least receive the honest receiver's true outcome. The dishonest receiver cannot perform any cheating by announcing a false outcome or making no announcement. However, Alice expects that both receivers will broadcast their outcomes if she has prepared a cheat-detecting state. Therefore, Alice will be aware of any cheating behavior that disturbs the qubits and changes of the correlation of outcomes.

In some quantum secret protocols [1,2], the honest receiver can determine cheating only after the two receivers have discussed a public portion of the sequence of measurement basis and outcomes. The honest receiver can discern cheating by statistical violation of the outcome sequence. An important advantage of the proposed protocol is that the honest receiver can discern possible cheating immediately.

(4) In step 6, the dishonest receiver could deliberately declare the wrong outcomes. However, such cheating will be detected since it leads to a change in the correlation of outcomes. Therefore, the dishonest receiver does not benefit from lying about his outcomes.

(5) In some sense, the two-qubit Grover's algorithm is used to find the state that corresponds to the phase error. Consequently, the proposed scheme hides the secret bit in a phase-flip error. Notably, however, since $-U_{S_i}$ is a unitary transformation,

$$-U_{S_i}-U_{S_i}|w\rangle=|w\rangle. \tag{3}$$

Therefore, the proposed protocol can be regarded as encoding and decoding the secret bit by the same collective operation $-U_{S_i}$. In general, $|S_i\rangle_w$ is a linear superposition of the four marked state candidates with a phase error. In addition, the message states are equivalent to cheat-detecting states. That is, for some different i and i',

$$U_{w_1}|S_i\rangle = U_{w_2}|S_{i'}\rangle, \tag{4}$$

where w_1 is either 00 or 11 and w_2 is either 01 or 10.

The following discussion involves two cases. First, for illustration, Alice prepares either $|S_1\rangle_w$ or $|S_5\rangle_w$. Such preparation will be shown to suffice the proposed protocol. Second, the most generalized case is considered. That is, Alice can prepare any possible $|S_i\rangle_w$, where i can be 1,2, . . . ,16.

For illustration, let the initial state prepared by Alice be either $|S_1\rangle_w$ or $|S_5\rangle_w$. Bob is assumed to be the dishonest receiver. His aim is to discover Alice's secret bit without Charlie's assistance, and to do so in a way that cannot be detected [1]. He intercepts Charlie's qubit, and then he performs either $-U_{S_1}$ or $-U_{S_5}$ on the two qubits. If Bob chooses the wrong $-U_{S_j}$, then

$$-U_{S_j}|S_i\rangle_w = -|S_i\rangle, \tag{5}$$

where w is 01 or 10, and $(i, j)=(1,5)$ or $(5,1)$. In addition, it is easy to verify that

$$(-U_{S_5})|S_1\rangle_{00} = -i|S_1\rangle_{11}, \tag{6}$$

$$(-U_{S_5})|S_1\rangle_{11} = i|S_1\rangle_{00}, \tag{7}$$

$$(-U_{S_1})|S_5\rangle_{00} = i|S_5\rangle_{11}, \tag{8}$$

$$(-U_{S_1})|S_5\rangle_{11} = -i|S_5\rangle_{00}. \tag{9}$$

If Bob performs the wrong collective operation $-U_{S_{j'}}$, he can access the secret information only with probability $\frac{1}{4}$. Assume that Alice prepares cheat-detecting states or message states with equal probability, and that dishonest Bob performs $-U_{S_5}$ or $-U_{S_1}$ with equal probability. Under some conditions, Alice can immediately detect cheating: (1) Alice prepares a message state but honest Charlie finds perfectly correlated outcomes. (2) Alice prepares a cheat-detecting state but honest Charlie finds antiperfectly correlated outcomes. (3) Alice prepares a cheat-detecting state and honest Charlie finds perfectly correlated outcomes. However, both receivers broadcast the outcomes that differ from her preparation. In this way, Alice can immediately find the cheating with probability $\frac{5}{16}$.

Furthermore, Charlie's ability of detecting Bob's cheating can be improved: Alice prepares some initial state $|S_i\rangle \in \mathfrak{S}$ randomly. Then Alice performs U_w on $|S_j\rangle_w$, w is either 01 or 10. Here Bob intercepts Charlie's qubit and he does not perform any measurement before Alice's announcement. Instead, he prepares some $|x\rangle = |S_{j'}\rangle_{w'}$ and then sends the corresponding qubit in $|x\rangle$ to Charlie. For example, let $|x\rangle$ be $|S_1\rangle_{10}$. Now Bob and Charlie together perform the correct $-U_{S_j}$ on $|x\rangle$. Table I lists all $-U_{S_j}|S_1\rangle_{10}$. According to Table I, after $-U_{S_j}|S_1\rangle_{10}$ is performed, Charlie and Bob can be easily verified to be able to measure either $|00\rangle$ or $|11\rangle$ with probability $\frac{1}{2}$. That is, the sender and the honest receiver can immediately detect such cheating with probability $\frac{1}{2}$.

Now, let dishonest Bob intercept Charlie's qubit and perform some collective operation $-U_{S_j}$. According to Table I, Bob can access exactly the marked state without Charlie's assistance and detection only when Bob performs the correct $-U_{S_i}$. Moreover, assume that Bob performs the measurement on the qubits in the computational basis. Using simple algebra, the probability that Bob knows either Alice's secret bit or incorrect bit can be verified as being $\frac{1}{4}$ [Bob is assumed to perform any of the 16 $-U_{S_i}$s with equal probability]. However, Alice can detect Bob's cheating with probability $\frac{1}{2}$. Since Bob cannot gain more information than that by making a random guess, the proposed quantum secret-sharing protocol guarantees high security for secret sharing.

Another means of cheating is considered. As previously stated, all possible $|S_i\rangle_w$ are Bell states. Cheating Bob intercepts Charlie's qubit. In addition, Bob prepares a singlet state and sends Charlie a qubit of the singlet state. Then Bob performs the necessary unitary transformation on his qubit immediately after Alice' broadcasts of S_i. However, four preparations are possible, $|S_i\rangle_{00}$, $|S_i\rangle_{11}$, $|S_i\rangle_{01}$, and $|S_i\rangle_{10}$. Since dishonest Bob does not know what the marked state is, Bob is assumed to be able to prepare some $|S_i\rangle_w$ with probability $\frac{1}{4}$. If Alice prepares a message state, she can detect such cheating with probability $\frac{1}{2}$ when Bob prepares a cheat-detecting state. However, if Alice prepares a cheat-detecting state, she can detect such cheating with probability $\frac{3}{4}$ when Bob prepares any other wrong state. On average, Alice can detect such an attack with probability $\frac{5}{8}$. Again, dishonest Bob does not know Alice's preparation in advance. In other words, Alice is expected to prevent the Trojan horse attacks quite well [12]. Alice's detection is not based on the statistical violation of an outcome sequence, but on the correlation of the outcomes of every qubit pair. Alice can tell Bob and Charlie in public whether deception has occurred.

Other eavesdropping strategies are considered. For example, dishonest Bob can use the intercept-resend strategy with orthogonal measurements [9]. Suppose Bob perform the collective measurement in the either basis $\{|-+++\rangle, |+-++\rangle, |++-+\rangle, |+++-\rangle\}$ or $\{|--(+i)(+i)\rangle, |++(+i)(+i)\rangle, |+-(-i)(+i)\rangle, |+-(+i)(-i)\rangle\}$, where $|-+++\rangle = \frac{1}{2}(-|00\rangle+|11\rangle+|01\rangle+|10\rangle)$ and $|--(+i)(+i)\rangle = \frac{1}{2}(-|00\rangle-|11\rangle+i|01\rangle+i|10\rangle)$, and so on. For illustration, Alice is assumed to prepare either $|S_1\rangle_w$ or $|S_5\rangle_w$ and Bob decides to perform the orthogonal measurement in the basis $\{|-+++\rangle, |+-++\rangle, |++-+\rangle, |+++-\rangle\}$. If Alice prepares $|S_1\rangle_w$, then Bob can eavesdrop on the message without being detected [10]. However, if Alice prepares $|S_5\rangle_w$, such a state projects into any measurement basis with equal probability $\frac{1}{4}$. As a result, even after Alice broadcasts S_5, dishonest Bob cannot gain any

knowledge of w from his dishonest operation. As a result, Bob can obtain Alice's secret information with probability $\frac{5}{8}$. However, as previously said, Alice can detect Bob's cheating with the probability $\frac{5}{8}$ if Bob resends one qubit of the singlet state to Charlie. In addition, suppose that Alice prepares every possible $|S_i\rangle_w$, where i can be 1, 2, . . . , 16 and w can be 00, 11, 01, and 10, with equal probability. Dishonest Bob intercepts the two qubits and measures them in the basis $\{|-+++\rangle, |+-++\rangle, |++-+\rangle, |+++-\rangle\}$. Consequently, whatever the outcome, dishonest Bob will gain no information about the correlation of the marked state since he can only infer that the probability associated with either the perfectly correlated marked state ($|00\rangle$ or $|11\rangle$) or the antiperfectly correlated marked state ($|01\rangle$ or $|10\rangle$) is $\frac{1}{2}$.

Some eavesdropping strategies are based on entanglement [9,11]. Here Bob's making his qubit entangled with another qubit initially set as $|0\rangle_{b'}$ is considered. Suppose Alice prepares $|S_1\rangle_{w=01}$ and Bob entangles the sent qubit with another auxiliary qubit $|0\rangle_{b'}$ using a controlled-NOT gate. Then, $|S_1\rangle_{w=01}\otimes|0\rangle_{b'}$ becomes

$$|S_1\rangle_{w=01}\otimes|0\rangle_{b'}\rightarrow|S_1\rangle_{w=01,b'}=\frac{1}{\sqrt{2}}(|0\rangle|-\rangle|0\rangle_{b'}+|1\rangle|+\rangle|1\rangle_{b'}). \quad (10)$$

Suppose, then, that Bob does nothing. Charlie and Bob perform $(-U_{S_1})$ together.

$$(-U_{S_1}\otimes\mathbf{1})(|S_1\rangle_{w=01,b'})=\frac{1}{2}[-(|00\rangle-|w\rangle)|0\rangle_{b'}+(|00\rangle+|w\rangle)|1\rangle_{b'}]. \quad (11)$$

Therefore, Alice can detect Bob's entanglement with probability $\frac{1}{2}$. Moreover, by simple algebra, for any $(-U_{S_i}\otimes\mathbf{1})$, $i=1,\ldots,16$, the outcome of $(-U_{S_i}\otimes\mathbf{1})(|S_1\rangle_{w=01,b'})$ is either $|00\rangle$ or $|11\rangle$ with probability $\frac{1}{2}$. Furthermore, suppose that Bob performs some $(-U_{S_1}\otimes\mathbf{1})$, Charlie can still detect Bob's entanglement by measuring $|00\rangle$ or $|11\rangle$ with probability $\frac{1}{2}$.

In conclusion, a one-to-two-party quantum secret-sharing protocol, based on Grover's algorithm, is considered. Some possible eavesdropping strategies of the dishonest receiver are investigated. The proposed protocol is shown to resist these attacks. In addition, the dishonest receiver gains no information without the assistance of the honest one. Our protocol works even if Alice prepares either $|S_1\rangle_w$ or $|S_5\rangle_w$.

The author would like to thank Mark Hillery for his valuable comments.

[1] M. Hillery, V. Buzěk, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[2] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[3] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[4] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[5] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).
[6] A. Cabello, Phys. Rev. Lett. **89**, 100402 (2002).
[7] L.M.K. Vandersypen, M. Steffen, M.H. Sherwood, C.S. Yannoni, G. Breyta, and I.L. Chuang, Appl. Phys. Lett. **76**, 646 (2000).
[8] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
[9] A.K. Ekert, B. Huttner, G.M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[10] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).
[11] J.I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).