Quantum secret sharing between multiparty and multiparty without entanglement

Feng-Li Yan[1,2] and Ting Gao[2,3,4]
[1]*College of Physics, Hebei Normal University, Shijiazhuang 050016, China*
[2]*CCAST (World Laboratory), P.O. Box 8730, Beijing 100080, China*
[3]*College of Mathematics and Information Science, Hebei Normal University, Shijiazhuang 050016, China*
[4]*Department of Mathematics, Capital Normal University, Beijing 100037, China*
(Received 18 February 2005; published 7 July 2005)

We propose a quantum secret sharing protocol between multiparty (m members in group 1) and multiparty (n members in group 2) using a sequence of single photons. These single photons are used directly to encode classical information in a quantum secret sharing process. In this protocol, all members in group 1 directly encode their respective keys on the states of single photons via unitary operations; then, the last one (the mth member of group 1) sends $1/n$ of the resulting qubits to each of group 2. Thus the secret message shared by all members of group 1 is shared by all members of group 2 in such a way that no subset of each group is efficient to read the secret message, but the entire set (not only group 1 but also group 2) is. We also show that it is unconditionally secure. This protocol is feasible with present-day techniques.

DOI: 10.1103/PhysRevA.72.012304 PACS number(s): 03.67.Dd, 03.67.Hk, 89.70.+c

I. INTRODUCTION

Suppose two groups such as two government departments, where there are m and n members, respectively, want to correspond with each other, but members of each group do not trust each other. What can they do? Classical cryptography gives an answer which is known as secret sharing [1]. It can be used to guarantee that no single person or part of each department can read out the secret message, but all members of each group can. This means that for security to be breached, all people of one group must act in concert, thereby making it more difficult for any single person who wants to gain illegal access to the secret information. It can be implemented as follows: from his original message, every person (called sender) of group 1 separately creates n coded messages and sends each of them to each member (called receiver) of group 2. Each of the encrypted message contains no information about the senders' original message, but the combination of all coded messages contains the complete message of group 1. However, either a $(m+n+1)$th party (an "external" eavesdropper) or the dishonest member of two groups who can gain access to all senders' transmissions can learn the contents of their (all senders) message in this classical procedure. Fortunately, quantum secret sharing protocols [2–5] can accomplish distributing information securely where multiphoton entanglement is employed. Recently, many kinds quantum secret sharing with entanglement have been proposed [6–10]. Lance *et al.* have reported an experimental demonstration of a (2,3) threshold quantum secret sharing scheme [11]. The combination of a quantum key distribution (QKD) and classical sharing protocol can realize secret sharing safely. Quantum secret sharing protocol provides for secure secret sharing by enabling one to determine whether an eavesdropper has been active during the secret sharing procedure. But it is not easy to implement such multiparty secret sharing tasks [2,6], since the efficiency of preparing even tripartite or four-partite entangled states is very low [12,13]; at the same time, the efficiency of the existing quantum secret sharing protocols using quantum entanglement can only approach 50%.

More recently, a protocol for quantum secret sharing without entanglement has been proposed by Guo and Guo [14]. They present an idea to directly encode the qubit of the quantum key distribution and accomplish one splitting of a message into many parts to achieve multiparty secret sharing only by product states. The theoretical efficiency is doubled to approach 100%. Brádler and Dušek have given two protocols for secret-information splitting among many participants [15].

In this paper, we propose a quantum secret sharing scheme employing single qubits to achieve the aim mentioned above—the secret sharing between multiparty (m parties of group 1) and multiparty (n parties of group 2). That is, instead of giving his information to any one individual of group 1, each sender splits his information in such a way that no members of group 1 or group 2 have any knowledge of the combination of all senders (group 1), but all members of each group can jointly determine the combination of all senders (group 1). The security of our scheme is based on the quantum no-cloning theory just as the BB84 quantum key distribution. Comparing with the efficiency 50% limiting for the existing quantum secret sharing protocols with quantum entanglement, the present scheme can also be 100% efficient in principle.

II. QUANTUM KEY SHARING BETWEEN MULTIPARTY AND MULTIPARTY

Suppose there are $m(m\geqslant 2)$ and $n(n\geqslant 2)$ members in government department 1 and department 2, respectively, and Alice 1, Alice 2, …, Alice m and Bob 1, Bob 2, …, Bob n are their respective all members. m parties of department 1 want quantum key sharing with n parties of department 2 such that neither one nor part of each department knows the key, but only by all members working together can each department determine what the string (key) is. In this case it is the quantum information that has been split into n pieces, no one of which separately contains the original information, but whose combination does.

Alice 1 begins with A_1 and B_1, two strings each of nN random classical bits. She then encodes these strings as a block of nN qubits,

$$|\Psi^1\rangle = \otimes_{k=1}^{nN}|\psi_{a_k^1 b_k^1}\rangle = \otimes_{j=0}^{N-1}|\psi_{a^1_{nj+1}b^1_{nj+1}}\rangle|\psi_{a^1_{nj+2}b^1_{nj+2}}\rangle\cdots|\psi_{a^1_{nj+n}b^1_{nj+n}}\rangle, \quad (1)$$

where a_k^1 is the kth bit of A_1 (and similar for B_1) and each qubit is one of the four states

$$|\psi_{00}\rangle = |0\rangle, \quad (2)$$

$$|\psi_{10}\rangle = |1\rangle, \quad (3)$$

$$|\psi_{01}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad (4)$$

$$|\psi_{11}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \quad (5)$$

The effect of this procedure is to encode A_1 in the basis $Z=\{|0\rangle,|1\rangle\}$ or $X=\{|+\rangle,|-\rangle\}$, as determined by B_1. Note that the four states are not all mutually orthogonal; therefore, no measurement can distinguish between all of them with certainty. Alice 1 then sends $|\Psi^1\rangle$ to Alice 2 over their public quantum communication channel.

Depending on a string A_2 of nN random classical bits which she generates, Alice 2 subsequently applies a unitary transformation $\sigma_0=I=|0\rangle\langle 0|+|1\rangle\langle 1|$ (if the kth bit a_k^2 of A_2 is 0) or $\sigma_1=i\sigma_y=|0\rangle\langle 1|-|1\rangle\langle 0|$ (if $a_k^2=1$) on each $|\psi_{a_k^1 b_k^1}\rangle$ of the nN qubits she receives from Alice 1 such that $|\psi_{a_k^1 b_k^1}\rangle$ is changed into $|\psi^0_{a_k^2 b_k^1}\rangle$, and obtains nN-qubit product state $|\Psi^{20}\rangle=\otimes_{k=1}^{nN}|\psi^0_{a_k^2 b_k^1}\rangle$. After that, she performs a unitary operator I (if $b_k^2=0$) or $H=(1/\sqrt{2})(|0\rangle+|1\rangle)\langle 0|+(1/\sqrt{2})(|0\rangle-|1\rangle)\langle 1|$ (if $b_k^2=1$) on each qubit state $|\psi^0_{a_k^2 b_k^1}\rangle$ according to her another random classical bits string B_2 and makes $|\psi^0_{a_k^2 b_k^1}\rangle$ to be turned into $|\psi_{a_k^2 b_k^2}\rangle$. Alice 2 sends Alice 3 $|\Psi^2\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^2 b_k^2}\rangle$. Similar to Alice 2, Alice 3 applies quantum operations on each qubit and sends the resulting nN qubits to Alice 4. This procedure goes on until Alice m.

Similarly, Alice m first creates two strings A_m and B_m of nN random classical bits. Then she makes a unitary operation σ_0 (if $a_k^m=0$) or σ_1 (if $a_k^m=1$) on each qubit state $|\psi_{a_k^{m-1}b_k^{m-1}}\rangle$. It follows that $|\psi_{a_k^{m-1}b_k^{m-1}}\rangle$ is changed into $|\psi^0_{a_k^m b_k^{m-1}}\rangle$. After that, she applies operator I (if $b_k^m=0$) or H (if $b_k^m=1$) on the resulting qubit state $|\psi^0_{a_k^m b_k^{m-1}}\rangle$ such that $|\psi^0_{a_k^m b_k^{m-1}}\rangle$ is turned into $|\psi_{a_k^m b_k^m}\rangle$. Alice m sends N-qubit product states $|\Psi_1^m\rangle = \otimes_{j=0}^{N-1}|\psi_{a^m_{nj+1}b^m_{nj+1}}\rangle, |\Psi_2^m\rangle = \otimes_{j=0}^{N-1}|\psi_{a^m_{nj+2}b^m_{nj+2}}\rangle, \ldots, |\Psi_n^m\rangle = \otimes_{j=0}^{N-1}|\psi_{a^m_{nj+n}b^m_{nj+n}}\rangle$ of the resulting nN-qubit state $|\Psi^m\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^m b_k^m}\rangle$ to Bob 1, Bob 2, …, Bob n, respectively.

When all Bob 1, Bob 2, …, Bob n have announced the receiving of their strings of N qubits, Alice 1, Alice 2, …, Alice m publicly announce the strings $B_1,B_2,\ldots,B_m$ one after another, respectively. Note that $B_1,B_2,\ldots,B_m$ reveal nothing about A_i $(i=1,2,\ldots,m)$, but it is important that all Alice 1, Alice 2, …, Alice m not publish their respective $B_1,B_2,\ldots,B_m$ until after all Bob 1, Bob 2, …, Bob n announce the reception of the N qubits Alice m sends to them.

Bob 1, Bob 2, …, Bob n then measure each qubit of their respective strings in the basis X or Z according to the XOR result of corresponding bits of strings $B_1,B_2,\ldots,B_m$. Since the unitary transformation $\sigma_1=i\sigma_y$ flips the states in both measuring bases such that $\sigma_1|0\rangle=-|1\rangle$, $\sigma_1|1\rangle=|0\rangle$, $\sigma_1|+\rangle=|-\rangle$, and $\sigma_1|-\rangle=-|+\rangle$, i.e., $I,i\sigma_y$ leave bases X and Z unchanged, but H turns $|0\rangle,|1\rangle,|+\rangle$, and $|-\rangle$ into $|+\rangle$, $|-\rangle,|0\rangle$, and $|1\rangle$, respectively, i.e., H changes bases X and Z, so if $\oplus_{i=2}^m b_k^i=b_k^2\oplus b_k^3\oplus\cdots\oplus b_k^m=0$, then $|\psi_{a_k^m b_k^m}\rangle$ should be measured in the same basis with $|\psi_{a_k^1 b_k^1}\rangle$; if $\oplus_{i=2}^m b_k^i=1$, $|\psi_{a_k^m b_k^m}\rangle$ should be measured in the basis different from $|\psi_{a_k^1 b_k^1}\rangle$, where the symbol $\oplus$ is the addition modulo 2. Therefore, if $\oplus_{i=2}^m b_k^i=b_k^1$, $|\psi_{a_k^m b_k^m}\rangle$ is measured in the Z basis, otherwise in the basis X. That is, if $\oplus_{i=1}^m b^i_{nj+l}=0$, then Bob l measures $|\psi_{a^m_{nj+l}b^m_{nj+l}}\rangle$ in the basis Z; otherwise, he measures in the basis X. Moreover, after measurements, Bob l can extract out all Alices's encoding information $\oplus_{i=1}^m a^i_{nj+l}$, $j=0,1,2,\ldots,N-1$, for $l=1,2,\ldots,n$.

Now all Alices and Bobs perform some tests to determine how much noise or eavesdropping happened during their communication. Alice 1, Alice 2, …, Alice m select some bits nj_r+l (of their nN bits) at random and publicly announce the selection. Here $j_r\in\{j_1,j_2,\ldots,j_{r_0}\}\subset\{j_1,j_2,\ldots,j_{r_0},j_{r_0+1},\ldots,j_N\}=\{0,1,2,\ldots,N-1\}$ and $l=1,2,\ldots,n$. All Bobs and all Alices then publish and compare the values of these checked bits. If they find too few the XOR results $\oplus_{i=1}^m a^i_{nj_r+l}$ of the corresponding bits $a^i_{nj_r+l}$ of these checked bits of all Alices and the values of Bob l's checked bits $|\psi_{a^m_{nj_r+l}b^m_{nj_r+l}}\rangle$ agree, then they abort and retry the protocol from the start. The XOR results $\oplus_{l=1}^n(\oplus_{i=1}^m a^i_{nj_s+l})$ of Bob l's corresponding bits $\oplus_{i=1}^m a^i_{nj_s+l}$ of the rest unchecked bits nj_s+l of $\{\oplus_{i=1}^m a^i_{nj+1}\}_{j=0}^{N-1}, \{\oplus_{i=1}^m a^i_{nj+2}\}_{j=0}^{N-1},\ldots,\{\oplus_{i=1}^m a^i_{nj+n}\}_{j=0}^{N-1}$ (or $\otimes_{j=0}^{N-1}|\psi_{a^m_{nj+1}b^m_{nj+1}}\rangle, \otimes_{j=0}^{N-1}|\psi_{a^m_{nj+2}b^m_{nj+2}}\rangle,\ldots,\otimes_{j=0}^{N-1}|\psi_{a^m_{nj+n}b^m_{nj+n}}\rangle$) can be used as raw keys for secret sharing between all Alices and all Bobs, where $j_s=j_{r_0+1},j_{r_0+2},\ldots,j_N$.

This protocol is summarized as follows.

(M1) Alice 1 chooses two random nN-bit strings A_1 and B_1. She encodes each data bit of A_1 as $\{|0\rangle,|1\rangle\}$ if the corresponding bit of B_1 is 0 or $\{|+\rangle,|-\rangle\}$ if B_1 is 1. Explicitly, she encodes each data bit 0 (1) of A_1 as $|0\rangle$ ($|1\rangle$) if the corresponding bit of B_1 is 0 or $|+\rangle$ ($|-\rangle$) if the corresponding bit of B_1 is 1; i.e., she encodes each bit a_k^1 of A_1 as $|\psi_{a_k^1 b_k^1}\rangle$ of Eqs. (2)–(5), where b_k^1 is the corresponding bit of B_1. Then she sends the resulting nN-qubit state $|\Psi^1\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^1 b_k^1}\rangle$ to Alice 2.

(M2) Alice 2 creates two random nN-bit strings A_2 and B_2. She applies σ_0 or σ_1 to each qubit $|\psi_{a_k^1 b_k^1}\rangle$ of nN-qubit state $|\Psi^1\rangle$ according to the corresponding bit of A_2 being 0 or 1; then, she applies I or H to each qubit of the resulting nN-qubit state depending on the corresponding bit of B_2 being 0 or 1. After this, she sends Alice 3 the resulting nN-qubit state $|\Psi^2\rangle$.

(M3) Alice i does likewise, $i=3,4,\ldots,m-1$. Depending on the corresponding bit a_k^m of a random nN-bit string A_m, which she generates on her own, Alice m performs σ_0 (if $a_k^m=0$) or σ_1 (if $a_k^m=1$) on each qubit of $|\Psi^{m-1}\rangle$. According to a random bit string B_m which she generates, she subsequently applies I (if the corresponding bit b_k^m of B_m is 0) or H (if $b_k^m=1$) on each qubit of the resulting nN-qubit state $|\Psi^{m0}\rangle$, which results in nN-qubit state $|\Psi^m\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^m b_k^m}\rangle$. After it, she sends N-qubit state $\otimes_{j=0}^{N-1}|\psi_{a_{nj+l}^m b_{nj+l}^m}\rangle$ to Bob l, $1\leqslant l\leqslant n$.

(M4) Bob 1, Bob 2, …, Bob n receive N qubits and announce this fact, respectively.

(M5) Alice 1, Alice 2, …, Alice m publicly announce the strings $B_1,B_2,\ldots,B_m$, respectively.

(M6) Bob 1, Bob 2, …, Bob n measure each qubit of their respective strings in the basis Z or X according to the XOR results of corresponding bits of strings $B_1,B_2,\ldots,B_m$. That is, Bob l measures $|\psi_{a_{nj+l}^m b_{nj+l}^m}\rangle$ in the basis Z (if $\oplus_{i=1}^m b_{nj+l}^i=0$) or in the basis X (if $\oplus_{i=1}^m b_{nj+l}^i=1$), $j=0,1,\ldots,N-1$, $l=1,2,\ldots,n$.

(M7) All Alices select randomly a subset that will serve as a check on Eve's interference and tell all Bobs the bits they choose. In the check procedure, all Alices and Bobs are required to broadcast the values of their checked bits and compare the XOR results of the corresponding bits of checked bits of $A_1,A_2,\ldots,A_m$ and the values of the corresponding bits of Bob 1, Bob 2, …, Bob n. If more than an acceptable number disagree, they abort this round of operation and restart from first step.

(M8) The XOR results $\oplus_{l=1}^n(\oplus_{i=1}^m a_{nj_s+l}^i)$ of Bob l's corresponding bits $\oplus_{i=1}^m a_{nj_s+l}^i$ of the remaining bits nj_s+l of $\{\oplus_{i=1}^m a_{nj+1}^i\}_{j=0}^{N-1},\{\oplus_{i=1}^m a_{nj+2}^i\}_{j=0}^{N-1},\ldots,\{\oplus_{i=1}^m a_{nj+n}^i\}_{j=0}^{N-1}$ (or $\otimes_{j=0}^{N-1}|\psi_{a_{nj+1}^m b_{nj+1}^m}\rangle,\otimes_{j=0}^{N-1}|\psi_{a_{nj+2}^m b_{nj+2}^m}\rangle,\ldots,\otimes_{j=0}^{N-1}|\psi_{a_{nj+n}^m b_{nj+n}^m}\rangle$) can be used as key bits for secret sharing between all Alices and all Bobs, where $j_s=j_{r_0+1},j_{r_0+2},\ldots,j_N$.

For example, $m=2$ and $n=3$. Suppose $A_1=\{1,0,0,1,0,1,0,1,1,0,0,0,1,1,1,0,1,0\}$ and $B_1=\{0,1,0,1,1,0,1,1,0,0,1,0,1,0,1,0,0,1\}$ are two random 18-bit strings of Alice 1. Depending on B_1, then she encodes A_1 as $|\Psi^1\rangle=|1\rangle|+\rangle|0\rangle|-\rangle|+\rangle|1\rangle|+\rangle|-\rangle|1\rangle|0\rangle|+\rangle|0\rangle|-\rangle|1\rangle|-\rangle|0\rangle|1\rangle|+\rangle$. If Alice 2's two strings of random bits are $A_2=\{1,1,1,0,0,1,1,1,0,0,0,1,0,1,1,0,0,1\}$ and $B_2=\{1,0,0,1,1,0,0,0,1,1,1,1,0,0,0,1,0,1\}$, she applies $i\sigma_y$ to the 1st, 2nd, 3rd, 6th, 7th, 8th, 12th, 14th, 15th, 18th qubits of $|\Psi^1\rangle$, getting $|\Psi^{20}\rangle=|0\rangle|-\rangle|1\rangle|-\rangle|+\rangle|0\rangle|-\rangle|+\rangle|1\rangle|0\rangle|+\rangle|1\rangle|-\rangle|0\rangle|+\rangle|0\rangle|1\rangle|-\rangle$; then, she performs H on 1st, 4th, 5th, 9th, 10th, 11th, 12th, 16th, 18th qubits of $|\Psi^{20}\rangle$, obtaining $|\Psi^2\rangle=\otimes_{k=1}^{18}|\psi_{a_k^2 b_k^2}\rangle=|+\rangle|-\rangle|1\rangle|1\rangle|0\rangle|0\rangle|-\rangle|+\rangle|-\rangle|+\rangle|0\rangle|-\rangle|-\rangle|0\rangle|+\rangle|+\rangle|1\rangle|1\rangle$. After that, she sends the 6-qubit states $|\Psi_1^2\rangle=\otimes_{j=0}^5|\psi_{a_{3j+1}^2 b_{3j+1}^2}\rangle=|+\rangle|1\rangle|-\rangle|+\rangle|-\rangle|+\rangle$, $|\Psi_2^2\rangle=\otimes_{j=0}^5|\psi_{a_{3j+2}^2 b_{3j+2}^2}\rangle=|-\rangle|0\rangle|+\rangle|0\rangle|0\rangle|1\rangle$, and $|\Psi_3^2\rangle=\otimes_{j=0}^5|\psi_{a_{3j+3}^2 b_{3j+3}^2}\rangle=|1\rangle|0\rangle|-\rangle|-\rangle|+\rangle|1\rangle$ to Bob 1, Bob 2, and Bob3, respectively. When each of Bob 1, Bob 2, and Bob 3 has received 6-qubit state and announced the fact, Alice 1 and Alice 2 publicly inform all Bobs their respective strings B_1 and B_2. Then Bob l measures his qubit state $|\psi_{a_{3j+l}^2 b_{3j+l}^2}\rangle$ in the basis Z if $b_{3j+l}^1\oplus b_{3j+l}^2=0$ or in the basis X if $b_{3j+l}^1\oplus b_{3j+l}^2=1$, for $j=0,1,\ldots,5$, $l=1$, 2, 3. From this, Bob 1, Bob 2, and Bob 3 derive Alice 1 and Alice 2's encoding information {0,1,1,0,1,0}, {1,0,0,0,0,1}, and {1,0,1,1,0,1} of their respective 6-qubit states if no Eve's eavesdropping exists. If Alice 1 and Alice 2 choose the 1st, 2nd, 3rd, 13th, 14th, 15th bits as the check bits, then the XOR results $1\oplus 0\oplus 0$, $1\oplus 0\oplus 1$, $0\oplus 0\oplus 1$, $0\oplus 1\oplus 1$ (or 1, 0, 1, 0) of the corresponding bits of Bob 1, Bob 2, and Bob 3's remaining bits {1,1,0,0}, {0,0,0,1}, and {0,1,1,1} are used as raw keys for secret sharing between two Alices and three Bobs.

Note that $B_1,B_2,\ldots,B_m$ reveal nothing about A_i ($i=1,2,\ldots,m$), but it is important that all Alice 1, Alice 2, …, Alice m not publish their respective $B_1,B_2,\ldots,B_m$ until after all Bob 1, Bob 2, …, Bob n announce the reception of the N qubits Alice m sends to them. If all Alices broadcast their respective $B_1,B_2,\ldots,B_m$ before all Bobs announce the reception of the N qubits Alice m sends to them, then either a $(m+n+1)$th party (an "external" eavesdropper) or the dishonest member of two groups intercepts the nN-qubit state $|\Psi^m\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^m b_k^m}\rangle$ can learn the contents of their (all senders) message in this procedure by measuring each qubit in the Z basis (if $\oplus_{i=1}^m b_{nj+l}^i=0$) or in the X basis (if $\oplus_{i=1}^m b_{nj+l}^i=1$).

It is necessary for Alice i ($2\leqslant i\leqslant m$) applying unitary operation H randomly on some qubits. Each sender Alice i encoding string B_i on the sequence of states of qubits is to achieve the aim such that no one or part of Alice 1, …, Alice m can extract some information of others. Case I: Alice 2 does not encode a random string of I and H on the sequence of single photons; Alice 1 can enforce the intercept-resend strategy to extract Alice 2's whole information. Alice 1 can intercept all the single photons and measure them, then resend them. As the sequence of single photons is prepared by Alice 1, Alice 1 knows the measuring basis and the original state of each photon. She uses the same measuring basis when she prepared the photon to measure the photon and read out Alice 2's complete secret messages directly. Case II: Alice i_0 ($3\leqslant i_0\leqslant m$) is the first one who does not encode a random string of I and H on the sequence of single photons; then, one of Alice 1, Alice 2, …, Alice (i_0-1) can also enforce the intercept-resend strategy to extract Alice i_0's whole information by their cooperation. Without loss of generality, suppose that Alice 2 intercepts all the particles that Alice i_0 sends. Alice 2 can obtain Alice i_0's secret message if Alice 1, Alice 3, …, Alice (i_0-1) inform her their respective strings $B_1,B_3,\ldots,B_{i_0-1}$ and $A_1,A_3,\ldots,A_{i_0-1}$.

This secret sharing protocol between m parties and n parties is almost 100% efficient as all the keys can be used in the ideal case of no eavesdropping, while the quantum secret sharing protocols with entanglement states [2] can be at most 50% efficient in principle. In this protocol, quantum memory is required to store the qubits which has been shown available in the present experiment technique [16]. However, if no quantum memory is employed, all Bobs measure their qubits before Alice i's ($1\leqslant i\leqslant m$) announcement of basis, the efficiency of the present protocol falls to 50%.

Two groups can also realize secret sharing by Alice 1 preparing a sequence of nN polarized single photons such that the n-qubit product state of each n photons is in the basis

Z or X as determined by N-bit string B_1, instead that in the above protocol. For instance, (A) Alice i $(1 \leqslant i \leqslant m)$ creates a random nN-bit string A_i and a random N-bit string B_i, and Alice 1 encodes her two strings as a block of nN-qubit states $|\Phi^1\rangle = \otimes_{j=1}^{N} |\phi_{a^1_{n(j-1)+1} b^1_j}\rangle |\phi_{a^1_{n(j-1)+2} b^1_j}\rangle \cdots |\phi_{a^1_{n(j-1)+n} b^1_j}\rangle$, where each qubit state $|\phi_{a^1_{n(j-1)+l} b^1_j}\rangle$ is one of $|\phi_{00}\rangle = |0\rangle$, $|\phi_{10}\rangle = |1\rangle$, $|\phi_{01}\rangle = |+\rangle$, and $|\phi_{11}\rangle = |-\rangle$. Then Alice 1 sends $|\Phi^1\rangle$ to Alice 2. Alice i $(2 \leqslant i \leqslant m)$ applies σ_0 or σ_1 to each qubit state $|\phi_{a^{i-1}_{n(j-1)+l} b^{i-1}_j}\rangle$ $(1 \leqslant l \leqslant n)$ according to the corresponding bit $a^i_{n(j-1)+l}$ of A_2 being 0 or 1; then, she applies I (if $b^i_j = 0$) or H (if $b^i_j = 1$) to each resulting qubit state $|\phi^0_{a^i_{n(j-1)+l} b^i_j}\rangle$. Alice m sends N qubits $\otimes_{j=1}^{N} |\phi_{a^m_{n(j-1)+l} b^m_j}\rangle$ of the resulting nN-qubit state $|\Phi^m\rangle = \otimes_{j=1}^{N} |\phi_{a^m_{n(j-1)+1} b^m_j}\rangle |\phi_{a^m_{n(j-1)+2} b^m_j}\rangle \cdots |\phi_{a^m_{n(j-1)+n} b^m_j}\rangle$ to Bob l, $1 \leqslant l \leqslant n$. After all Bobs receive their respective N qubits, Alice i announces B_i; then, Bob l measures each of his qubit states $|\phi_{a^m_{n(j-1)+l} b^m_j}\rangle$ in the basis Z if $\oplus_{i=1}^{m} b^i_j = 0$ or X if $\oplus_{i=1}^{m} b^i_j = 1$ and deduces its value $\oplus_{i=1}^{m} a^i_{n(j-1)+l}$ if there is no Eve's eavesdropping. A subset of $\{\oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{n(j-1)+l})\}_{j=1}^{N}$ will serve as a check, passing the test; the unchecked bits of $\{\oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{n(j-1)+l})\}_{j=1}^{N}$ will take as the raw keys for secret sharing between two groups. (B) Alice i chooses two random N-bit strings A_i and B_i, and Alice 1 prepares a block of nN-qubit states $|\Psi^1\rangle = \otimes_{j=1}^{N} |\psi_{a^1_{j1} b^1_j}\rangle |\psi_{a^1_{j2} b^1_j}\rangle \cdots |\psi_{a^1_{jn} b^1_j}\rangle$, where a^1_{jl} is 0 or 1 and $\oplus_{l=1}^{n} a^1_{jl} = a^1_j$. Alice i applies a unitary operation σ_0 or σ_1 to each qubit state $|\psi_{a^{i-1}_{jl} b^{i-1}_j}\rangle$ depending on the j th bit a^i_j of A_i being 0 or 1, following it, I or H according to B_i, to each particle. Bob l measures each of his particles $|\psi_{a^m_{jl} b^m_j}\rangle$ in the basis Z (if $\oplus_{i=1}^{m} b^i_j = 0$) or X (if $\oplus_{i=1}^{m} b^i_j = 1$). All Alices select randomly some bits and announce their selection. All Bobs and all Alices compare the values of these check bits. If the test passes, then the rest of the unchecked bits of $\{\oplus_{l=1}^{n} (a^1_{jl} \oplus a^2_j \oplus \cdots \oplus a^m_j)\}_{j=1}^{N}$ are the raw key for secret sharing between two groups. We should emphasize that n must be odd in case (B) since $\oplus_{l=1}^{n} (a^1_{jl} \oplus a^2_j \oplus \cdots \oplus a^m_j) = a^1_j \oplus n a^2_j \oplus \cdots \oplus n a^m_j = a^1_j$ if n is even.

III. SECURITY

Now we discuss the unconditional security of this quantum secret sharing protocol between m parties and n parties. Note that the encoding of secret messages by Alice i $(1 \leqslant i \leqslant m)$ is identical to the process in a one-time-pad encryption where the text is encrypted with a random key as the state of the photon in the protocol is completely random. The great feature of a one-time-pad encryption is that as long as the key strings are truly secret, it is completely safe and no secret messages can be leaked even if the cipher text is intercepted by the eavesdropper. Here the secret sharing protocol is even more secure than the classical one-time-pad in the sense that an eavesdropper Eve cannot intercept the whole cipher text as the photons' measuring basis is chosen randomly. Thus the security of this secret sharing protocol depends entirely on the second part when Alice m sends the lth sequence of N photons to Bob l $(1 \leqslant l \leqslant n)$.

The process for ensuring a secure block of nN qubits (n secure sequences of N photons) is similar to that in the BB84 QKD protocol [17]. The process of this secret sharing between m parties and n parties after all Alices encoding their respective messages using unitary operations is in fact identical to n independent BB84 QKD processes, which has been proven unconditionally secure [18,19]. Thus the security for the present quantum secret sharing between multiparty and multiparty is guaranteed.

In practice, some qubits may be lost in transmitting. In this case, all Alices and Bobs can take two kind strategies: one is removing these qubits, the other using a qubit chosen at random in one of four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ as a substitute for a lost qubit. If a member does not receive a qubit and wants to delete it, she or he must announce and let all members in the two groups know the fact. All Alices and all Bobs sacrifice some randomly selected qubits to test the "error rate." If the error rate is too high, they abort the protocol. Otherwise, by utilizing a Calderbank-Shor-Steane (CSS) code [18,20,21], they perform information reconciliation and privacy amplification on the remaining bits to obtain secure final key bits for secret sharing. They proceed to this step, obtaining the final key while all Alices communicate with all Bobs. In a CSS mode, classical linear codes C_1 and $C_2^{\perp}$ are used for bit and phase error correction, respectively, where $C_2 \subset C_1$. The best codes that we know exist satisfy the quantum Gilbert-Varshamov bound. The number of cosets of C_2 in C_1 is $|C_1|/|C_2| = 2^M$, so there is a one-to-one correspondence $u_K \to K$ of the set of representatives u_K of the 2^M cosets of C_2 in C_1 and the set of M-bit strings K. As in the BB84 protocol, C_1 is used to correct bit errors in the key and C_2 to amplify privacy. For the sake of convenience, we suppose that after the verification test all Alices are left with the N'-bit string $v = \{\oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{n+l}), \oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{2n+l}), \ldots, \oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{nN'+l})\} = \{\oplus_{l=1}^{n} (\oplus_{i=1}^{m} a^i_{ns+l})\}_{s=1}^{N'}$, but all Bobs with $v + \epsilon$ by the effect of losses and noise. Let us assume that *a priori* it is known that along the communication channel used by all Alices and all Bobs, the expected number of errors per block caused by losses and all noise sources including eavesdropping is less than $t = \delta N'$, where δ is the bit error rate. How can an upper bound be placed on t? In practice, this can be established by random testing of the channel, leaving us with a protocol which is secure [22], even against collective attacks. If δ is low enough, we can be confident that error correction will succeed, so that all Alices and all Bobs share a secure common key. The secure final key for secret sharing can be extracted from the raw key bits (consisting of the remaining noncheck bits) at the asymptotic rate $R = \mathrm{Max}\{1 - 2H(\delta), 0\}$ [22], where δ is the bit error rate found in the verification test (assuming $\delta < 1/2$). Using a predetermined t error correcting CSS code [18], the two groups share a secret key string and realize secure communication. Suppose that government department 1 wishes to send messages to government department 2. Then, all Alices gather together, choose a random code word u in C_1 (u may be $u_1 + u_2 + \cdots + u_m$, where u_i is a code word in C_1 selected randomly by Alice i), and encode their M-bit message P by adding the message and the M-bit string K together, where $u + C_2 = u_K + C_2$. Then they send it to government department 2. Bobs receive the secret message and publicly announce this fact. All Alices announce $u+v$. All Bobs subtract this from their result $v+\epsilon$ and correct the result $u+\epsilon$ with code C_1 to obtain the code word u. All Alices and all Bobs use the M-bit string K as the final key for secret sharing. That is, all Alices and all Bobs perform information reconciliation by the use of the classical code C_1 and perform privacy amplification by computing the coset of $u+C_2$. All Bobs can decode and read out the message P by subtracting K. No one in department 1 tells the final key K to someone in or others part of department 2, since the aim of all Alices is to let all Bobs know their message.

In summary, we propose a scheme for quantum secret sharing between multiparty and multiparty, where no entanglement is employed. In the protocol, Alice 1 prepares a sequence of single photons in one of four different states according to her two random bit strings; the other Alice i $(2 \leq i \leq m)$ directly encodes her two random classical information strings on the resulting sequence of Alice $(i-1)$ via unitary operations. After that, Alice m sends $1/n$ of the sequence of single photons to each Bob l $(1 \leq l \leq n)$. Each Bob l measures his photons according to all Alices' measuring-basis sequences. All Bobs must cooperate in order to infer the secret key shared by all Alices. Any subset of all Alices or all Bobs cannot extract secret information, but the entire set of all Alices and the entire set of all Bobs can. As entanglement, especially the inaccessible multiparty entangled state, is not necessary in the present quantum secret sharing protocol between m and n parties, it may be more applicable when the numbers m and n of the parties of secret sharing are large. Its theoretic efficiency is also doubled to approach 100%. This protocol is feasible with present-day techniques.

ACKNOWLEDGMENTS

This work was supported by the Hebei Natural Science Foundation of China under Grant Nos. A2004000141 and A2005000140 and the Key Natural Science Foundation of Hebei Normal University.

[1] B. Schneier, *Applied Cryptography* (Wiley, New York, 1996). See also J. Gruska, *Foundations of Computing* (Thomson Computer Press, London, 1997).
[2] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[3] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
[4] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).
[5] A. C. A. Nascimento, J. Mueller-Quade, and H. Imai, Phys. Rev. A **64**, 042311 (2001).
[6] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[7] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[8] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002).
[9] S. Bagherinezhad and V. Karimipour, e-print quant-ph/0204124.
[10] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A **69**, 052307 (2004).
[11] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
[12] D. Bouwmeester, J. W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
[13] J. W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **86**, 4435 (2001).
[14] G. P. Guo and G. C. Guo, Phys. Lett. A **310**, 247 (2003).
[15] K. Brádler and M. Dušek, J. Opt. B: Quantum Semiclassical Opt. **6**, 63 (2004).
[16] G. P. Guo and G. C. Guo, Quantum Inf. Comput. **3**, 627 (2003).
[17] C. H. Bennett and G. Brassard, in a *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, (IEEE, New York, 1984), pp. 175–179.
[18] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[19] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[20] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[21] A. M. Steane, Proc. R. Soc. London, Ser. A **452**, 2551 (1996).
[22] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).