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 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 \([2, 3, 4, 5]\) can accomplish distributing information securely where multi-photon entanglement is employed. Recently, many kinds quantum secret sharing with entanglement have been proposed \([6, 7, 8, 9, 10]\). Lance et al. have reported an experimental demonstration of a \((2,3)\) threshold quantum secret sharing scheme \([11]\). The combination of quantum key distribution (QKD) and classical sharing protocol can realize secret sharing safely. Quantum secret sharing protocol provides for secret secure 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 multi-party secret sharing tasks \([2, 3]\), since the efficiency of preparing even tripartite or four-party 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 quantum key distribution and accomplish one splitting a message into many parts to achieve multi-party 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 multi-party \((m \text{ parties of group 1})\) and multi-party \((n \text{ parties of group 2})\). That is, instead of giving his information to any one individual of group 1, each sender to split his information in such a way that no part 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 MULTI-PARTY AND MULTI-PARTY

Suppose there are $m$ ($m \geq 2$) and $n$ ($n \geq 2$) members in government department 1 and department 2, respectively, and Alice 1, Alice 2, ⋅⋅⋅, Alice n, 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,

$$|\Psi^1\rangle = \bigotimes_{k=1}^{nN} |\psi_{a_k}\rangle |b_k\rangle$$

$$= \bigotimes_{j=0}^{N-1} |\psi_{a_{j+1}b_1}^{1}\rangle |\psi_{a_{j+2}b_2}^{1}\rangle \cdots |\psi_{a_{nj+b_n}}^{1}\rangle (\text{1})$$

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

$$|\psi_{00}\rangle = |0\rangle,$$  

$$|\psi_{10}\rangle = |1\rangle,$$  

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

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

The effect of this procedure is to encode $A_1$ in the basis $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+, |-\rangle\}$, 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 $\sigma_0 = I$ (if the $k$th bit $a_k^2$ of $A_2$ is 0), or $\sigma_1 = i\sigma_y = |0\rangle(|0\rangle - |1\rangle)/\sqrt{2} (\text{if} a_k^2 = 1)$ on each $|\psi_{a_k^1}\rangle$ of the $nN$ qubits she receives from Alice 1 such that $|\psi_{a_k^1}\rangle$ is changed into $|\psi_{a_k^2}\rangle$, and obtains $nN$-qubit product state $|\Psi^2\rangle = \bigotimes_{k=1}^{nN} |\psi_{a_k^2}\rangle |b_k\rangle$n. After that, she performs a unitary operator $I$ (if $b_k^2 = 0$) or $H = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (if $b_k^2 = 1$) on each qubit state $|\psi_{a_k^2}\rangle$ according to her another random classical bits string $B_2$, and makes $|\psi_{a_k^2}\rangle$ to be turned into $|\psi_{a_k^{2'}}\rangle$. Alice 2 sends Alice 3 $|\Psi^2\rangle = \bigotimes_{k=1}^{k=N} |\psi_{a_k^{2'}}\rangle$.

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 n.

Similarly, Alice m first creates two strings $A_m$ and $B_m$ of $nN$ random classical bits. Then she makes a unitary operation $\sigma_0$ (if $a_k^m = 0$) or $\sigma_1$ (if $a_k^m = 1$) on each qubit state $|\psi_{a_k^m-1}\rangle$ in the corresponding bits $a_k^{m-l}$ of these checked bits of all Alices and the values of Bob’s checked bits $|\psi_{a_k^{m-l}}\rangle$. Then they abort and re-try the protocol from the start. The XOR results $\oplus_{i=1}^{m} |\psi_{a_k^{m-l}}\rangle$ of Bob’s corresponding bits $\oplus_{i=1}^{m} |\psi_{a_k^{m-l}}\rangle$ of the rest unchecked
bits $n_j + l$ of $\{\oplus^m_{i=1}a_{i,j+l}^j\}^{N-1}_{j=0}$, $\{\oplus^m_{i=1}a_{i,j+2l}^j\}^{N-1}_{j=0}$, \ldots, $\{\oplus^m_{i=1}a_{i,j+n+l}^j\}^{N-1}_{j=0}$ (or $\ominus^N_{j=0}|\psi_{a_{m+j}^m+b_{m+j}^m}\rangle$, $\ominus^{N-1}_{j=0}|\psi_{a_{m+j+2}^m+b_{m+j+2}^m}\rangle$, \ldots, $\ominus^N_{j=0}|\psi_{a_{m+j+n}^m+b_{m+j+n}^m}\rangle$) can be used as raw keys for secret sharing between all Alice and all Bobs, where $j = j_{r0+1}, j_{r0+2}, \ldots, j_{N}$.

This protocol is summarized as follows:

M1. Alice1 chooses two random $n$-bit strings $A_1$ and $B_1$. She encodes each data bit of $A_1$ as $\{0,1\}$ if the corresponding bit of $B_1$ is 0 or $\{0\} = 0$ if $B_1$ is 1. Explicitly, she encodes each data bit 0 (1) as $A_1$ as $\{1\}$ if the corresponding bit of $B_1$ is 0 or $\{+\}$ (+) if the corresponding bit of $B_1$ is 1. Then she sends the resulting $n$-qubit state $|\Psi^1\rangle = \otimes_{j=0}^n |\psi_{a_{j}^j}\rangle$ to Alice2.

M2. Alice2 creates two random $n$-bit strings $A_2$ and $B_2$. She applies $\sigma_0$ or $\sigma_1$ to each qbit $|\psi_{a_{j}^j}\rangle$ of $n$-qubit state $|\Psi^1\rangle$ corresponding to the corresponding bit of $A_2$ being 0 or 1, then she sends $I$ or $H$ to each qubit of the resulting $n$-qubit state depending on the corresponding bit of $B_2$ being 0 or 1. After this, she sends Alice3 the resulting $n$-qubit state $|\Psi^2\rangle$.

M3. Alicei does likewise, $i = 3, 4, \ldots, m - 1$. Depending on the corresponding bit $a_{j}^i$ of a random $n$-bit string $A_m$, which she generates on her own, Alicem performs $\sigma_0$ (if $a_{j}^m = 0$) or $\sigma_1$ (if $a_{j}^m = 1$) 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 $b_{j}^m$ of $B_m$ is 0) or $H$ (if $b_{j}^m = 1$) on each qubit of the resulting $n$-qubit state $|\Psi^m\rangle = \otimes_{j=0}^n |\psi_{a_{j}^j+b_{j}^j}\rangle$. After it, she sends $N$-qubit state $\otimes_{j=0}^{N-1} |\psi_{a_{m+j}^m+b_{m+j}^m}\rangle$ to Bob1, $1 \leq l \leq n$.

M4. Bob1, Bob2, \ldots, Bobn receive $N$ qubits, and announce this fact, respectively.

M5. Alice1, Alice2, \ldots, and Alicem publicly announce the strings $B_1, B_2, \ldots, B_m$, respectively.

M6. Bob1, Bob2, \ldots, and Bobn 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, Bobl measures $|\psi_{a_{m+j}^m+b_{m+j}^m}\rangle$ in the basis $Z$ (if $\oplus^m_{i=1}b_{i,j+l}^i = 0$) or in the basis $X$ (if $\oplus^m_{i=1}b_{i,j+l}^i = 1$), $j = 0, 1, \ldots, N - 1, l = 1, 2, \ldots, n$.

M7. All Allcise 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 Alice and Bob are required to broadcast the values of their checked bits, and compare the XOR results of the corresponding bits of checked bits of Alice1, Alice2, \ldots, Alicem and the values of the corresponding bits of Bob1, Bob2, \ldots, and Bobn. If more than an acceptable number disagree, they abort this round of operation and restart from step first.

M8. The XOR results $\oplus^m_{i=1}b_{i,j+l}^i$ of Bobl’s corresponding bits $\oplus^m_{i=1}a_{i,j+l}^i$ of the remaining bits $n_j + l$ of $\{\oplus^m_{i=1}a_{i,j+l}^j\}^{N-1}_{j=0}$, $\{\oplus^m_{i=1}a_{i,j+2l}^j\}^{N-1}_{j=0}$, \ldots, $\{\oplus^m_{i=1}a_{i,j+n+l}^j\}^{N-1}_{j=0}$ (or $\ominus^N_{j=0}|\psi_{a_{m+j}^m+b_{m+j}^m}\rangle$, $\ominus^{N-1}_{j=0}|\psi_{a_{m+j+2}^m+b_{m+j+2}^m}\rangle$, \ldots, $\ominus^N_{j=0}|\psi_{a_{m+j+n}^m+b_{m+j+n}^m}\rangle$) can be used as secret keys for secret sharing between all Alice and all Bobs, where $j = j_{r0+1}, j_{r0+2}, \ldots, j_{N}$.
Alice1 encoding string $B_i$ on the sequence of states of qubits is to achieve the aim such that no one or part of Alice1, $\cdots$, Alice$m$ can extract some information of others. Case I: Alice2 does not encode a random string of $I$ and $H$ on the sequence of single photons, Alice1 can enforce the intercept-resend strategy to extract Alice2’s whole information. Alice1 can intercept all the single photons and measure them, then resend them. As the sequence of single photons is prepared by Alice1, Alice1 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 Alice2’s complete secret messages directly. Case II: Alice1$_0$ (3 ≤ $i_0$ ≤ $m$) is the first one who does not encode a random string of $I$ and $H$ on the sequence of single photons, then one of Alice1, Alice2, $\cdots$, Alice($i_0$ $-$ 1) can also enforce the intercept-resend strategy to extract Alice1$_0$’s whole information by their cooperation. Without loss of generality, suppose that Alice2 intercepts all the particles that Alice1$_0$ sends. Alice2 can obtain Alice1$_0$’s secret message if Alice1, Alice3, $\cdots$, Alice($i_0$ $-$ 1) inform her their respective strings $B_1$, $B_3$, $\cdots$, $B_{i_0}$-1 and $A_1$, $A_3$, $\cdots$, $A_{i_0}$-$1$.

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 [14]. However, if no quantum memory is employed, all Bobs measure their qubits before Alice1’s ($1 \leq i \leq m$) announcement of basis, the efficiency of the present protocol falls to 50%.

Two groups can also realize secret sharing by Alice1 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) Alice1 ($1 \leq i \leq m$) creates a random $n$-bit string $A_i$ and a random $N$-bit string $B_i$, and Alice1 encodes her two strings as a block of $nN$ qubits state $|\Phi^1\rangle = \otimes_{j=1}^{N} |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle \cdots |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$, where each qubit state $|\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$ is one of $|\phi_0\rangle = |0\rangle$, $|\phi_1\rangle = |1\rangle$, $|\phi_{01}\rangle = |+\rangle$ and $|\phi_{11}\rangle = |–\rangle$. Then Alice1 sends $|\Phi^1\rangle$ to Alice2. Alice2 ($2 \leq i \leq m$) applies $\sigma_0$ or $\sigma_1$ to each qubit state $|\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$ ($1 \leq l \leq n$) according to the corresponding bit $a_i^{n(j-1)+l}$ of $A_2$ being 0 or 1, then she applies I (if $b_j = 0$) or $H$ (if $b_j = 1$) to each resulting qubit state $|\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$. Alice1 sends $N$ qubits $\otimes_{j=1}^{N} |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$ of the resulting $nN$ qubits state $|\Phi^m\rangle = \otimes_{j=1}^{N} |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle \cdots |\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$ to Bob1, $1 \leq i \leq n$. After all Bobs receive their respective $N$ qubits, Alice1 announces $B_i$, then Bob1 measures each of his qubit states $|\phi_{a_i^{n(j-1)+b_j}}^{a_i^{n(j-1)+b_j}}\rangle$ in the basis $Z$ if $\oplus_{l=1}^{m} b_j = 0$ or $X$ if $\oplus_{l=1}^{m} b_j = 1$, and deduces its value $\oplus_{l=1}^{m} a_i^{n(j-1)+l}$ if there is no Eve’s eavesdropping. A subset of $\{\oplus_{l=1}^{m} a_i^{n(j-1)+l}\}_{j=1}^{N}$ will serve as a check, passing the test, the unchecked bits of $\{\oplus_{l=1}^{m} a_i^{n(j-1)+l}\}_{j=1}^{N}$ will take as the raw keys for secret sharing between two groups. (B) Alice1 chooses two random $N$-bit strings $A_i$ and $B_i$, and Alice1 prepares a block of $nN$ qubits state $|\Psi^1\rangle = \otimes_{j=1}^{N} |\psi_{a_{j1}^{n(j-1)+b_j}}^{a_{j1}^{n(j-1)+b_j}}\rangle |\psi_{a_{j1}^{n(j-1)+b_j}}^{a_{j1}^{n(j-1)+b_j}}\rangle \cdots |\psi_{a_{j1}^{n(j-1)+b_j}}^{a_{j1}^{n(j-1)+b_j}}\rangle$, where $a_{j1}^{n(j-1)+l}$ is 0 or 1 and $\oplus_{l=1}^{m} a_{j1}^{n(j-1)+l} = a_j$. Alice1 applies unitary operation $\sigma_0$ or $\sigma_1$ to each qubit state $|\psi_{a_{j1}^{n(j-1)+l}}\rangle$ depending on the $j$-th bit $a_j$ of $A_j$ being 0 or 1, following it, $I$ or $H$ according to $B_j$, to each particle. Bob1 measures each of his particles $|\psi_{a_{j1}^{n(j-1)+l}}\rangle$ in the basis $Z$ (if $\oplus_{l=1}^{m} b_{j1} = 0$) or $X$ (if $\oplus_{l=1}^{m} b_{j1} = 1$). 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 $\{\oplus_{l=1}^{m} a_{j1}^{n(j-1)+l} + a_{j2}^{n(j-1)+l} + \cdots + a_{jm}^{n(j-1)+l}\}_{j=1}^{N}$ are the raw key for secret sharing between two groups. We should emphasize that $n$ must be odd in case (B) since $\oplus_{l=1}^{m} a_{j1}^{n(j-1)+l} + a_{j2}^{n(j-1)+l} + \cdots + a_{jm}^{n(j-1)+l} = a_j + na_j^2 + \cdots + na_j^n = a_j$ 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 Alice1 ($1 \leq i \leq m$) 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 Alice1 sends the $l$-th sequence of $N$ photons to Bob1 ($1 \leq l \leq n$).

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 Alice1 encoding their respective messages using unitary operations is in fact identical to $n$ independent BB84 QKD processes, which has been proven unconditional secure [18, 19]. Thus the security for the present quantum secret sharing between multi-party and multi-party is guaranteed.

In practice, some qubits may be lost in transmitting. In this case, all Alice1s and Bob1s can take two kind
strategies, one is removing these qubits, the other is using a qubit chosen at random in one of four states \{\{0\},\{1\},\{+\},\{-\}\} as a substitute for a lost qubit. If a member does not receive a qubit and wants to delete it, she/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, using a Calderbank-Shor-Steane (CSS) code \[15, 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 \(C_2\) 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 \(u_K \rightarrow K\) 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 verification test all Alices are left with the \(N\)’ bit string \(v = \{\oplus_{i=1}^n(a_{1i}^{m}),\oplus_{i=1}^n(a_{1i}^{m}a_{2i}^{m}),\ldots,\oplus_{i=1}^n(a_{1i}^{m}a_{2i}^{m}a_{3i}^{m}a_{4i}^{m})\}\) \(=\{\oplus_{i=1}^n(a_{i}^{m})\oplus_{i=1}^n(a_{i+1}^{m})\}_{i=1}^{n}\), but all Bobs with \(v + \epsilon\) by the effect of losses and noise. Let us assume that \(a\) \(a\) 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 \(t = aN\), where \(\delta\) 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 \(\delta\) 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 = \text{Max}\{1 - 2H(\delta), 0\} \[22\], where \(\delta\) is the bit error rate found in the verification test (assuming \(\delta < 1/2\)). Using a pre-determined \(t\) error-correcting CSS code \[15\], the two groups share a secret key string and realize secret communication. Suppose that government department1 wishes to send messages to government department2, 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 department2. 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 performs 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 department1 tells final key \(K\) to someone or part of department2, since the aim of all Alice is to let all Bobs know their message.

In summary, we propose a scheme for quantum secret sharing between multi-party and multi-party, where no entanglement is employed. In the protocol, Alice1 prepares a sequence of single photons in one of four different states according to her two random bits strings, 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\(i\) 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 Alice\(i\)’s 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 can not extract secret information, but the entire set of all Alices and the entire set of all Bobs can. As entanglement, especially the inaccessible multi-party entangled state, is not necessary in the present quantum secret sharing protocol between \(m\)-party and \(n\)-party, 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. M. 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, arXiv: 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 Semiclass. Opt. 6, 63 (2004).
[16] G. P. Guo and G. C. Guo, Quant. Infor. Comp. 3, 627 (2003).
[17] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. 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. Roy. Soc. Lond. A 452, 2551 (1996).
[22] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Infor. Comp. 4, 325 (2004).