Comment on "Quantum secret sharing between multiparty and multiparty without entanglement"

Chuan-Ming Li,[1] Chi-Chao Chang,[2] and Tzonelih Hwang[1]
[1]*Department of Computer Science and Information Engineering, National Cheng Kung University , No. 1, Ta-Hsueh Road, Tainan City, 701, Taiwan, Republic of China*
[2]*Department of Information Management,Chang Jung Christian University, 396 Chang Jung Road, SEC 1, Kway Jen, Tainan, 711, Taiwan, Republic of China*
(Received 21 October 2005; published 6 January 2006)

Recently, Yan and Gao [Phys. Rev. A **72**, 012304 (2005)] presented a quantum secret sharing protocol which allows a secret message to be shared between two groups of parties (*m* parties in group 1 and *n* parties in group 2). Their protocol is claimed to be secure that, except with the cooperation of the entire group 1 or group 2, no subgroup of either group 1 or group 2 can extract the secret message. However, this study points out that the *m*th party (the last party to process the quantum state) of group 1 can maliciously replace the secret message with an arbitrary message without the detection of the other parties.

DOI: 10.1103/PhysRevA.73.016301 PACS number(s): 03.67.Dd

I. INTRODUCTION

In [1], Yan and Gao proposed a quantum secret sharing (QSS) protocol which allows a secret message to be shared between two groups of parties (*m* parties in group 1 and *n* parties in group 2). In their protocol, all *m* parties in group 1 collectively generate the secret message by directly encoding their respective secret strings on a sequence of single photons. The *m*th party (the last party to process the single photons) of group 1 then sends $1/n$ of the resulting qubits to each of *n* parties of group 2. Thus the secret message shared by all parties of group 1 is shared by all parties of group 2 in such a way that no subset of each group can correctly determine the secret message except with the cooperation of either the entire set of group 1 or the entire set of group 2.

Yan and Gao [1] have shown that their protocol is unconditionally secure based on the quantum no-cloning theory. However, this study points out that if the *m*th party of group 1 is not honest, he can generate either another sequence of single photons or a sequence of EPR pairs to replace the original photons without the detection of the other parties. In other words, the *m*th party of group 1 can maliciously replace the original secret message with an arbitrary message and pass the check procedure performed by all parties in group 1 and in group 2.

The rest of this study is organized as follows. The next section briefly reviews the QSS protocol proposed by Yan and Gao [1]. Section III shows the weakness of their protocol and gives a suggestion to avoid the flaw. Finally, a short conclusion is given in Sec. IV.

II. REVIEW OF YAN AND GAO'S QSS PROTOCOL

Let Alice 1, Alice 2,…, Alice *m* be *m* parties of group 1 and Bob 1, Bob 2,…, Bob *n* be *n* parties of group 2. Yan and Gao's QSS protocol [1] is briefly described as follows.

(a) (Step 1) Alice 1 chooses two random *nN* bit strings A_1 and B_1. She then encodes each bit a_k^1 of A_1 as $|\psi_{a_k^1 b_k^1}\rangle$ for $k=1,2,\ldots,nN$, where a_k^1 is the *k*th bit of A_1, b_k^1 is the corresponding bit of B_1, and each qubit is one of the four states

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

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

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

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

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; thus, no measurement can distinguish between all of them with certainty. Then Alice 1 sends the resulting *nN* qubit state

$$|\Psi^1\rangle = \otimes_{k=1}^{nN}|\psi_{a_k^1 b_k^1}\rangle = \otimes_{j=0}^{N-1}|\psi_{a_{nj+1}^1 b_{nj+1}^1}\rangle|\psi_{a_{nj+2}^1 b_{nj+2}^1}\rangle\cdots|\psi_{a_{nj+n}^1 b_{nj+n}^1}\rangle$$

to Alice 2.

(b) (Step 2) Alice 2 creates two random *nN* bit strings A_2 and B_2. She applies a unitary transformation σ_0 (if the *k*th bit a_k^2 of A_2 is 0) or σ_1 (if $a_k^2=1$) to each qubit $|\psi_{a_k^1 b_k^1}\rangle$ of *nN* qubit state $|\Psi^1\rangle$, where

$$\sigma_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|,$$

$$\sigma_1 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

Then, she performs a unitary transformation *I* (if $b_k^2=0$) or *H* (if $b_k^2=1$) to each qubit of the resulting *nN* qubit state, where

$$H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|.$$

After this, she sends Alice 3 the resulting *nN* qubit state $|\Psi^2\rangle$.

(c) (Step 3) Alice *i* does likewise, for $i=3,4,\ldots,m$. After Alice *m* finishes the unitary transformations on each qubit of $|\Psi^{m-1}\rangle$ according to the strings A_m and B_m, she sends *N* qubit state $|\Psi_l^m\rangle = \otimes_{j=0}^{N-1}|\psi_{a_{nj+l}^m b_{nj+l}^m}\rangle$ of the resulting *nN* qubit state

$|\Psi^m\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^m b_k^m}\rangle$ to Bob l, for $l=1,2,\ldots,n$.

(d) (Step 4) Bob 1, Bob 2,..., Bob n receive N qubits and announce this fact, respectively.

(e) (Step 5) Alice 1, Alice 2,..., Alice m publicly announce the strings $B_1,B_2,\ldots,B_m$ one after another, respectively.

(f) (Step 6) 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 $|\psi_{a^m_{nj+l}b^m_{nj+l}}\rangle$ in the basis Z (if $\oplus_{i=1}^m b^i_{nj+l}=0$) or in the basis X (if $\oplus_{i=1}^m b^i_{nj+l}=1$), for $j=0,1,\ldots,N-1$, and $l=1,2,\ldots,n$.

(g) (Step 7) All Alices select some bits nj_r+l of their nN bits at random and publicly announce the selection, where $j_r\in\{j_1,j_2,\ldots,j_{r_0}\}\subset\{0,1,\ldots,N-1\}$ and $l=1,2,\ldots,n$. 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 the first step.

(h) (Step 8) 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 remaining bits nj_s+l of $\{\oplus_{i=1}^m a^i_{nj+1}\}_{j=0}^{N-1}$, $\{\oplus_{i=1}^m a^i_{nj+2}\}_{j=0}^{N-1}$, ..., $\{\oplus_{i=1}^m a^i_{nj+n}\}_{j=0}^{N-1}$ can be used as raw keys for secret sharing between all Alices and all Bobs, where $j_s\notin\{j_1,j_2,\ldots,j_{r_0}\}$ and $j_s\in\{0,1,\ldots,N-1\}$.

III. THE SECURITY FLAW IN YAN AND GAO'S PROTOCOL

Yan and Gao's protocol is claimed to be secure that, except with the cooperation of all Alices or all Bobs, no subgroup of either group 1 or group 2 can extract the secret message. However, this study shows that if Alice m is not honest, she can maliciously replace the original secret message with an arbitrary message she chooses without the detection of other parties. Two ways are proposed to replace the original secret message with some other forged one: the first one is using single photons and the other is using EPR pairs. These attacks are given as follows.

A. The attack with single photons

(a) Let Alice i, for $i=1,2,\ldots,m-1$, perform the same process as that in Yan and Gao's protocol.

(b) When the malicious Alice m receives the nN qubit state $|\Psi^{m-1}\rangle$ from Alice $m-1$, she preserves it. Then she chooses two random nN bit strings A'_m and B'_m. Instead of applying unitary transformations on $|\Psi^{m-1}\rangle$, she creates a new nN qubit state $|\Psi^m\rangle=\otimes_{k=1}^{nN}|\psi_{a_k^m b_k^m}\rangle$ according to each bit a_k^m of A'_m and b_k^m of B'_m, for $k=1,2,\ldots,nN$. Alice m sends N qubit state $|\Psi_l^m\rangle=\otimes_{j=0}^{N-1}|\psi_{a^m_{nj+l}b^m_{nj+l}}\rangle$ of the resulting nN qubit state $|\Psi^m\rangle$ to Bob l, for $l=1,2,\ldots,n$.

(c) When all Bob 1, Bob 2,..., Bob n have announced the receiving of their string of N qubits and Alice 1, Alice 2,..., Alice $m-1$ have announced the strings $B_1,B_2,\ldots,B_{m-1}$, Alice m calculates

$$B_m=B'_m\oplus B_1\oplus B_2\oplus\cdots\oplus B_{m-1}.$$

Alice m publicly announces the string B_m. Note that the measuring basis used by Bob l to measure the qubit $|\psi_{a^m_{nj+l}b^m_{nj+l}}\rangle$ is determined by the bit b^m_{nj+l} of B'_m, in which the basis Z (the basis X) is used if $b^m_{nj+l}=0$ (if $b^m_{nj+l}=1$), for $j=0,1,\ldots,N-1$ and $l=1,2,\ldots,n$. Accordingly, the measuring result of the qubit $|\psi_{a^m_{nj+l}b^m_{nj+l}}\rangle$ should be decoded as the same bit value as the bit a^m_{nj+l} of A'_m.

(d) Since Alice m has preserved the nN qubit state $|\Psi^{m-1}\rangle$, she can learn the contents of the message $A'=\oplus_{i=1}^{m-1}A_i$ by measuring each qubit $|\psi_{a_k^{m-1}b_k^{m-1}}\rangle$ of $|\Psi^{m-1}\rangle$ in the Z basis (if $\oplus_{i=1}^{m-1}b_k^i=0$) or in the X basis (if $\oplus_{i=1}^{m-1}b_k^i=1$), for $k=1,2,\ldots,nN$. Alice m then calculates

$$A_m=A'_m\oplus A',$$

and uses A_m to cooperate with other Alices during the check procedure (steps 7 and 8).

According to the above description, Alice m can replace the nN qubit state $|\Psi^{m-1}\rangle$ with the new state $|\Psi^m\rangle$, and she can also calculate the strings A_m and B_m to successfully cheat on other parties during the check procedure. Consequently, the secret message shared between all Alices and all Bobs is indeed chosen by Alice m rather than the collaboration of all Alices.

B. The attack with EPR pairs

In the above attack, Alice m cannot announce the string B_m until she obtains all the strings B_1, $B_2,\ldots,B_{m-1}$ from Alice 1, Alice 2,..., Alice $m-1$ respectively. However, this can be a risk for the cheating of Alice m if Alice m is asked to announce her string B_m before other Alices do. We now propose another attack to Yan and Gao's protocol in which Alice m can announce her string B_m without first knowing other string B_i, for $i=1,2,\ldots,m-1$.

(a) Let Alice i, for $i=1,2,\ldots,m-1$, perform the same process as that in Yan and Gao's protocol.

(b) When the malicious Alice m receives the nN qubit state $|\Psi^{m-1}\rangle$ from Alice $m-1$, she preserves it. Rather than prepare the nN qubit state, Alice m generates nN EPR pairs in the state $\otimes_{k=1}^{nN}|\Phi_k\rangle$, where $|\Phi_k\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)$. Alice m keeps the first qubit of each EPR pair and takes the second qubit of each EPR pair as the nN qubit state $|\Psi^m\rangle$. She then sends N qubit state $|\Psi_l^m\rangle$ of $|\Psi^m\rangle$ to Bob l, for $l=1,2,\ldots,n$, as the same procedure as that described above.

(c) Alice m chooses a random nN bit string B_m. When all Bob 1, Bob 2,..., Bob n have announced the receiving of their string of N qubits, Alice 1, Alice 2,..., Alice m publicly announce the strings $B_1,B_2,\ldots,B_m$, respectively. Note that Alice m can select the string B_m without first knowing other string B_i, for $i=1,2,\ldots,m-1$.

(d) Alice m calculates $B'_m=B_1\oplus B_2\oplus\cdots\oplus B_m$. She then measures the first qubit of each EPR pair according to the corresponding bit of B'_m and decodes the measuring results to obtain the string A'_m. Note that Bob 1, Bob 2,..., Bob n measure each qubit of their respective states in the basis Z or X according to the XOR results of corresponding bits of strings $B_1,B_2,\ldots,B_m$. Thus, the measuring results of Bobs

and Alice m should be identical owing to the property of the EPR pair.

(e) Similar to the previous attack, Alice m can learn the contents of the message $A' = \oplus_{i=1}^{m-1} A_i$ by measuring each qubit $|\psi_{a_k^{m-1} b_k^{m-1}}\rangle$ of $|\Psi^{m-1}\rangle$, for $k = 1, 2, \ldots, nN$. She then calculates

$$A_m = A'_m \oplus A',$$

and uses A_m to cooperate with other Alices during the check procedure.

According to the above description, Alice m can replace the nN qubit state $|\Psi^{m-1}\rangle$ with nN EPR pairs. Due to the property of the EPR pairs, Alice m can announce her string B_m without first knowing other string B_i, for $i = 1, 2, \ldots, m-1$. As a result, the attacker in this attack does not necessarily have to be the last party of group 1 if she can collect the string A_i from the other Alices during the check procedure.

C. An improvement of Yan and Gao's protocol

In the above attacks, Alice m can successfully cheat on other parties because she can calculate the proper strings A_m and B_m by gathering the string $B_1, B_2, \ldots, B_{m-1}$ and measuring the nN qubit state $|\Psi^{m-1}\rangle$ according to the result of $\oplus_{i=1}^{m-1} B_i$. Hence, to avoid the security flaw, we suggest that all Alices must cooperatively extract the secret message $A' = \oplus_{i=1}^{m} A_i$ before they publicly announce the strings $B_1, B_2, \ldots, B_m$, respectively. Moreover, the announcement of the string B_i, for $i = 1, 2, \ldots, m$, must be in a random sequential order so that Alice m cannot calculate the proper strings A_m and B_m during the check procedure. Note that all Alices also have to keep the string A' secret from all Bobs before they publicly announce the strings $B_1, B_2, \ldots, B_m$.

IV. CONCLUSION

This study has pointed out a security flaw in Yan and Gao's QSS protocol, in which the secret message shared by all Alices and all Bobs can be maliciously replaced by Alice m without detection of the other parties. We have proposed two ways to perform the attack: one is to use the single photons and the other makes use of the EPR pairs. Nevertheless, a possible way to avoid the security flaw is also given in this study.

ACKNOWLEDGMENT

The authors wish to thank Kuo-Chang Lee for his helpful discussion on the solution to avoid the weakness of Yan and Gao's QSS protocol.

[1] F. L. Yan and T. Gao, Phys. Rev. A **72**, 012304 (2005).