International Symposium on Information Theory and its Applications, ISITA2008
Auckland, New Zealand, 7-10, December, 2008

Quantum Secret Sharing between Multiparty and Multiparty against the Attacks with Single Photons or EPR-pair

Atsushi WASEDA[†], Takayuki TAKAGI[‡], Masakazu SOSHI[††] and Atsuko MIYAJI[‡]

[†] National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
E-mail:a-waseda@nict.go.jp

[‡] Japan Advanced Institute of Science and Technology
1-1, Asahidai, Nomi, Ishikawa, 923-1292 Japan
E-mail: {t-takagi, miyaji}@jaist.ac.jp

[††] Hiroshima City University
3-4-1 Ozuka-Higashi, Asa-Minami-Ku, Hiroshima 731-3194, Japan
E-mail: soshi@hiroshima-cu.ac.jp

Abstract

We propose and evaluate new quantum secret sharing schemes (QSSS) for sharing a classical secret between two groups, group 1 and group 2 . It is observed that the proposed scheme is secure against well-known attacks on QSSS, particularly attacks with single photons or EPR pairs.

1. Introduction

Quantum Secret Sharing Schemes (QSSS), which are enhanced by using quantum mechanics for *Secret Sharing Schemes* (SSS), were proposed by Hillery, Buzek, and Berthiaume [1] for the first time in 1999.

In 2005, a notable scheme of QSSS is proposed by Feng-Li Yan and Ting Gao[2]. In the proposed scheme classical secret information can be shared between two parties (one party with m members, called *Alice*, and the other with n members, called *Bob*), and the secret is divided in such a manner that all members of each party can reconstruct the secret, however, members fewer than the total number of members in each party cannot reconstruct the secret. Moreover the protocol has an advantage that it can be executed without quantum entanglement, Dealer (Trust party) or secure distribution of the shares. This type of protocol was continuously proposed in 2006, 2007 and 2008[3, 4, 5]. However, the disadvantage of such protocols is that the probability of success of an attack with a single photon[6] is $\frac{2m-1}{2m}$.

Therefore, in order to counter the abovementioned problem, in this paper, we propose a new quantum secret sharing scheme for sharing secrets between various parties. One of the advantages of our protocol is that it is secure against attacks with single photons. Apparently our scheme does not depend on quantum entanglement, designation of a Dealer (Trust party) and secure distribution of the shares. Furthermore, we shall demonstrate that our scheme is secure against several well-known attacks on QSSS.

This paper is organized as follows. In Section 2, we propose the scheme to overcome the problem. In section 3, we examine the security of our proposed scheme. Finally in Section 4 we conclude this paper.

This work was supported by KAKENHI (2070018).

2. Proposed Scheme

In this section, we propose a new quantum secret sharing scheme.

In our scheme, the following six states:

$$
\begin{aligned}
&|\phi_0^0\rangle = |0\rangle\,, && |\phi_0^1\rangle = |1\rangle\,,\\
&|\phi_1^0\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\,, && |\phi_1^1\rangle = -\frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle\,,\\
&|\phi_2^0\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\,, && |\phi_2^1\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle
\end{aligned}
\quad (1)
$$

and the following five quantum operations are used:

$$
U_0 = I, U_1 = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}, U_2 = \begin{pmatrix} -\frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \quad (2)
$$

$$
V_0 = I, V_2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (3)
$$

U_1, U_2 and V_1 operate in the following manner:

$$\begin{aligned} U_1: \quad & \{|\phi_0^0\rangle, |\phi_0^1\rangle\} \rightarrow \{|\phi_1^0\rangle, |\phi_1^1\rangle\} \\ & \rightarrow \{|\phi_2^0\rangle, |\phi_2^1\rangle\} \rightarrow \{|\phi_0^0\rangle, |\phi_0^1\rangle\}, \quad (4) \\ U_2: \quad & \{|\phi_0^0\rangle, |\phi_0^1\rangle\} \rightarrow \{|\phi_2^0\rangle, |\phi_2^1\rangle\} \\ & \rightarrow \{|\phi_1^0\rangle, |\phi_1^1\rangle\} \rightarrow \{|\phi_0^0\rangle, |\phi_0^1\rangle\} \quad \text{and} \quad (5) \\ V_1: \quad & \{|\phi_0^0\rangle, |\phi_1^0\rangle, |\phi_2^0\rangle\} \leftrightarrow \{|\phi_0^1\rangle, |\phi_1^1\rangle, |\phi_2^1\rangle\}. \quad (6) \end{aligned}$$

After completing the protocol, the classical secret information is shared between the parties *Alice* and *Bob*, and the information is divided in such a mannery that all members of each party can reconstruct the secret, ; however, members fewer the total number of members in each party cannot reconstruct the key.

Now we are in a position to present our new scheme, as follows:

(STEP1) Bob_j $(1 \leq j \leq n)$ creates a random bit string C_j and a random trit string D_j of length N, that is, $C_j = c_1^j, c_2^j, \cdots, c_N^j$ $(c_k^j \in_R \{0,1\})$, $D_j = d_1^j, d_2^j, \cdots, d_N^j$ $(d_k^j \in_R \{0,1,2\})$. Bob_j then creates the qubit string $|\Phi_j^0\rangle = \otimes_{k=1}^N |\varphi_{0,j,k}\rangle = \otimes_{k=1}^N |\phi_{d_k^j}^{c_k^j}\rangle$ of length N corresponding to C_j and D_j. Finally, Bob_j sends $|\Phi_j^0\rangle$ to $Alice_1$.

(STEP2) $Alice_1$ receives the qubit string (7) of length nN:

$$|\Phi^0\rangle = \otimes_{j=1}^n |\Phi_j^0\rangle \quad (7)$$

First, $Alice_1$ performs an eavesdropping check by using a part of the received qubit string. $Alice_1$ avoids invisible photons from an (possible) eavesdropper in a similar manner as that described in [7], and checks for eavesdropping by using a photon splitter [8] whether or not two or more photons in one signal appear in this communication. If an extra photon is discovered in the communication, then $Alice_1$ aborts this execution. Subsequently, $Alice_1$ evaluates the error-rate by measuring the qubit on a random basis and communicating with $Bob_{1,2,\cdots,n}$. If the error-rate is higher than some threshold value specified beforehand, then $Alice_1$ quits.

$Alice_1$ creates a bit string A_1 and a trit string B_1 of length nN at random, i.e., $A_1 = a_{1,1}^1, a_{1,2}^1, \cdots, a_{1,n}^1, a_{2,1}^1, \cdots, a_{n,N}^1$ $(a_{j,k}^1 \in_R \{0,1\})$, $B_2 = b_{1,1}^1, b_{1,2}^1, \cdots, b_{nN}^1$ $(b_{j,k}^1 \in_R \{0,1,2\})$. $Alice_1$ then applies the quantum operation $U_{b_{j,k}^1} V_{a_{j,k}^1}$ to the k-th $(1 \leq k \leq N)$ qubit sent by Bob_j. Here, the quantum operation $U_{b_{j,k}^1}$ is one of (2) and $V_{a_{j,k}^1}$ is one of (3) . The qubit state after applying the quantum operation is denoted by $|\phi_{1,j,k}\rangle$.

$Alice_1$ sends to $Alice_2$ the following qubit string:

$$\begin{aligned} |\Phi^1\rangle &= \otimes_{j=1}^n \otimes_{k=1}^N |\varphi_{1,j,k}\rangle \\ &= \otimes_{j=1}^n \otimes_{k=1}^N U_{b_{j,k}^1} V_{a_{j,k}^1} |\varphi_{0,j,k}\rangle . \quad (8) \end{aligned}$$

(STEP3) $Alice_i$ $(2 \leq i \leq m)$ performs the same operations performed by $Alice_1$. First, she performs an eavesdropping check and evaluates the error-rate by using a part of the received qubit string. Subsequently, $Alice_i$ creates the bit strings A_i and the trit string B_i of length nN at random, that is, $A_i = a_{1,1}^i, a_{1,2}^i, \cdots, a_{1,n}^i, a_{2,1}^i, \cdots, a_{n,N}^i$ $(a_{j,k}^i \in_R \{0,1\})$, $B_i = b_{1,1}^i, b_{1,2}^i, \cdots, b_{n,N}^i$ $(b_{j,k}^i \in_R \{0,1,2\})$, and applies the quantum operation $U_{b_{j,k}^i} V_{a_{j,k}^i}$ to the k-th $(1 \leq k \leq N)$ qubit sent by Bob_j.

(STEP4) $Alice_i$ $(2 \leq i < m)$ sends the following qubit string:

$$\begin{aligned} |\Phi^i\rangle &= \otimes_{j=1}^n \otimes_{k=1}^N |\varphi_{i,j,k}\rangle \\ &= \otimes_{j=1}^n \otimes_{k=1}^N U_{b_{j,k}^i} V_{a_{j,k}^i} |\varphi_{i-1,j,k}\rangle \quad (9) \end{aligned}$$

to $Alice_{i+1}$. $Alice_m$ sends the following qubit strings:

$$\begin{aligned} |\Phi_1^m\rangle &= \otimes_{k=1}^N |\varphi_{m,1,k}\rangle , \\ |\Phi_2^m\rangle &= \otimes_{k=1}^N |\varphi_{m,2,k}\rangle , \\ &\vdots \quad (10) \\ |\Phi_n^m\rangle &= \otimes_{k=1}^N |\varphi_{m,n,k}\rangle \end{aligned}$$

to $Bob_1, Bob_2, \cdots, Bob_n$ respectively.

(STEP5) Bob_j $(1 \leq j \leq n)$ performs an eavesdropping check and evaluates the error-rate by using a part of the received qubit string as well as *Alice*. Then, he asks $Alice_i$ to announce publicly the string B_i. Bob_j computes $x_{j,k} = d_{j,k} + \sum_{i=1}^m b_{i,j,k} \pmod 3$ and measures $|\varphi_{m,j,k}\rangle$, i.e., by measuring $\{|\phi_0^0\rangle\langle\phi_0^0|, |\phi_0^1\rangle\langle\phi_0^1|\}$ if $x_{j,k} = 0$; $\{|\phi_1^0\rangle\langle\phi_1^0|, |\phi_1^1\rangle\langle\phi_1^1|\}$ if $x_{j,k} = 1$; and $\{|\phi_2^0\rangle\langle\phi_2^0|, |\phi_2^1\rangle\langle\phi_2^1|\}$ if $x_{j,k} = 2$.

Let $e_{j,k}$ $(1 \leq j \leq n, 1 \leq k \leq N)$ be 0 or 1 according to the two cases of outputs of measurement of Bob_j's k-th $(1 \leq k \leq N)$ qubit: (i) $\{|\phi_0^0\rangle, |\phi_1^0\rangle, |\phi_2^0\rangle\}$, and (ii) $\{|\phi_0^1\rangle, |\phi_1^1\rangle, |\phi_2^1\rangle\}$, respectively.

(STEP6) Both hte parties (*Alice* and *Bob*) examine the number of qubits in the qubit strings that are (possibly) influenced by an eavesdropper (if it exists) or noise in this execution. Bob_j $(1 \leq j \leq n)$ randomly selects a part of the qubit string k_r and discloses it to the public. The members of both parties discloses their shares corresponding to the selected qubit string.

If the cases where $(e_{j,k_r} + d_{j,k_r}) = (\sum_{i=1}^{m} a_{i,j,k_r}) \bmod 2$ are insufficient, the execution is aborted and restarted from the beginning.

(STEP7) The share of $Alice_i (1 \leq i \leq m)$ is expressed as

$$s_i^{Alice} = \sum_{j=1}^{n} \sum_{k=1}^{N} a_{i,j,k} \pmod 2. \tag{11}$$

Moreover, the share of $Bob_j (1 \leq j \leq n)$ is expressed as

$$s_j^{Bob} = \sum_{k} e_{j,k} + d_{j,k} \pmod 2. \tag{12}$$

Therefore, if there is no eavesdropper and noise, then $S \equiv \sum_{i=1}^{m} s_i^{Alice} \equiv \sum_{j=1}^{n} s_j^{Bob} \bmod 2$ holds.

From this result, we can conclude that the secret is shared between both parties and it is divided in such a manner that all members of each party can reconstruct the secret, but no fewer number of members of each party can.

3. Security

In this section, we evaluate the security of our proposed scheme. We consider well-known attacks on QSSS[5]. The PNS attack, IPE scheme, and Trojan horse attack can be detected by using the test of (STEP2), (STEP3) and (STEP5)[4]. Therefore, in the subsequent section we consider other types of attacks such as attacks with single photons or EPR pairs and fake-signal attacks.

3.1. Attacks with single photons/EPR pairs

In this attack, first, in (STEP3) and (STEP4), attacker $Alice_m$ creates a random bit string A'_m and random trit string B'_m of length nN and sends the offensive photons $\otimes_{k=1}^{N} |\phi_{b_k^{m'}}^{a_k^{m'}}\rangle$ to Bob. Subsequently, in (STEP5), if it is requested that the trit string B be disclosed to the public by Bob, $Alice_m$ calculates B_m by using $B_1, B_2, \cdots B_{m-1}$ and B'_m to measure it accurately, and opens B_m.

This attack will succeed if $Alice_m$ selects correct states, or selects wrong states and Bob obtains a measurement result.

In our scheme, because the trit string D, that is the secret information of Bob, is necessary for deciding the basis, it is not possible to create a correct string B_m selected from the information sent by $Alice$. As a result, the scheme succeeds in the detection of this attack at a probability 1/2. Table1 shows the *worst* detection probability of the attack with single photons or EPR pairs for each qubit according to the evaluation method of [4]. The result in [4] should note that it is *not* the worst case, because the attacker is one person. When the detection probability becomes the worst, attackers is all members except one person of each group.

Table 1: Detection probability of the attack with single photons / EPR pair

scheme	probability
YG05[2]	0
YGL06[3]	$2/3m$
YGL07[4]	$1/2m$
YGL08[5]	$1/2(m+n-1)$
our scheme	1/2

Table1 indicates that our scheme is different from the existing researches with regard to the point that the detection probability does not depend on the number of members in of each group.

Hence, the proposed scheme is secure against the attacks with single photons or EPR pairs.

3.2. Fake-Signal Attack with any Two-Particle Entangle States

We estimate the maximum probability with which we can obtain the correct measurement result by a fake-signal attack with any two-particle entangle states. In this attack, attacker $Alice_i$ generates a general EPR-pair $|\psi\rangle$,

$$|\psi\rangle = |0\rangle_A |\alpha\rangle_E + |1\rangle_A |\beta\rangle_E \tag{13}$$

where $|\alpha\rangle_E$ and $|\beta\rangle_E$ are unnormalized states. Subsequently, $Alice_i$ sends particle A in $|\psi\rangle$ to $Alice_{i+1}$ and holds particle E. The particle A is collected after quantum operations are applied by $Alice_{i+1}$, and the attacker must distinguish between all the states that can be taken. The probability of success of the fake-signal attack for the proposed and previous schemes are summarized in Table 2.

Table 2: Success probability of the fake-signal attack

scheme	probability
YG05[2]	1
YGL06[3]	$1-(1+\sqrt{2})/8$
YGL07[4]	$1-\sqrt{2}/7$
YGL08[5]	$1-\sqrt{2}/7$
our scheme	1/2

Therefore, the proposed scheme is secure against a fake-signal attack with two-particle entangle states.

4. Conclusion

In this paper, we proposed a scheme which shares the secret between two parties and divides it in such a manner that all members of each party can reconstruct the secret, but members fewer than the number of members in each party cannot reconstruct the secret. The proposed scheme, does not depend on quantum entanglement, designation of a Dealer (Trust party) and secure distribution of the shares. Furthermore, we showed that our scheme is secure against several well-known attacks on QSSS, particularly, attacks with single photons or EPR pairs.

References

[1] M. Hillery, V. Bužek and A. Berthiaume: "Quantum secret sharing", Phys. Rev. A, **59**, 3, pp. 1829–1834 (1999).

[2] F.-L. Yan and T. Gao: "Quantum secret sharing between multiparty and multiparty without entanglement", Phys. Rev. A, **72**, p. 012304 (2005).

[3] F.-L. Yan, T. Gao and Y.-C. Li: "Quantum secret sharing between m-party and n-party with six states". quant-ph/0601111.

[4] F.-L. Yan, T. Gao and Y.-C. Li: "Quantum secret sharing between multiparty and multiparty with four states", Science in China Series G: Physics Mechanics and Astronomy, **50**, p. 572 (2007).

[5] F.-L. Yan, T. Gao and Y.-C. Li: "Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations". quant-ph/0801.4052.

[6] C.-M. Li, C.-C. Chang and T. Hwang: "Comment on "quantum secret sharing between multiparty and multiparty without entanglement"", Phys. Rev. A, **73**, 1, p. 016301 (2006).

[7] W.-H. Kye and M. S. Kim: "Kye and kim reply:", Physical Review Letters, **96**, 7, p. 078902 (2006).

[8] X.-B. Wang: "Beating the photon-number-splitting attack in practical quantum cryptography", Physical Review Letters, **94**, 23, p. 230503 (2005).