Int J Theor Phys (2012) 51:1674–1679
DOI 10.1007/s10773-011-1044-z

# Multiparty Quantum Secret Information Sharing in Enterprise Management Based on Single Qubit with Random Rotation Angle

**Sheng-Bin Hao · Bo Yu**

Received: 29 September 2011 / Accepted: 30 November 2011 / Published online: 17 December 2011


**Abstract** We propose a new multiparty quantum secret information sharing (MQSIS) scheme in enterprise management based on single-qubit with arbitrarily random rotation angle. The secret messages are split into several parts, and each part is distributed to a separate information receiver by transmitting qubits with arbitrary rotation angles. We show that the present scheme can efficiently resist the measure-resend attack, disturbance attack, intercept-and-resend attack, entangle-measure attack, and PNS attack.

**Keywords** Multiparty quantum secret information sharing · Single-qubit · Random rotation angle · Hash function

Quantum communication has become one of the most promising applications of quantum mechanics in quantum information science today. Quantum secret information sharing (QSIS), which is a quantum mechanical version of classical secret sharing scheme [1, 2], is an useful tool in the cryptographic applications and has attracted a lot of attention [3–11]. The interesting aspect of employing quantum mechanics for secret sharing is that it allows for the unconditionally secure distribution of the information between the participants. The basic idea of secret sharing in the simplest case is that a secret message is shared between two persons, say Bob and Charlie who are not entirely trusted by Alice, in such a way that it can only be absolutely recovered if both of them agree to collaborate. In 1999, Hillery et al. [3] first proposed a QSIS scheme using three-particle and four-particle Greenberger-Horne-Zeilinger (GHZ) entangled states for distributing a private key among some agents and sharing a classical information. Subsequently, Karlsson et al. [4] put forward another QSIS scheme with a two-photon polarization-entangled state. So far a lot of QSIS schemes [6, 7, 10, 12–19] have been proposed in both theoretical and experimental aspects. In all these QSIS schemes [6–19], quantum entanglement plays a important role. In other words, multiparticle entangled states are widely used to implement the QSIS schemes.

S.-B. Hao (✉) · B. Yu
School of Management, Department of Business Management, Harbin Institute of Technology, Harbin, Heilongjiang 150001, People's Republic of China
e-mail: haoshengbin@hit.edu.cn

Very recently, a particular quantum key distribution (QKD) scheme has been proposed by Kye and Kim [20], in which the basis reconciliation via a classical channel is not necessary as a advantage. In this paper, based on Kye-Kim's QKD scheme, we propose a MQSIS scheme by using single-qubit with arbitrarily random rotation angle. In this MQSIS scheme, Alice randomly chooses a value of angle $\theta_i$ and prepares a single-qubit state with the rotation of that angle. The receivers rotate the received qubit states by $-\theta_i$ and then measure the qubits to read out the states of qubits, i.e., Alice's secret messages. If all the receivers agree to cooperate, they can successfully share Alice's secret messages. Otherwise, nobody can get access to Alice's secret messages with 100% certainty.

Now let us turn to depict our MQSIS scheme. For convenience, let us first describe a three-party QSIS scheme, and then generalize it to the case of $N$ agents. Suppose that Alice is the boss, Bob and Charlie are two employees in an enterprise. Here Alice wants to send a secret message to two distant employees, Bob and Charlie. However, Alice doubts that one of them may be dishonest and she does not know who the dishonest one is, but she knows that if the two employees coexist, the honest one will keep the dishonest one from doing any damage. Bob and Charlie, can obtain Alice's secret messages only by their mutual cooperation. In this three-party QSIS scheme, Alice, Bob and Charlie agree that they utilize the formula: $M_{A_i} = M_{B_i} \oplus M_{C_i}$ $(i = 1, 2, 3, \ldots, m)$ to decode Alice's secret messages, where $M_{A_i}$ represents Alice's secret message, $M_{B_i}$ represents Bob's measurement result, $M_{C_i}$ represents Charlie's measurement result, $\oplus$ represents an addition mod 2, and $M_{A_i}, M_{B_i}, M_{C_i} \in \{0, 1\}$. This three-party QSIS scheme can be completed with the following procedures below.

Step 1: Suppose that Alice has a secret message sequence $\{M_{A_1}, M_{A_2}, \ldots, M_{A_m}\}$ $(M_{A_i} \in \{0, 1\}, i = 1, 2, \ldots, m)$, she prepares two sets of ordered sequences of qubits according to her secret message sequence: $[B_1, B_2, \ldots, B_m]$, $[C_1, C_2, \ldots, C_m]$, where $B_i, C_i \in \{|0\rangle, |1\rangle\}$, the subscript indicates each qubit's order in the sequence, and $|0\rangle$ and $|1\rangle$ represent two orthogonal states of the qubit respectively. We call them $B$ sequence and $C$ sequence, respectively. For instance, if Alice's secret message is 0, she prepares qubits $B_i$, $C_i$ in the states $|0\rangle_B, |0\rangle_C$ or $|1\rangle_B, |1\rangle_C$; if Alice's secret message is 1, she prepares qubits $B_i$, $C_i$ in the states $|0\rangle_B, |1\rangle_C$ or $|1\rangle_B, |0\rangle_C$. Then Alice rotates each qubit in sequence $B$ by a arbitrary angle $\theta_{B_i}$, and a arbitrary angle $\theta_{C_i}$ for each qubit in sequence $C$. After that, the state of qubit becomes:

$$\begin{aligned} |0\rangle &\longrightarrow U_y(\theta)|0\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \\ |1\rangle &\longrightarrow U_y(\theta)|1\rangle = -\sin\theta|0\rangle + \cos\theta|1\rangle, \end{aligned} \tag{1}$$

where $U_y(\theta) = \cos\theta I - i\sin\theta\sigma_y$ is the unitary operator which rotates the arbitrary angle along the $y$ axis and $I$ is the identity operator, $\sigma_y$ is the Pauli-$y$ operator. Then Alice first sends the $B$ sequence to Bob.

Step 2: Bob confirms Alice that he has received the $B$ sequence via classical channel. Then he checks the security of transmission for sequence $B$ with Alice. Usually, in order to check the security of transmission, the common method is to use a public channel to reveal some part of qubits [6, 7]. That verification method has two disadvantages. (1) It usually degrades the efficiency for qubits. (2) It does not guarantee the integrity of the *remaining qubits*. *In order to overcome those problems*, we utilize the one-way hash function as Ref. [20] for checking the integrity of the qubits.

Step 3: Alice first announces some of the values of angle $\theta_{B_i}$ that she rotated for each qubit in sequence $B$ and the one-way hash function $H$ via a classical channel.

Step 4: Bob rotates the corresponding angle of each qubit in sequence $B$ by $-\theta_{B_i}$ and then measures them under the measuring basis (MB) $Z \equiv \{|0\rangle, |1\rangle\}$. Alice and Bob evaluate the

hash function values, $h_{A_1} = H(k_{A_1})$ and $h_{B_1} = H(k_{B_1})$ respectively, where $k_{A_1}$ and $k_{B_1}$ are shared keys in Alice and Bob. If $h_{A_1} = h_{B_1}$, they keep the shared keys, and Alice announces the other values of angle $\theta_{B_i}$ that she rotated for each qubit in sequence $B$. Otherwise, they abolish the keys and start the process again from Step 1. Alice and Bob evaluate the hash function values of the remaining qubits respectively, $h_{A_2} = H(k_{A_2})$ and $h_{B_2} = H(k_{B_2})$. If $h_{A_2} = h_{B_2}$, they keep the shared keys, otherwise, they abolish the keys and start the process again from Step 1.

In Step 4, the difference between $h_A$ and $h_B$ ($h_A = h_{A_1} + h_{A_2}$ and $h_B = h_{B_1} + h_{B_2}$) shows that Alice and Bob do not share the exactly same keys. This is due to imperfection in the transmission or to Eve (eavesdropper) who intervened between Alice and Bob.

Step 5: After ensuring the security of the transmission for sequence $B$, Alice sends the sequence $C$ to Charlie and announces the one-way hash function $H$ via a classical channel.

Step 6: Alice and Charlie check the security of transmission for sequence $C$, similar to that for sequence $B$. If $h_A = h_C$, they keep the shared keys, otherwise, they abolish the keys and start the process again from Step 1.

Step 7: If Bob and Charlie collaborate, they can decode Alice's secret messages utilizing the formula: $M_{A_i} = M_{B_i} \oplus M_{C_i}$. Otherwise, neither of them can get Alice's secret messages with the probability 100%.

So far we have proposed a three-party QSIS scheme based on Kye-Kim's QKD scheme [20] by using single-qubit with arbitrarily random rotation angle. In Kye-Kim's scheme, in order to share a key between Alice and Bob, the qubit need being transmitted three times, it is not secure because of too many times of transmission between the sender and the receiver (see [21] in detail). Different from Kye-Kim's scheme, in the present scheme, in order to share a key between Alice and Bob (or Alice and Charlie), the qubit only need being transmitted once depending on adding classical communication once, which ensures the security of the present scheme against eavesdropping which we will discuss later.

Now let us generalize the three-party QSIS scheme to the case of $N$ agents, Bob, Charlie, Dick, ..., and Zack. The basic step of the MQSIS scheme is the same as that in the three-party QSIS scheme.

Step I: Alice prepares $N$ sets of ordered sequences of qubits according to her secret message sequence: $[B_1, B_2, \ldots, B_m]$, $[C_1, C_2, \ldots, C_m]$, ..., $[Z_1, Z_2, \ldots, Z_m]$. Then Alice first sends sequence $B$ to Bob.

Step II: Bob confirms Alice that he has received the $B$ sequence. Alice first announces some of the values of angle $\theta_{B_i}$ that she rotated for each qubit in sequence $B$ and the one-way hash function $H$. Bob rotates the corresponding angle of each qubit in sequence $B$ by $-\theta_{B_i}$ and then measures them under the MB $Z$. Alice and Bob evaluate the hash function values, $h_{A_1} = H(k_{A_1})$ and $h_{B_1} = H(k_{B_1})$ respectively. If $h_{A_1} = h_{B_1}$, they keep the shared keys, and Alice announces the other values of angle $\theta_{B_i}$ that she rotated for each qubit in sequence $B$. Otherwise, they abolish the keys and start the process again from Step 1. Alice and Bob evaluate the hash function values of the remaining qubits respectively, $h_{A_2} = H(k_{A_2})$ and $h_{B_2} = H(k_{B_2})$. If $h_{A_2} = h_{B_2}$, they keep the shared keys, otherwise, they abolish the keys and start the process again from Step 1.

Step III: After ensuring the security of the transmission for sequence $B$, Alice sends sequence $C$ to Charlie.

Step IV: After repeating the step II $N$ times, the $Z$ sequence is received securely by the last agent, say Zach. Then Alice and Zach evaluate the hash function values, $h_A = H(k_A)$ and $h_Z = H(k_Z)$ respectively. If $h_A = h_Z$, they keep the shared keys, otherwise, they abolish the keys and start the process again from Step 1.

Step V: If all the agents collaborate, they can decode Alice's secret messages utilizing the formula: $M_{A_i} = M_{B_i} \oplus M_{C_i} \oplus \ldots \oplus M_{Z_i}$.

So far we have established a MQSIS scheme based on single-qubit with arbitrarily random rotation angle. In our MQSS scheme, only the single-qubit states are used, the multi-qubit GHZ states in all the existing MQSS schemes [3, 13, 14] are not necessary. Although in [18], they claimed that only the Bell states are required, they must distinguish the multi-qubit GHZ states, which makes the scheme experimentally difficult to realize. It is known that the preparation of multi-qubit entangled states is very complicated and difficult in experiment, so our scheme is easier and simpler than the existing MQSIS schemes [3, 13, 14, 18] to the implementation of MQSIS.

Now we analyze the security of the present scheme. For a perfect quantum channel with single-qubit, it is obvious that Eve can not obtain much information by the measure-resend attack, disturbance attack, intercept-and-resend attack, and entangle-measure attack as all the transmissions of qubits are of random rotation. In this scheme, the random rotation depend on the equator of the Poincaré sphere. The optimum estimation of a qubit in this case gives the fidelity 3/4 [22] where the fidelity is one when the estimation is perfect or zero when the initial state is orthogonal to the estimation.

Let us continue to discuss how the present MQSIS scheme can efficiently resist the measure-resend attack, disturbance attack, intercept-and-resend attack, entangle-measure attack, and PNS attack, respectively.

*Measure-resend attack*—Eve intercepts the qubits emerging from Alice and measures them under the MB $Z$, then she resends them to the receiver $M$. The initial superposition states of qubits will probabilistically collapse into $|0\rangle$ states or $|1\rangle$ states of qubits after Eve's measurement. The receiver $M$ rotates the states of qubits by $-\theta_{M_i}$ and then measures them, he will probabilistically obtain $|0\rangle$ states or $|1\rangle$ states of qubits. Hence Eve's attack will be detected after the receiver $M$ compares the values of hash function with Alice.

*Disturbance attack*—Eve can intercept the qubits when the qubits are transmitted from Alice to the receiver $M$ and randomly perform one of the four unitary operations $I$, $\sigma_x$, $i\sigma_y$, and $\sigma_z$ ($I$ is the identity operator, and $\sigma_x$, $i\sigma_y$, and $\sigma_z$ are the Pauli operators) on each qubit. By doing so, the initial superposition states of qubits will be changed. In this case, after the receiver $M$ rotates the states of qubits by $-\theta_{M_i}$ and measures them, he will obtain the wrong results. This behavior will be found after the receiver $M$ compares the values of hash function with Alice.

*Intercept-and-resend attack*—Suppose that Eve prepares a lot of the single qubits in the state $(|0\rangle, |1\rangle)$ or $(\alpha|0\rangle + \beta|1\rangle, \alpha|0\rangle - \beta|1\rangle)$ randomly. When Alice sends qubits to the receiver $M$, Eve intercepts the qubits and keeps them with him, and sends the qubits that he prepared to the receiver $M$. The receiver $M$ will take the fake qubits for Alice's, and rotate the fake qubits by $-\theta_{M_i}$ and measure them. This behavior can also be found after the receiver $M$ compares the values of hash function with Alice.

*Entangle-measure attack*—Eve may steal some information by entangling his auxiliary qubit (prepared, say, in the state $|\chi\rangle_E$) with a qubit $m$ (assumed to be in the state $|i\rangle_M$) before the qubit reaches the receiver $M$: $|\chi\rangle_E|i\rangle_m \longrightarrow \alpha|\chi_i\rangle_E|i\rangle_m + \beta|\overline{\chi}_i\rangle_E|i \oplus 1\rangle_m$ where $|\alpha|^2 + |\beta|^2 = 1$ and ${}_E\langle\chi_i|\overline{\chi}_i\rangle_E = 0$. Then he resends the qubit $m$ to the receiver $M$. After the receiver $M$ rotates the states of qubits by $-\theta_{M_i}$, the state of qubits $E$, $m$ become a two-qubit entangled state consist of the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. The initial state prepared by Alice is completely destroyed. When the receiver $M$ measures the qubit $m$, he will obtain the correct and wrong result with the probability 1/2 respectively, while Eve can not obtain the correct secret message too. But after the receiver $M$ compares the values of hash function with Alice, they will find the existence of Eve.

In the above discussions, we analyze the security of the present scheme and show that how the present scheme can efficiently against different kinds of attacks only for the perfect

quantum channel, i.e., a noise-free quantum channel. In a noise quantum channel, the error correction and the privacy amplification techniques should be used on those qubits for improving the security. The quantum error correction technique is not difficult in principle to be implemented, and a quantum privacy amplification way for the single-qubit was proposed also [23]. Now let us consider the most efficient attack in practice, i.e., PNS attack.

*PNS attack*—In practice, a reliable single-photon source for MQSIS is not very economical, we can use not-so weak coherent laser pulses as qubits in the present scheme. It is known that if a message is encoded on a coherent-state pulse, the scheme may be insecure under the PNS attack which is a conventional strategy for weak coherent laser pulses. Eve can split out a qubit from each pulse and keep it in the quantum storage. In Kye-Kim's scheme [20], they give out the maximum amount of information Eve can get from the channel

$$I_E = \sum_{n=0}^{\infty} P(n) I(n). \tag{2}$$

Where

$$P(n) = \exp[-(1-\eta^2)\alpha^2] \frac{[(1-\eta^2)\alpha^2]^n}{n!}, \tag{3}$$

is the probability of there being $n$ photons in the coherent state $|\sqrt{1-\eta^2}\rangle\alpha$, and

$$I(n) = \frac{1}{2} + \frac{1}{2^{n+1}} \sum_{l=0}^{n-1} \sqrt{\binom{n}{l}\binom{n}{l+1}}, \tag{4}$$

is the maximal mean fidelity of the optimum state estimation from $n$ qubits. The amount of information $I_E$ which Eve can get grows as $\eta$ ($\eta$ is the amplitude transmittivity of the beam splitter) grows but it eventually converges to $I_E = 0.5$ as $\eta^2 \longrightarrow 1$. On the other hand, if Eve can split out a qubit from each pulse, then after Alice announces the values of angle $\theta_{B_i}$ to Bob, Eve rotates the corresponding angle of each qubit by $-\theta_{B_i}$ and then measures them under the MB $Z$, Eve can absolutely get the message of the sequence $B$ without being detected. In order to prevent the PNS attack of Eve's, Alice should also put some PNSs near the single-photon source and split out the qubits from each pulse and keep them in her own quantum storage so that only one complete single-photon quantum signal being sent to the receiver. In this way, Eve cannot split out a qubit from each pulse and get Alice's messages without being found.

In summary, we proposed a new MQSIS scheme using single-qubit with arbitrarily random rotation angle. Alice rotates each qubit by a arbitrary angle $\theta_i$, which is equivalent to the encryption on each qubit with a random key, which makes any other one have no ability for reading out the information on the qubit. Since we do not need to reveal some qubits to check the security of transmission for the qubits by using hash function, its intrinsic efficiency for qubit approaches the maximal value. The measure-resend attack, disturbance attack, intercept-and-resend attack, and entangle-measure attack can be detected via comparing the hash function between Alice and the receivers. The PNS attack can also be prevented by using the PNSs to split out the qubits from each pulse so that only one complete single-photon quantum signal being sent to the receiver. If all the receivers agree to cooperate, they can successfully share Alice's secret messages. Otherwise, nobody can get access to Alice's secret messages.

**Acknowledgements** This work was supported by the Fundamental Research Funds for the Central Universities under Grant No. HIT.HHS. 201101.

## References


1. Blakley, G.R.: In: Proceeding of the American Federation of Information Processing 1979 National Computer Conference, pp. 313–317. American Federation of Information Processing, Arlington (1979)
2. Shamir, A.: Commun. ACM **22**, 612 (1979)
3. Hillery, M., Buzek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
4. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
5. Nascimento, A.C.A., Mueller-Quade, J., Imai, H.: Phys. Rev. A **64**, 042311 (2001)
6. Guo, G.P., Guo, G.C.: Phys. Lett. A **310**, 247 (2003)
7. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Lam, P.K.: Phys. Rev. Lett. **92**, 177903 (2004)
8. Deng, F.G., Zhou, H.Y., Long, G.L.: Phys. Lett. A **337**, 329 (2005)
9. Deng, F.G., Long, G.L., Zhou, H.Y.: Phys. Lett. A **340**, 43 (2005)
10. Hsu, L.Y., Li, C.M.: Phys. Rev. A **71**, 022321 (2005)
11. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Tyc, T., Ralph, T.C., Lam, P.K.: Phys. Rev. A **71**, 033814 (2005)
12. Tittel, W., Zbinden, H., Gisin, N.: Phys. Rev. A **63**, 042301 (2001)
13. Bandyopadhyay, S.: Phys. Rev. A **62**, 012308 (2000)
14. Cleve, R., Gottesman, D., Lo, H.K.: Phys. Rev. Lett. **83**, 648 (1999)
15. Chau, H.F.: Phys. Rev. A **66**, 060302(R) (2002)
16. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A **69**, 052307 (2004)
17. Yan, F.L., Gao, T.: Phys. Rev. A **72**, 012304 (2005)
18. Li, M.Y., Zhang, K.S., Peng, K.C.: Phys. Lett. A **324**, 420 (2004)
19. Zhang, Y.Q., Jin, X.R., Zhang, S.: Phys. Lett. A **341**, 380 (2005)
20. Kye, W.H., Kim, C.M.: Phys. Rev. Lett. **95**, 040501 (2005)
21. Zhang, Q., Wang, X.B., Chen, Y.A., Yang, T., Pan, J.W.: Phys. Rev. Lett. **96**, 078901 (2006)
22. Derka, R., Buzek, V., Ekert, A.K.: Phys. Rev. Lett. **80**, 1571 (1998)
23. Deng, F.G., Long, G.L.: quant-ph/0408102