Quantum Secret Sharing Using GHZ-Like State

Commun. Theor. Phys. (Beijing, China) **54** (2010) pp. 1019–1022
© Chinese Physical Society and IOP Publishing Ltd Vol. 54, No. 6, December 15, 2010

Quantum Secret Sharing Using GHZ-Like State*

Chao-Ren Hsieh (谢朝任), Chia-Wei Tasi (蔡家纬),† and Tzonelih Hwang (黄宗立)

Department of Computer Science and Information Engineering, National Cheng Kung University, Tainan City 701, Taiwan, China

(Received March 19, 2010; revised manuscript received May 27, 2010)

Abstract *This paper presents a simple and novel quantum secret sharing scheme using GHZ-like state. The characteristics of the GHZ-like state are used to develop the quantum secret sharing scheme. In contrast with the other GHZ-based QSS protocols with the same assumptions, the proposed protocol provides the best quantum bit efficiency.*

PACS numbers: 03.67.Hk, 03.65.Ud
Key words: quantum cryptography, quantum secret sharing, GHZ-like state

1 Introduction

Quantum secret sharing (QSS), an important branch of quantum cryptography, is the generalization of classical secret sharing into a quantum scenario. The main idea of secret sharing is that Alice, the boss, expects to share her secret to both Bob and Charlie, the employees. Alice's secret can be revealed only when Bob and Charlie cooperate with each other. None of them can derive the secret alone.

Since Hillery *et al.* proposed the first quantum secret sharing scheme,[1] namely HBB QSS, using Greenberger-Horne-Zeilinger (GHZ) state, various QSS protocols have been proposed. References [2–6] constructed QSS schemes based on the single photon. References [7–15] devised QSS schemes based on the characteristic of Einstein-Podolsky-Rosen (EPR) pair. Reference [17] used the dense coding of GHZ states to establish QSS protocol. Moreover, the Grover's algorithm and the quantum fourier transform (QFT) have also been employed to establish QSS protocols in Refs. [18] and [19], respectively.

It is noted here that all the above mentioned QSS schemes assume that Alice, the boss, does not have to share any secret information beforehand with the other agents in order to distribute the shadows. Though Ref. [16] did improve the HBB QSS to a multi-party environment and also highly enhance the quantum efficiency, it essentially assumes that the boss shares some secret information with the agents. Therefore, it will not be considered as a target scheme to compare with in the latter section. Similarly, another promising research direction focusing on the secret sharing of quantum states instead of classical bit information, such as in Refs. [20–22], will not be discussed here too.

In 2008, Yang *et al.*[23] introduced the GHZ-like entangled quantum state,

$$|\psi\rangle = \frac{1}{2}(|010\rangle + |100\rangle + |001\rangle + |111\rangle)\,,$$

which can be constructed from an EPR pair and a single photon rather than from the GHZ experiment. An important characteristic is that the GHZ-like state is robust against loss of any single qubit. That is, if a particle is lost in the GHZ-like state, the remaining two particles still have an entanglement relationship between each other. On the other hand, if any one of qubits in the GHZ state is lost, the other two particles reduce to a product state without any entanglement relationship.

Based on this property and an observation on the GHZ-like state described in the next section, a QSS scheme will be proposed among three parties, Alice, Bob, and Charlie. The two agents, Bob and Charlie use only the single photon R-basis measurement on their qubit to obtain the shadows. Unitary operations or round trip quantum channels that are frequently used in other QSS's, are not needed here. Moreover, the insertion of single photons and the rearrangement of order particles[24] are used to ensure the security during the quantum transmission.

This paper is organized as follows. Section 2 proposes a quantum secret sharing scheme using GHZ-like state. Section 3 analyzes the security of proposed scheme. Finally, Sec. 4 makes a short conclusion.

2 QSS using GHZ-Like State

This section introduces an observation on the GHZ-like state in Subsec. 2.1 and then proposes the new QSS scheme in Subsec. 2.2.

2.1 *An Observation on GHZ-Like State*

From Yang's GHZ-like state

$$|\psi\rangle = \frac{1}{2}(|010\rangle + |100\rangle + |001\rangle + |111\rangle)\,,$$

it is easily observed that if Alice, Bob, and Charlie measure the first, the second, and the third particle of the same GHZ-like state by the R-basis respectively to obtain the corresponding measurement results: a, b, and c, then

*Supported by the National Science Council, Taiwan, China, under the Contract No. NSC 98-2221-E-006-097-MY3

†Corresponding author, E-mail: redbear676@gmail.com

these measuring results have the following relationship: $a = \overline{b \oplus c}$.

Base on this observation, we are going to develop the new QSS scheme among three parties.

2.2 *Proposed QSS Scheme*

This section describes the detailed process of the proposed QSS using GHZ-like state (see also Fig. 1). The notations used in the QSS scheme are given as follows:

$$R\text{-basis} = \{|0\rangle, |1\rangle\}\,, \quad D\text{-basis} = \Big\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big\}\,.$$

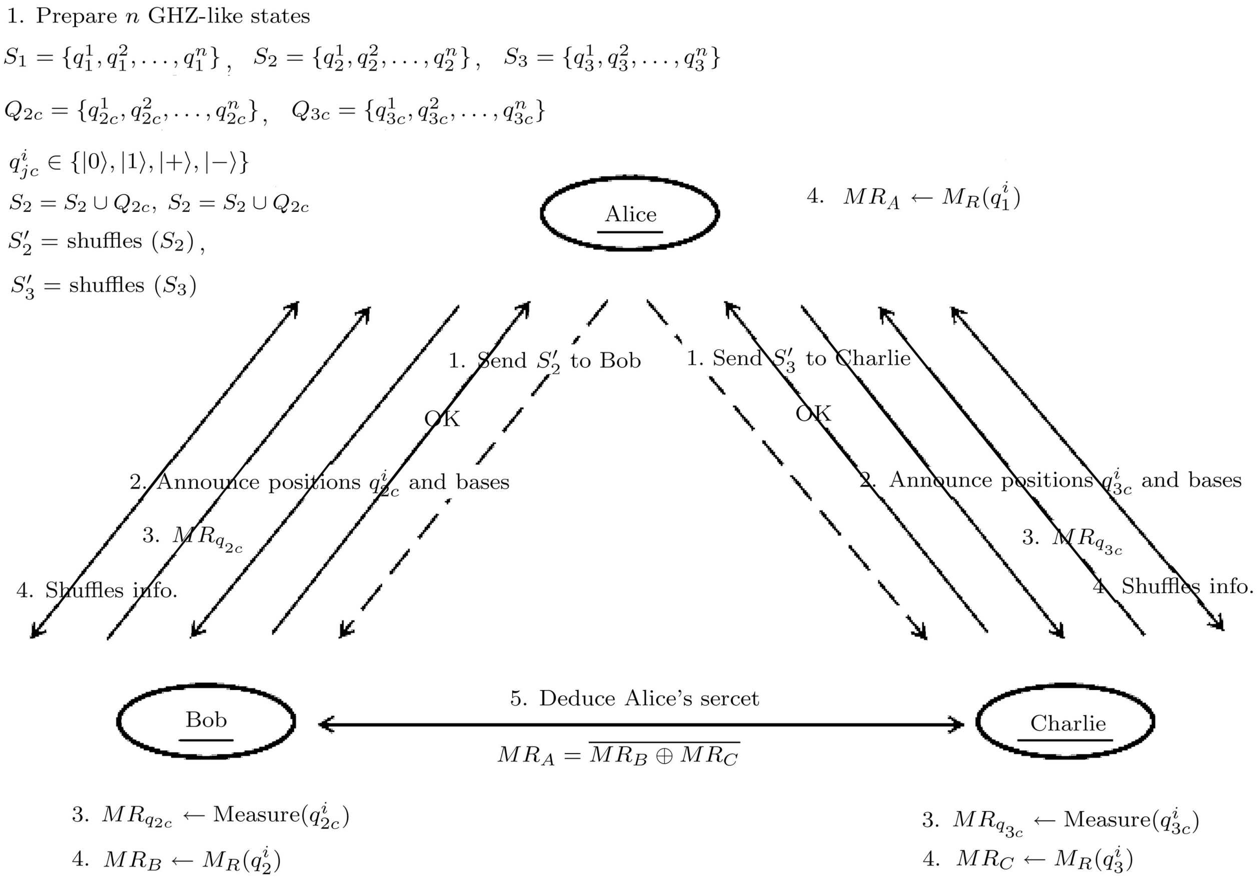
1. Prepare n GHZ-like states
$S_1 = \{q_1^1, q_1^2, \ldots, q_1^n\}$, $S_2 = \{q_2^1, q_2^2, \ldots, q_2^n\}$, $S_3 = \{q_3^1, q_3^2, \ldots, q_3^n\}$
$Q_{2c} = \{q_{2c}^1, q_{2c}^2, \ldots, q_{2c}^n\}$, $Q_{3c} = \{q_{3c}^1, q_{3c}^2, \ldots, q_{3c}^n\}$
$q_{jc}^i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$
$S_2 = S_2 \cup Q_{2c},\ S_2 = S_2 \cup Q_{2c}$
$S_2' =$ shuffles (S_2),
$S_3' =$ shuffles (S_3)
Alice
4. $MR_A \leftarrow M_R(q_1^i)$
1. Send S_2' to Bob
1. Send S_3' to Charlie
OK
OK
2. Announce positions q_{2c}^i and bases
2. Announce positions q_{3c}^i and bases
3. $MR_{q_{2c}}$
3. $MR_{q_{3c}}$
4. Shuffles info.
4. Shuffles info.
5. Deduce Alice's sercet
Bob
Charlie
$MR_A = \overline{MR_B \oplus MR_C}$
3. $MR_{q_{2c}} \leftarrow$ Measure(q_{2c}^i)
4. $MR_B \leftarrow M_R(q_2^i)$
3. $MR_{q_{3c}} \leftarrow$ Measure(q_{3c}^i)
4. $MR_C \leftarrow M_R(q_3^i)$

Fig. 1 Steps of quantum secret sharing scheme.

There are five steps in the protocol:

Step 1 Alice prepares a sequence of n GHZ-like states. By the multi-step transmission[25] and the block transmission,[26] Alice transmits photons to Bob and Charlie. She first divides particles of these GHZ-like states into three sequences: $S_1 = \{q_1^1, q_1^2, \ldots, q_1^n\}$, $S_2 = \{q_2^1, q_2^2, \ldots, q_2^n\}$, and $S_3 = \{q_3^1, q_3^2, \ldots, q_3^n\}$, where q_1^i, q_2^i, and q_3^i are the order of particles in the i-th GHZ-like state and $i = 1, 2, \ldots, n$. Then, Alice prepares sufficient single photons $Q_{2c} = \{q_{2c}^1, q_{2c}^2, \ldots, q_{2c}^n\}$, and $Q_{3c} = \{q_{3c}^1, q_{3c}^2, \ldots, q_{3c}^n\}$ where $q_{jc}^i \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ ($i = 1, 2, \ldots, n$ and $j = 2, 3$) for eavesdropper checking and appends photons in Q_{2c} and Q_{3c} to the sequences S_2 and S_3, respectively. Alice shuffles the particles in the sequences S_2 and S_3 to get S_2' and S_3', respectively.[24] Then, she sends the sequences S_2' and S_3' to Bob and Charlie, respectively. S_1 is kept to herself.

Step 2 After Alice confirms that Bob and Charlie have received all particles, she announces all the positions and the measuring bases of the single photons q_{jc}^i's in the sequences S_2' and S_3'. Bob (and Charlie) selects the corresponding particles q_{2c}^i's (q_{3c}^i's) from the sequences S_2' (and S_3') and measures these particles by the corresponding bases.

Step 3 Bob and Charlie send their measuring results to Alice respectively. Because Alice knows the initial states of the single photons q_{jc}^i, she can evaluate the error rate by comparing their measuring results. If the error rate exceeds a predetermined threshold, Alice aborts this communication and starts a new one.

Step 4 Alice announces the order of the remaining particles in the sequences S_2' and S_3' for Bob and Charlie to recover their particles in the original order respectively. Then, Alice, Bob, and Charlie measure their particles by the R-basis to get the measuring results MR_A, MR_B, and MR_C respectively. Alice performs exclusive-or operation on MR_A and K, her master key, to obtain K_A. Finally, she publishes the K_A to Bob and Charlie.

Step 5 When Bob and Charlie want to reveal Alice's master key K, they collaboratively use the exclusive-or and complement operation on their measuring results to obtain MR_A, i.e., $MR_A = \overline{MR_B \oplus MR_C}$. Then, Alice's master key K can be revealed by $K = MR_A \oplus K_A$.

The proposed QSS is based on the above mentioned robust property and the observation on the GHZ-like state. The robust characteristic of the GHZ-like state prevents any agent from knowing the other agent's measuring results and thus Bob (or Charlie) alone cannot obtain Alice's secret key without the other agent's cooperation. The observation, on the other hand, allows both agents to reveal Alice's secret using only the exclusive-or and the complement operation. In the protocol, the insertion of single photons and the rearrangement of order particles facilitate the eavesdropping checking process.

3 Security and Efficiency Analysis

This section is divided into three subsections. Subsec. 3.1 analyzes the eavesdropping detection of the proposed scheme. Subsec. 3.2 discusses secret sharing policy and shows that none of the two agents can reveal Alice's secrets alone without the cooperation of the other agent. Finally, Subsec. 3.3 analyzes the efficiency of the proposed QSS protocol and shows that it is more efficient than the HBB QSS.

3.1 *Eavesdropper Checking*

Considering the intercept-resend attack, assume that Eve is an eavesdropper. Eve intercepts both sequences S_2' and S_3' and measures all particles by the R-basis. He then generates fake particles base on these measuring results. Then, he sends the fake particles to Bob and Charlie, respectively. However, in average half of the single photons q_{jc}^i should be measured by the D-basis. If a single photon q_{jc}^i is measured by the wrong basis (Eve does not know the permutation order on S_2' and S_3', thus he does not even know the positions of q_{jc}^i's.), an inconsistent result may be detected during the eavesdropper checking with a probability of $1/4$. Thus, the probability for Eve to be detected in the eavesdropper checking is $1-(1-1/4)^{n/4}$.

3.2 *Secret Sharing Policy*

None of the two agents alone can reveal Alice's secret without the cooperation of the other. For instance, assume that Bob wants to obtain Alice's secret based on his measuring result alone. For example, if Bob's measuring result is $|0\rangle$, the GHZ-like state reduces to $(1/\sqrt{2})(|100\rangle+|001\rangle)_{ABC}$ and Alice's secret bit may be either 0 or 1 with the same probability. On the other hand, if Bob's measuring result is $|1\rangle$, the GHZ-like state reduces to $(1/\sqrt{2})(|010\rangle + |111\rangle)_{ABC}$. Alice's secret bit could be either 0 or 1 with the same probability, too. Similarly, if Charlie's measuring result is $|0\rangle$, the GHZ-like state reduces to $(1/\sqrt{2})(|010\rangle + |100\rangle)_{ABC}$ and if it is $|1\rangle$, the GHZ-like state is $(1/\sqrt{2})(|001\rangle + |111\rangle)_{ABC}$. Both cases indicate that Alice's secret bit is either 0 or 1 with the same probability.

3.3 *Efficiency Analysis*

Alice prepares n GHZ-like states for secret sharing and $2n$ single photons for eavesdropping check. In total, $5n$ photons are used to distribute Alice's n-bit secret. Thus, the quantum bit efficiency of the proposed QSS scheme is $1/5$.

In the HBB QSS,[1] n GHZ states are used to distribute only $n/4$ secret bits (half of n GHZ states are wasted in bases selection and half of the remained ones are used to perform the eavesdropper checking.) Thus, the quantum bit efficiency of HBB QSS scheme is

$$\frac{1}{3n} \times \frac{n}{4} = \frac{1}{12}\,.$$

In Deng *et al.*'s QSS,[17] each GHZ state can share 2-bit secret, but only $n/4$ GHZ states are used to in sharing the secret. Thus, the quantum efficiency is

$$\frac{2}{3n} \times \frac{n}{4} = \frac{1}{6}\,.$$

Moreover, Deng's scheme needs additional devices to prevent the Trojan horse attack,[27] which could even worsen the quantum bit efficiency. The newly proposed QSS is free from Trojan horse attack.

4 Conclusions

This paper proposes a novel QSS scheme using the GHZ-like state. The quantum bit efficiency is better than the other GHZ-based QSS protocols with the same assumptions (i.e., the HBB QSS and Deng's QSS). The new QSS is free from Trojan horse attack[27] and the operations required for agents are very simple: the R-basis measuring, the exclusive-oring, and the complement. However, the proposed scheme for now works only for two agents. How to extend this idea to multiple participants will be an interesting future research.

References

[1] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59** (1999) 162.

[2] F.G. Deng, H.Y. Zhou, and G.L. Long, Phys. Lett. A **337** (2005) 329.

[3] Z.J. Zhang, Y. Li, and Z.X. Man, Phys. Rev. A **71** (2005) 044301.

[4] L.F. Han, Y.M. Liu, J. Liu, and Z.J. Zhang, Opt. Commun. **281** (2008) 2690.

[5] Tian-Yin Wang , Qiao-Yan Wen, Xiu-Bo Chen, Fen-Zhuo Guo, and Fu-Chen Zhu, Opt. Commun. **281** (2008) 6130.

[6] Ting Gao, FengLi Yan, and YouCheng Li, Sci. Chin. Ser. G-Phys. Mech. Astron. **52(8)** (2009) 1191.

[7] Anders Karlsson, Masato Koashi, and Nobuyuki Imoto, Phys. Lett. A **59** (1999) 162.

[8] Guo-Ping Guo and Guang-Can Guo, Phys. Lett. A **310** (2003) 247.

[9] Fu-Guo Deng, Gui-Lu Long, and Hong-Yu Zhou, Phys. Lett. A **340** (2005) 43.

[10] Zhan-Jun Zhang, Phys. Lett. A **342** (2005) 60.

[11] Zhan-Jun Zhang and Zhong-Xiao Man, Phys. Rev. A **72** (2005) 022303.

[12] Fu-Guo Deng, Xi-Han Li, and Hong-Yu Zhou, Phys. Lett. A **372** (2008) 1957.

[13] Ping Zhou, Xi-Han Li, Yu-Jie Liang, Fu-Guo Deng, and Hong-Yu Zhou, Physica A **381** (2007) 164.

[14] Song Lin, Fei Gao, Fen-Zhuo Guo, Qiao-Yan Wen, and Fu-Chen Zhu, Phys. Rev. A **76** (2007) 036301.

[15] J.H. Chen, K.C. Lee, and T. Hwang, Int. J. Mod. Phys. C **20** (2009) 1535.

[16] Li Xiao, Gui-Lu Long, Fu-Guo Deng, and Jian-Wei Pan, Phys. Rev. A **69** (2004) 052307.

[17] Fu-Guo Deng, Ping Zhou, Xi-Han Li, Chun-Yan Li, and Hong-Yu Zhou, Chin. Phys. Lett. **23** (2006) 1084.

[18] Liang Hao, JunLin Li, and GuiLu Long, Sci. Chin. Phys. Mech. & Astron. **53(3)** (2010) 491.

[19] Da-Zu Huang, Zhi-Gang Chen, and Ying Guo, Commun. Theor. Phys. **51** (2009) 221.

[20] Hao Yuan, Jun Song, Kui Hou, Xiao-Yuan Hu, Lian-Fang Han, and Shou-Hua Shi, Commun. Theor. Phys. **52** (2009) 50.

[21] Xiao-Feng Yin, Yi-Min Liu, Shi-Wei Shi, Wen Zhang, and Zhan-Jun Zhang, Commun. Theor. Phys. **52** (2009) 606.

[22] Y.H. Wang and H.S. Song, Chin. Sci. Bulletin **54(15)** (2009) 2599.

[23] Kan Yang, Liusheng Huang, Wei Yang, and Fang Song, Int. J. Theor. Phys. **48** (2009) 516.

[24] F.G. Deng and G.L. Long, Phys. Rev. A **68** (2003) 042315.

[25] G.L. Long and X.S. Liu, Phys. Rev. A **65** (2002) 032302.

[26] F.G. Deng, G.L. Long, and X.S. Liu, Phys. Rev. A **68** (2003) 042317.

[27] J.C. Boileau, R. Laflamme, M. Laforest, and C.R. Myers, Phys. Rev. Lett. **93** (2004) 220501.