Vol 17 No 2, February 2008
1674-1056/2008/17(02)/0419-05

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

Circular threshold quantum secret sharing*

Yang Yu-Guang(杨宇光)[a)b)] and Wen Qiao-Yan(温巧燕)[c)]

[a)] *College of Computer Science and Technology, Beijing University of Technology, Beijing* 100022, *China*
[b)] *State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing* 100049, *China*
[c)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 19 April 2007; revised manuscript received 28 May 2007)

This paper proposes a circular threshold quantum secret sharing (TQSS) scheme with polarized single photons. A polarized single photon sequence runs circularly among any t or more of n parties and any t or more of n parties can reconstruct the secret key when they collaborate. It shows that entanglement is not necessary for quantum secret sharing. Moreover, the theoretic efficiency is improved to approach 100% as the single photons carrying the secret key are deterministically forwarded among any t or more of n parties, and each photon can carry one bit of information without quantum storage. This protocol is feasible with current technology.

Keywords: quantum secret sharing, threshold quantum secret sharing, quantum secure direct communication

PACC: 0365, 4230

1. Introduction

Quantum secret sharing (QSS) is a quantum counterpart of classical secret sharing.[1] Now, there are many theoretical and experimental studies on QSS, for instance in Refs.[2–16]. QSS provides a secure way for sharing not only classical information[2−10] but also quantum secret.[11−16] Most existing QSS protocols use entangled states and the participants choose randomly one of two sets of measuring bases (MBs), for example the protocols proposed in Refs.[2–7, 11, 12]. The intrinsic efficiency of some protocols is nearly 50%, for example the protocols in Refs.[2, 3]. Some techniques from quantum key distribution (QKD) for improving the intrinsic efficiency[6,17,18] can be used for improving their efficiency in some QSS protocols. For example, the favoured-measuring-basis technique[17] and the measuring-basis-encrypted technique[18] are extended to the multiparty QSS schemes in Ref.[7]. In the measuring-basis-encrypted QSS scheme, a three-party control key is generated first among the three parties, and they are used repeatedly to control the use of the alternative MBs. In Ref.[19], Deng *et al* propose an efficient QSS scheme with Einstein–Podolsky–Rosen pairs which employs dense coding[20] and an order-rearrangement idea.[21]

Entanglement is not necessary in QSS. In Ref.[8], Guo *et al* propose a QSS protocol without entanglement based on a modified BB84 QKD protocol and the efficiency is improved to approach 100%, with the use of quantum data storage. In Ref.[9], based on a quantum secure direct communication (QSDC) protocol,[22] Zhang *et al* propose a (n, n)-threshold scheme of multiparty QSS of classical messages (QSSCM) using only single photons. In Ref.[23], Deng *et al* present QSS and secret splitting protocols with single photons running back and forth between the participating parties. In Ref.[24], Hsu *et al* propose three QSS protocols using product states. The first two protocols adopt the QKD protocol using product states.[25] In the third proposed protocol, three-level Bell states are exploited for qutrit preparation via nonlocality swapping. However, about half of the outcomes have to be dropped. In Ref.[26], Deng *et al* propose a circular QSS protocol, which is useful

*Project supported by the National Basic Research Program of China (973 Program) (Grant No 2007CB311100), the National High Technology Research and Development Program of China (Grant Nos 2006AA01Z419 and 20060101Z4015), the Major Research plan of the National Natural Science Foundation of China (Grant No 90604023), 2008 Scientific Research Common Program of Beijing Municipal Commission of Education, the Scientific Research Foundation for the Youth of Beijing University of Technology (Grant No 97007016200701), the National Research Foundation for the Doctoral Program of Higher Education of China (Grant No 20040013007), the National Laboratory for Modern Communications Science Foundation of China (Grant No 9140C1101010601), and the Doctor Scientific Research Activation Foundation of Beijing University of Technology (Grant No 52007016200702).

and efficient when one of the parties of secret sharing is remote to the others who are adjacent, especially the parties are more than three. However, Deng's protocol can't be used for m-out-of-n scheme in which any m parties can reconstruct the secret message when they collaborate.

In this paper, we propose a circular threshold QSS scheme with polarized single photons. Similar to the classical Shamir's secret sharing scheme,[1] the boss, Alice makes n shares, $S_1, \cdots, S_n$ of secret key K and each agent keeps a share secretly. If Alice wants to generate a private key $K_{\rm A}$ with her agents, she sends a single photon sequence each randomly in one of the following non-orthogonal quantum states $\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$ and makes a record of the quantum states. According to the secret shares and their private keys, the t agents sequentially perform the corresponding unitary operations on the single photon sequence and at last the last agent forwards it to Alice. According to her secret key K and her record of the measurement basis of the initial single photon sequence, Alice makes the corresponding measurement and obtains the $K_{\rm A} = \oplus_{i=1}^{t} K_{U_i}$ (K_{U_i} is the private key of the ith agent U_i) which the t agents can collaborate to obtain. The shared shares may be reusable if it can be judged that there is not an eavesdropper in line. We discuss that our protocol is feasible with current technology.

2. Circular threshold quantum secret sharing

2.1. Preparation phase

In this phase, the boss, Alice distributes the shared secrets to the agents.

(1) Alice chooses an original key

$$K = (b_1, b_2, \cdots, b_m), \tag{1}$$

where b_i is uniformly chosen from {0,1}.

(2) Alice then makes n shares, $S_1, \cdots, S_n$ of K similar to the classical Shamir's secret sharing scheme[1] over F_{2^N} as follows, where $N = m$. Alice shares n m-bit distinct, nonzero x_j's for $j = 1, \cdots, n$ with the agents using QSS schemes such as the ones in Refs.[8, 23]. Also she chooses (randomly and independently) secret a_i's for $i = 1, \cdots, t-1$ in F_{2^N}. She computes $S_j = f(\tilde{x}_j)$ for $j = 1, \cdots, n$ over F_{2^N}, where $\tilde{x}_j$ is a polynomial representation of x_j for $j = 1, \cdots, n$, where

$$f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \ldots + a_1 x + a_0 \bmod 2^N, \tag{2}$$

$f(0) = a_0 = \tilde{K}$ (here, $\tilde{K}$ is the polynomial representation of K).

(3) Alice sends $\tilde{S}_j$ to the agent U_j for each $j = 1, \cdots, n$, using QSDC schemes such as the ones in Refs.[22, 27], where $\tilde{S}_j$ is the binary representation of S_j.

2.2. Precomputation phase

In this phase, the agents compute the preliminary information for the following procedure of threshold QSS. The preliminary information depends on which subset of agents is chosen. Here, for simplicity of description, we assume that the t agents, $U_1, \cdots, U_t$, collaborate to do that.

(1) For each $j = 1, \cdots, t$, U_j calculate and secretly store the following value (given by the Lagrange interpolation formula)

$$K_j = S_j \prod_{1 \le l \le t, l \ne j} \frac{\tilde{x}_l}{\tilde{x}_l - \tilde{x}_j}, \tag{3}$$

over F_{2^N}. Let

$$K^{[j]} = \left(b_1^{[j]}, b_2^{[j]}, \cdots, b_m^{[j]}\right), \tag{4}$$

be the binary representation of K_j in F_{2^N}, where $b_i^{[j]}$ are in {0,1}. Although each secret value $S_j(K_j)$ is kept in each receiver U_j locally, these values satisfy the following equations globally:

$$\tilde{K} = \sum_{j=1}^{t} K_j, \tag{5}$$

over F_{2^N}. In the binary representation, Eq.(5) can be written as

$$K = \oplus_{j=1}^{t} K^{[j]}, \tag{6}$$

where $\oplus$ represents bitwise exclusive-OR. Note that even in the following collaborative procedure, $K_j(K^{[j]})$ is kept secret at U_j and the original key $\tilde{K}(K)$ is not recovered.

2.3. Circular threshold QSS scheme

The basic circular transmission idea of the circular-threshold QSS protocol with polarized single

photons is similar to Fig.1 in Ref.[26]. Suppose Alice wants to generate a private key $K_{\rm A}$ with her agents.

(1) The boss, Alice prepares a polarized single photon sequence whose length is $m+l$, using two sets of MB each into one of the above four states randomly

$$\{|0\rangle, |1\rangle, (|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}. \quad (7)$$

And she sends it to one agent, say U_1.

(2) After ensuring U_1 has received all the photons from Alice, Alice randomly chooses l sample photons and publicly announces the positions and the states of sample photons. Then U_1 measures these photons using the same bases as Alice announced. Comparing the results, U_1 can determine the error rate. If the error rate exceeds the threshold, the process is aborted. Otherwise, the remaining m-qubit quantum state is denoted with $|\phi^{[0]}\rangle$. Then U_1 randomly generates a private key $K_{U_1} = \left(a_1^{[1]}, a_2^{[1]}, ..., a_m^{[1]}\right)$ and applies $W^{[1]}$ to $|\phi^{[0]}\rangle$. $W^{[j]}$ is defined in Eq.(8). Suppose

$$W^{[j]} = U_1^{[j]} V_1^{[j]} \otimes U_2^{[j]} V_2^{[j]} \otimes \cdots \otimes U_m^{[j]} V_m^{[j]}, \quad (8)$$

where

$$U_i^{[j]} = U\left(a_i^{[j]}\right), V_i^{[j]} = V\left(b_i^{[j]}\right), \quad (9)$$

$$U(1) = \mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|,$$

$$U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|,$$

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

$$V(0) = |0\rangle\langle 0| + |1\rangle\langle 1|. \quad (10)$$

U_1 then obtains $|\phi^{[1]}\rangle$ by the unitary transformation

$$W^{[j]} : |\phi^{[j-1]}\rangle \to |\phi^{[j]}\rangle. \quad (11)$$

The single photons encoding quantum state $|\phi^{[1]}\rangle$ form M sequence. To check eavesdropping, U_1 prepares some sample photons randomly in one of the above four non-orthogonal states and inserts these single photons randomly into the M sequence. U_1 makes a record of the insertion positions of the sample photons for eavesdropping check. The sample photons for eavesdropping check form C sequence.

U_1 sends all the photons to U_2.

(3) After ensuring $U_j (j = 2, \cdots, t)$ has received all the photons from U_{j-1}, U_{j-1} publicly announces the positions and the states of sample photons. Then U_j measures these photons using the same bases as U_{j-1} announced. Comparing the results, U_j can determine the error rate. If the error rate exceeds the threshold, the process is aborted. Otherwise, the remaining m-qubit quantum state is denoted with $|\phi^{[j-1]}\rangle$. Then U_j randomly generates a private key $K_{U_j} = \left(a_1^{[j]}, a_2^{[j]}, ..., a_m^{[j]}\right)$ and applies $W^{[j]}$ to $|\phi^{[j-1]}\rangle$ and obtains $|\phi^{[j]}\rangle$.

The single photons encoding quantum state $|\phi^{[j]}\rangle$ form M sequence. To check eavesdropping, U_j prepares some sample photons randomly in one of the above four non-orthogonal states and inserts these single photons randomly into the M sequence. U_j makes a record of the insertion positions of the sample photons for eavesdropping check. The sample photons for eavesdropping check form C sequence.

If $j < t$, U_j sends all the photons to U_{j+1} and step (3) repeats. Otherwise U_t forward all the photons to Alice.

(4) After knowing that Alice has received all the photons from U_t, U_t publicly announces the positions and the states of sample photons. Then Alice measures these photons using the same bases as U_t announced. Comparing the results, Alice can determine the error rate. If the error rate exceeds the threshold, the process is aborted. Otherwise, according to the initial quantum state and her private key K, Alice applies the corresponding unitary operations to $|\phi^{[t]}\rangle$ and obtains the key $K_{\rm A} = \left(\oplus_{j=1}^{t} a_1^{[j]}, \oplus_{j=1}^{t} a_2^{[j]}, ..., \oplus_{j=1}^{t} a_m^{[j]}\right)$.

3. Security analysis

Now we will analyse some possible cases: (1) intercept-resend attack; (2) Trojan horse attack and EPR-pair attack; (3) $(t-1)$-party cheating attack.

(1) intercept-resend attack

The quantum state sent by U_j is multi-qubit tensor product. Each qubit is randomly in one of two conjugated bases. Without the information of $b_i^{[j]}$, the eavesdropper can't perform the correct unitary operation on each qubit. If he takes an intercept-resend attack, the probability of not being detected is $(1/4)^m$.

In addition, because of the randomness of the insertion positions and quantum states of the sample photons, Eve cannot be detected with a probability of $(1/4)^n$ only by guessing (if the number of the sample photons is n).

(2) Trojan horse attack and EPR-pair attack

By inserting some sample photons randomly into the M sequence, the protocol can resist the Trojan

horse attack[28,29] and EPR-pair attack.[30]

(3) $(t-1)$-party cheating attack

Suppose a dishonest member U_i aims at finding out another member U_j's share and then to forge the share with other $t-2$ members. U_i prepares a fake signal and sends it to U_j. Then from the fake signal operated by U_j, U_i tries to gain U_j's share.

Without loss of generality, we assume that U_j does one of four kinds of operations on every qubit with equal probability and that every single-qubit operation is independent. So it is sufficient to consider U_i's eavesdropping on one qubit.

U_i's fake signal can be presented as

$$|\theta\rangle = |0\rangle(a|0\rangle + b|1\rangle) + |1\rangle(c|0\rangle + d|1\rangle),$$

where $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. For simplicity, we regard every probability amplitude as a real number, but the security proof is fitted for plural number. U_i sends the first qubit to U_j and keeps the second one.

U_j encodes his share by applying one of four kinds of operations with equal probability. The state can be expressed by

$$\begin{aligned} w = & \frac{1}{4}|\theta\rangle\langle\theta| + \frac{1}{4}(I\otimes I)|\theta\rangle\langle\theta|(U^+\otimes I) \\ & + \frac{1}{4}(U\otimes I)|\theta\rangle\langle\theta|(U^+\otimes I) \\ & + \frac{1}{4}(V\otimes I)|\theta\rangle\langle\theta|(I\otimes V^+) \\ & + \frac{1}{4}(UV\otimes I)|\theta\rangle\langle\theta|(V^+U^+\otimes I). \end{aligned} \tag{12}$$

The mutual information between U_i and U_j that can be extracted from this state is given by the von-Neumann entropy, $I(U_i, U_j) \leq S(\mathrm{tr_e}(w))$. In order to calculate the von-Neumann entropy, we need to calculate the eigenvalues of $\mathrm{tr_e}(w)$, which are the roots of the characteristic polynomial $\det(\mathrm{tr_e}(w) - \lambda I)$. We can get the two roots λ_1 and λ_2, respectively

$$\lambda_1 = \lambda_2 = \frac{1}{2}(1 + 2ab + 2cd). \tag{13}$$

So we have

$$I(U_i, U_j) \leq -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2. \tag{14}$$

For $\lambda_1 = \lambda_2 = \frac{1}{2}$, $I(U_i, U_j)$ reaches the maximal value 1 bit. So U_i can eavesdrop 1 bit of 2 bit operation information on one qubit.

However, $I(U_i, U_j)$ can also reach the maximal value when U_i prepares the legal qubit, namely the options of the values of a, b, c, d meet the condition $ab + cd = 0$. Due to the large number of the options of a, b, c, d meeting the above condition, the values of a, b, c, d are not set forth here. So U_i can not gain more information by sending a fake signal than by sending a legal signal. U_i's eavesdropping will introduce errors and cause the protocol to fail.

4. Conclusion

In this paper, we propose a circular threshold QSS scheme with polarized single photons. Different from the protocol in Ref.[26], in which Deng *et al* propose a circular QSS protocol used for generating a random key between all the agents and the boss, we propose a t-out-of-n scheme in which any t or more of n agents can reconstruct the secret key when they collaborate. A polarized single photon sequence runs circularly among any t or more of n agents. It is shown that entanglement is not necessary for QSS. Moreover, the theoretic efficiency is improved to approach 100%, and each photon can carry one bit of information without quantum storage. The shared shares may be reusable if it can be judged there is not an eavesdropper in line. Our protocol is feasible with current technology.

References

[1] Shamir A 1979 *Commun. ACM* **22**(11) 612

[2] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[3] Karlsson A, Koashi M and Imoto N 1999 *Phys. Rev.* A **59** 162

[4] Bandyopadhyay S 2000 *Phys. Rev.* A **62** 012308

[5] Karimipour V, Bahraminasab A and Bagherinezhad S 2002 *Phys. Rev.* A **65** 042320

[6] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *European Physical Journal* D **39** 459

[7] Xiao L, Long G L, Deng F G and Pan J W 2004 *Phys. Rev.* A **69** 052307

[8] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[9] Zhang Z J and Man Z X 2005 *Phys. Rev.* A **72** 022303

[10] Chen P, Deng F G and Long G L 2006 *Chin. Phys.* **15** 2228

[11] Yang Y G, Wen Q Y and Zhu F C 2006 *Acta Phys Sin.* **55** 3255 (in Chinese)

[12] Li Y M, Zhang K S and Peng K C 2004 *Phys. Lett.* A **324** 420

[13] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2005 *Phys. Rev.* A **72** 044301

[14] Deng F G, Li C Y, Li Y S, Zhou H Y and Wang Y 2005 *Phys. Rev.* A **72** 022338
[15] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304
[16] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Phys. Lett.* A **354** 190
[17] Lo H K, Chau H F and Ardehali M 2005 *J. Cryptology* **18** 133
[18] Hwang W Y, Koh I G and Han Y D 1998 *Phys. Lett.* A **244** 489
[19] Deng F G, Long G L and Zhou H Y 2005 *Phys. Lett.* A **340** 43
[20] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[21] Deng F G and Long G L 2003 *Phys. Rev.* A **68** 042315
[22] Deng F G AND Long G L 2004 *Phys. Rev.* A **69** 052319
[23] Deng F G, Zhou H Y and Long G L 2005 *Phys. Lett.* A **337** 329
[24] Hsu L Y and Li C M 2005 *Phys. Rev.* A **71** 022321
[25] Guo G P, Li C F, Shi B S, Li Jian and Guo G C 2001 *Phys. Rev.* A **64** 042301
[26] Deng F G, Zhou H Y and Long G L 2006 *Journal of Physics A-Mathematical and General* **39** 14089
[27] Cai Q Y and Li B W 2004 *Chin. Phys. Lett.* **21** 601
[28] Cai Q Y 2006 *Phys. Lett.* A **351** 23
[29] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302
[30] Qin S J, Gao F, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **357** 101