Science in China Series G: Physics, Mechanics & Astronomy

© 2008 SCIENCE IN CHINA PRESS

Springer-Verlag

www.scichina.com
phys.scichina.com
www.springerlink.com

Threshold quantum secure direct communication without entanglement

YANG YuGuang[1,3†] & WEN QiaoYan[2]

[1] College of Computer Science and Technology, Beijing University of Technology, Beijing 100022, China;
[2] School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
[3] State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing 100049, China

For the first time, a threshold quantum secure direct communication (TQSDC) scheme is presented. Similar to the classical Shamir's secret sharing scheme, the sender makes *n* shares, S_1, ···, S_n of secret key *K* and each receiver keeps a share secretly. If the sender wants to send a secret message *M* to the receivers, he encodes the information of *K* and *M* on a single photon sequence and sends it to one of the receivers. According to the secret shares, the *t* receivers sequentially perform the corresponding unitary operations on the single photon sequence and obtain the secret message *M*. The shared shares may be reusable if it can be judged that there is no eavesdropper in line. We discuss that our protocol is feasible with current technology.

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

1 Introduction

One of the most remarkable applications of quantum mechanics in quantum information is quantum cryptography. Quantum cryptography exploits the principles of quantum mechanics to enable provably secure distribution of private information, including generating a key[1−5], secret sharing[6−10] and so on.

Recently, a novel branch of quantum communication, quantum secure direct communication (QSDC), was proposed and actively pursued by some groups[11−25]. With QSDC, the communicating parties, Bob and Carol can exchange the secret message directly without generating a pri-

Received October 26, 2006; accepted February 13, 2007
doi: 10.1007/s11433-008-0028-3

†Corresponding author (email: yangyang7357@bjut.edu.cn)

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), the 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 (Grants No. 9140C1101010601), the Doctor Scientific Research Activation Foundation of Beijing University of Technology (No. 52007016200702), and the Open Foundation of State Key Laboratory of Information Security (Graduate School of the Chinese Academy of Sciences)

vate key in advance and then encrypting the message, which is different from quantum key distribution (QKD). In 2002, Beige et al.[11] presented a deterministic quantum secure communication protocol in which the message could be read out after the transmission of an additional classical information for each qubit[12,17,23], similar to a QKD scheme in which each bit of key can represent one bit of secret message with an additional classical information, i.e., retaining or flipping the bit value in the key according to the secret message[23]. In 2002, Boström and Felbinger[12] proposed a ping-pong QSDC following some ideas in quantum dense coding with an EPR pair. The authors had claimed that it was secure for generating a private key and quasi-secure for direct communication as it would leak some of the secret message in a noisy channel. Wójcik and Zhang et al. pointed out that the ping-pong protocol was insecure for direct communication if there were losses in a practical quantum channel[13,14]. Also, the ping-pong protocol can be attacked without eavesdropping[15]. Cai and Li[16] modified the ping-pong protocol for transmitting the secret message directly by replacing the entangled photons with single photons in the mixed state, similar to the Bennett 1992 QKD[3] protocol, and inherited its nature of insecurity[17] as it was vulnerable to the opaque attack which is discussed in ref. [3]. They[18] also showed that the capacity of the ping-pong protocol could be doubled by introducing two additional unitary operations. However, it is not unconditionally secure as the analysis of eavesdropping check depends on the feature of statistics for which a lot of samples should be chosen randomly and measured. Wang et al.[19] introduced a QSDC protocol with high-dimensional quantum superdense coding. Refs. [20,21] introduced the idea of order-rearrangement into quantum secure direct communication. Recently, Lucamarini et al.[22] introduced a QSDC protocol for both communicating directly and creating a private key with some ideas in refs. [4,17]. It is secure for QKD, the same as ref. [4], but it is just quasi-secure for direct communication, similar to the QSDC protocol in ref. [18]. Deng et al. put forward a two-step QSDC protocol[23] with EPR pairs transmitted in block and another one based on a sequence of polarized single photons[17].

In most of the above schemes, entanglement is necessary. However, it is not easy for them to be realized experimentally, since the efficiency of preparing even tripartite or four-partite entangled states[26,27] is very low.

In this paper, for the first time, we present a t-out-of-n TQSDC scheme. Similar to the classical Shamir's secret sharing scheme, the sender makes n shares, $S_1,\cdots,S_n$ of secret key K and each receiver keeps a share secretly. If the sender wants to send a secret message M to the receivers, he encodes the information of K and M on a single photon sequence and sends it to one of the receivers. According to the secret shares, the t receivers sequentially perform the corresponding unitary operations on the single photon sequence and obtain the secret message M. We discuss that our protocol is feasible with current technology.

It has three main features: (1) there is no need to prepare any entanglement; (2) the shared shares are classical; (3) the shared shares are reusable if it can be judged that there is no eavesdropper in line.

2 TQSDC scheme

2.1 Preparation phase

In this phase, the sender distributes the shared secrets to the receivers.

(1) A sender chooses an original key

$$K=(a_1,b_1,a_2,b_2,\cdots,a_m,b_m), \tag{1}$$

where a_i,b_i are uniformly chosen from {0,1}.

(2) The sender then makes n shares, $S_1,\cdots,S_n$ of K similar to the classical Shamir's secret sharing scheme[28] over F_{2^N} as follows, where N = 2 m. The sender shares n 2m-bit distinct, non-zero x_j's for $j=1, \cdots, n$ with the receivers using quantum secret sharing schemes such as the ones in refs. [8,9]. Also he chooses (randomly and independently) secret a_i's for $i=1, \cdots, t-1$ in F_{2^N}. He 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

$$f(x)=a_{t-1}x^{t-1}+a_{t-2}x^{t-2}+\cdots+a_1x+a_0 \bmod 2^N, \tag{2}$$

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

(3) The sender sends $\tilde{S}_j$ to the receiver R_j for each $j=1, \cdots, n$, using quantum secure direct communication schemes such as the ones in refs. [16,17], where $\tilde{S}_j$ is the binary representation of S_j.

2.2 Precomputation phase

In this phase, the receivers compute the preliminary information for the following procedures of collaborating to recover the secret message. The preliminary information depends on which subset of receivers is chosen to collaborate. Here, for simplicity of description, we assume that the t receivers, $R_1, \cdots, R_t$, collaborate to do that.

(1) For each $j=1, \cdots, t$, R_j calculates and secretly stores the following value (given by the Lagrange interpolation formula):

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

over F_{2^N}. Let

$$K^{[j]}=(a_1^{[j]},\ b_1^{[j]},\ a_2^{[j]},\ b_2^{[j]},\ \cdots,\ a_m^{[j]},\ b_m^{[j]}) \tag{4}$$

be the binary representation of K_j in F_{2^N}, where $a_i^{[j]},\ b_i^{[j]}$ are in {0,1}. Although each secret value $S_j(K_j)$ is kept in each receiver R_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 R_j and the original key $\tilde{K}$ (K) is not recovered.

2.3 Secret message distribution phase

Suppose that the sender wants to send a secret message M to the receivers.

$$M=(c_1,c_2,\cdots,c_m), \tag{7}$$

where c_i is in {0,1}, $i=1, \cdots, m$.

(1)The sender generates a quantum state for the secret message M

$$|\phi\rangle=\left|\psi_{c_1\oplus a_1,b_1}\right\rangle\otimes\left|\psi_{c_2\oplus a_2,b_2}\right\rangle\otimes\cdots\otimes\left|\psi_{c_m\oplus a_m,b_m}\right\rangle, \tag{8}$$

where for each $i=1, \cdots, m$, a qubit $\left|\psi_{c_i\oplus a_i,b_i}\right\rangle$ is one of the following states

$$\begin{aligned}&\left|\psi_{0,0}\right\rangle=|0\rangle,\\&\left|\psi_{1,0}\right\rangle=|1\rangle,\\&\left|\psi_{0,1}\right\rangle=(|0\rangle+|1\rangle)/\sqrt{2},\\&\left|\psi_{1,1}\right\rangle=(|0\rangle-|1\rangle)/\sqrt{2}.\end{aligned} \tag{9}$$

The value of b_i determines the measurement basis. If b_i is 0, then $c_i\oplus a_i$ is encoded in the Z basis { $|0\rangle$, $|1\rangle$ }; if b_i is 1, then $c_i\oplus a_i$ is encoded in the X basis

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

From eq. (6),

$$(c_1\oplus a_1^{[1]}\oplus\cdots\oplus a_1^{[t]},\cdots,c_m\oplus a_m^{[1]}\oplus\cdots\oplus a_m^{[t]})=(c_1\oplus a_1,\cdots,c_m\oplus a_m) \tag{10}$$

is encoded using the bases

$$(b_1^{[1]}\oplus\cdots\oplus b_1^{[t]},\cdots,b_m^{[1]}\oplus\cdots\oplus b_m^{[t]})=(b_1,\cdots,b_m). \tag{11}$$

(2) The sender sends the quantum state $|\phi\rangle$ to one of the receivers. Here, for simplicity of description, we assume that the receiver, R_1, receives the quantum state $|\phi\rangle$. Whoever receives the quantum state $|\phi\rangle$ is unimportant, since for each R_j, $j=1, \cdots, t$, the quantum state $|\phi\rangle$ is unknown and he cannot get the information of $|\phi\rangle$ without disturbing it since quantum no-cloning theorem ensures its security.

2.4 Secret message recovery phase

In this phase, the t receivers collaborate to recover the secret message. Here, we assume the t receivers are $R_1, \cdots, R_t$. For each $j=1, \cdots, t$, R_j has calculated $K^{[j]}=(a_1^{[j]}, b_1^{[j]}, a_2^{[j]}, b_2^{[j]}, \cdots, a_m^{[j]}, b_m^{[j]})$ in the precomputation phase. Let $\left|\phi^{[0]}\right\rangle=|\phi\rangle$, and R_0 be the sender.

(1) For each $j=1, \cdots, t$, R_j receives the $\left|\phi^{[j-1]}\right\rangle$ from R_{j-1}. To check Trojan horse attack[25−27], he measures the state $\left|\phi^{[j-1]}\right\rangle$ with some photon number splitters (PNSs: 50/50) and some detectors. The measurements will at least have two outcomes if the quantum signal is a multiphoton one. Figure 1[26] is an example of a four-photon quantum signal as the fake signal.

If the quantum signal is a single one, then he applies $W^{[j]}$ to $\left|\phi^{[j-1]}\right\rangle$. $W^{[j]}$ is defined in eq. (12):

$$W^{[j]}=U_1^{[j]}V_1^{[j]}\otimes U_2^{[j]}V_2^{[j]}\otimes\cdots\otimes U_m^{[j]}V_m^{[j]}, \tag{12}$$

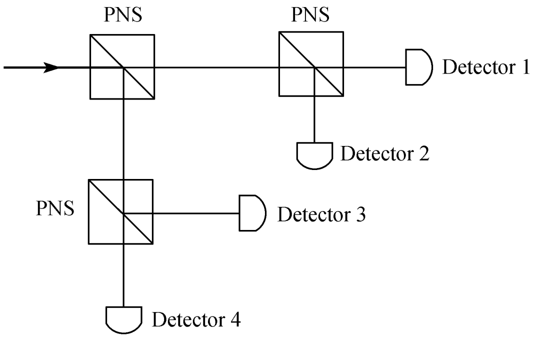

Figure 1 The measurements with the photon number splitters (PNS: 50/50) in the case that there are four photons in each signal[26].

where

$$U_i^{[j]} = U(a_i^{[j]}),\ V_i^{[j]} = V(b_i^{[j]}), \tag{13}$$

$$\begin{aligned} &U(1) = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|, \\ &U(0) = |0\rangle\langle 0| + |1\rangle\langle 1|, \\ &V(1) = H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|, \\ &V(0) = |0\rangle\langle 0|| + |1\rangle\langle 1|. \end{aligned} \tag{14}$$

R_j then obtains $\left|\phi^{[j]}\right\rangle$ by the unitary transformation

$$W^{[j]} : \left|\phi^{[j-1]}\right\rangle \longrightarrow \left|\phi^{[j]}\right\rangle. \tag{15}$$

If $j < t$, R_j sends $\left|\phi^{[j]}\right\rangle$ to R_{j+1}. Otherwise, he proceeds to step (2).

(2) R_t measures $\left|\phi^{[t]}\right\rangle$ on the basis of $(0, 0, \cdots, 0)$ and gets the secret message $(c_1, c_2, \cdots, c_m)$.

(3) To check whether any dishonest receiver or eavesdropper is in line, the sender should insert some decoy particles S_{e1} in the sequence before it is sent. The number of the particles in S_{e1} is not required to be very large, but enough for the statistical analysis. As any eavesdropper or dishonest receiver does not know the information about *K*, he cannot decrypt $|\phi\rangle$. Only by comparing the results of measurement of S_{e1} with the ones prepared by him can the sender judge whether any dishonest receiver or eavesdropper exists. If the error rate is lower than the threshold ε_{th}, the sender can judge that no dishonest receiver or eavesdropper is in line and the receivers can recover the secret message *M* with error correction methods. Otherwise, they start from the beginning.

3 Security analysis

Now we will analyze some possible cases: (1) intercept-resend attack; (2) individual cheating attack; (3) *t*-1-party cheating attack.

(1) Intercept-resend attack

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

(2) Individual cheating attack

The TTP sends the quantum state $|\phi\rangle$ to R_1. Whoever receives the quantum state $|\phi\rangle$ is unimportant, since for each R_j, $j=1, \cdots, t$, the quantum state $|\phi\rangle$ is unknown and he cannot get the information of $|\phi\rangle$ without disturbing it since quantum no-cloning theorem ensures its security. Before R_1 receives the quantum state sent by the TTP, Eve can take Trojan horse attack[29−31], i.e., he intercepts it and sends another multi-photon quantum state to R_1. Eve expects to obtain R_1's secret operation information by measuring the quantum state operated by R_1 with some photon number splitters (PNSs: 50/50) and some detectors. However his Trojan horse attack will be detected by R_1 in step (1) of secret message recovery phase. It is the similar case with the cheater being R_j $j=2, \cdots, t$.

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

Suppose a dishonest receiver R_i aims to find out another receiver R_j's share and then to recover the secret message with other t-2 receivers. R_i prepares a fake signal and sends it to R_j. Then from the fake signal operated by R_j, R_i tries to gain R_j's share.

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

R_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. R_i sends the first qubit to R_j and keeps the second one.

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

$$\begin{aligned} w = {} & \frac{1}{4}|\theta\rangle\langle\theta| + \frac{1}{4}(U \otimes I)|\theta\rangle\langle\theta|(U^+ \otimes I) \\ & + \frac{1}{4}(V \otimes I)|\theta\rangle\langle\theta|(V^+ \otimes I) + \frac{1}{4}(UV \otimes I)|\theta\rangle\langle\theta|(V^+U^+ \otimes I). \end{aligned} \tag{16}$$

The mutual information between R_i and R_j that can be extracted from this state is given by the von-Neumann entropy, $I(R_i, R_j) \leqslant S(Tr_e(w))$. In order to calculate the von-Neumann entropy, we need to calculate the eigenvalues of $Tr_e(w)$, which are the roots of the characteristic polynomial $\det(Tr_e(w) - \lambda I)$.

$$\lambda_{1,2} = \frac{1}{2}(1 + 2ab + 2cd). \tag{17}$$

So we have

$$I(R_i, R_j) \leqslant -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2. \tag{18}$$

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

However, $I(R_i, R_j)$ can also reach the maximal value when R_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 R_i cannot gain more information by sending a fake signal than by sending a legal signal. R_i's eavesdropping will introduce errors and be detected in step (3) of secret message recovery phase.

4 Conclusion

In this paper, for the first time, we present a *t*-out-of-*n* TQSDC scheme. Similar to the classical Shamir's secret sharing scheme, the sender makes *n* shares, $S_1, \cdots, S_n$ of secret key *K* and each receiver keeps a share secretly. If the sender wants to send a secret message *M* to the receivers, he encodes the information of *K* and *M* on a single photon sequence and sends it to one of the receivers. According to the secret shares, the *t* receivers sequentially perform the corresponding unitary operations on the single photon sequence and obtain the secret message *M*. We discuss that our protocol is feasible with current technology.

It has three main features: (1) there is no need to prepare any entanglement; (2) the shared shares are classical; (3) the shared shares are reusable if it can be judged that there is no eavesdropper in line.

1 Bennett C H, Brassard G. Quantum cryptography: Public-key distribution and coin tossing, Proc IEEE Int Conf on Computers, Systems and Signal Processing, Bangalore, India. New York: IEEE, 1984. 175－179

2 Ekert A. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661－664

3 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121－3124

4 Deng F G, Long G L. Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A, 2004, 70: 012311-1－4

5 Deng F G, Long G L. Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68: 042315-1－5

6 Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A, 1999, 59: 1829－1834

7 Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59: 162－168

8 Deng F G, Zhou H Y, Long G L. Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys Lett A, 2005, 337(4-6): 329－334

9 Guo G P, Guo G C. Quantum secret sharing without entanglement. Phys Lett A, 2003, 310(4): 247－251

10 Xiao L, Long G L, Deng F G, et al. Efficient multiparty quantum secret sharing schemes. Phys Rev A, 2004, 69: 052307-1－5

11 Beige A, Englert B G, Kurtsiefer C et al. Secure communication with single-photon two-qubit states**.** J Phys A: Math Gen, 2002, 35(28): L407-L413

12 Boström K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902-1－4

13 Wójcik A. Eavesdropping on the "Ping-Pong" quantum communication protocol. Phys Rev Lett, 2003, 90: 157901-1－4

14 Zhang Z J, Man Z X, Li Y. Improving Wójcik's eavesdropping attack on the ping–pong protocol. Phys Lett A, 2004, 333(1-2):

46－50

15 Cai Q Y. The "Ping-Pong" protocol can be attacked without eavesdropping. Phys Rev Lett, 2003, 91: 109801-1－1

16 Cai Q Y, Li B W. Deterministic secure communication without using entanglement. Chin Phys Lett, 2004, 21: 601－603

17 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319-1－4

18 Cai Q Y, Li B W. Improving the capacity of the Boström-Felbinger protocol. Phys Rev A, 2004, 69: 054301-1－3

19 Wang C, Deng FG, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305-1－4

20 Zhu A D, Xia Y, Fan Q B, et al. Secure direct communication based on secret transmitting order of particles. Phys Rev A, 2006, 73: 022338-1－4

21 Wang J, Zhang Q, Tang C J. Quantum secure direct communication based on order rearrangement of single photons. Phys Lett A, 2006, 358(4): 256－258

22 Lucamarini M, Mancini S. Secure deterministic communication without entanglement. Phys Rev Lett, 2005, 94: 140501-1－4

23 Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317-1－4

24 Cao H J, Song H S. Quantum secure direct communication with W State. Chin Phys Lett, 2006, 23: 290－292

25 Li X H, Zhou P, Liang Y-J, et al. Quantum secure direct communication network with two-step protocol. Chin Phys Lett, 2006, 23: 1080－1083

26 Bouwmeester D, Pan J W, Daniell M, et al. Observation of three-photon Greenberger-Horne-Zeilinger entanglement. Phys Rev Lett, 1999, 82: 1345－1349

27 Pan J W, Daniell M, Gasparoni S, et al. Experimental demonstration of four-photon entanglement and high-fidelity teleportation. Phys Rev Lett, 2001, 86: 4435－4438

28 Shamir A. How to share a secret. Commun ACM, 1979, 22(11): 612－613

29 Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A, 2006, 351(1-2): 23－25

30 Deng F G, Li X H, Zhou H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A, 2005, 72: 044302－044305

31 Qin S J, Gao F, Wen Q Y, et al. Improving the security of multiparty quantum secret sharing against an attack with a fake signal. Phys Lett A, 2006, 357(2): 101－103