Optics Communications 281 (2008) 6130–6134

Contents lists available at ScienceDirect

Optics Communications

journal homepage: www.elsevier.com/locate/optcom

An efficient and secure multiparty quantum secret sharing scheme based on single photons

Tian-yin Wang [a,b,*], Qiao-yan Wen [a], Xiu-bo Chen [a], Fen-zhuo Guo [a], Fu-chen Zhu [c]

[a] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Xitucheng Road 10#, Beijing 100876, China
[b] School of Mathematical Science, Luoyang Normal University, Luoyang 471022, China
[c] National Laboratory for Modern Communications, P.O. Box 810, Chengdu 610041, China

ARTICLE INFO

Article history:
Received 18 May 2008
Received in revised form 5 September 2008
Accepted 9 September 2008

PACS:
03.67.Hk
03.67.Dd
03.65.Ud

Keywords:
Quantum secret sharing
Single photons
Quantum teleportation

ABSTRACT

A scheme of multiparty quantum secret sharing of classical messages (QSSCM) is proposed based on single photons and local unitary operations. In this scheme, eavesdropping checks are performed only twice, and one photon can generate one bit of classical secret message except those chosen for eavesdropping check; in addition, only the sender and one of the agents are required to store photons. Thus, this scheme is more practical and efficient.

1. Introduction

The principles of quantum mechanics supplied many interesting applications in the field of quantum information in the last decade. Quantum secret sharing (QSS) is an important branch of quantum information, which allows a secret to be shared among many participants in such a way that only the authorized groups can reconstruct it [1]. QSS is an useful tool in the cryptographic applications and it is likely to play a key role in protecting secret quantum information, e.g., in secure operations of distributed quantum computation, sharing difficult-to-construct ancilla states and joint sharing of quantum money, and so on [2]. Classical secret sharing schemes are designed based on certain unproven computational assumptions such as the infeasibility of factoring large integers and solving discrete logarithm. Unfortunately, quantum algorithms are capable of factoring large integers and solving discrete logarithm [3]. Fortunately, in contrast to classical secret sharing, the security of QSS relies on quantum-mechanical law rather than on computational complexity, so QSS is secure even if the attackers have unlimited computational resources; in addition, the information splitting of a secret and the information distribution in QSS is realized by local measurements and unitary operations on distributed quantum states, so QSS allows to distribute the shares securely in the presence of eavesdropping; moreover, QSS can supplies a secure way for sharing not only a classical message (i.e., bit) but also a quantum state. Therefore, since Hillery et al. first proposed a QSS scheme using Greenberger-Horne-Zeilinger states in 1999 [4], a lot of QSS schemes [1,2,5–21] have been proposed in both theoretical and experimental aspects. All these schemes [1,2,4–21] can be divided into two kinds, one only deals with the QSSCM [1,5,9–12,14,16–21], or only deals with the QSS of quantum information [2,6–8,13,15] where the secret is an arbitrary quantum state, and the other studies both [4], that is, deals with QSS of classical messages and QSS of a quantum state simultaneously. In all these schemes [1,2,4–21] dealing with the QSS, entangled states are used.

In fact, entanglement is necessary in QSS of quantum states, but it is not necessary in QSSCM, and single photons are ideal source for quantum communication, compared with those QSSCM schemes using entangled state, the QSSCM schemes without entanglement are more practical within the present technology, so Guo and Guo first proposed a QSSCM scheme with multi-particle product states in Ref. [22] and then Deng et al. presented a scheme for bidirec-

* Corresponding author. Address: State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Xitucheng Road 10#, Beijing 100876, China.
E-mail address: wangtianyin@yahoo.cn (T.-y. Wang).

0030-4018/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.optcom.2008.09.026

tional quantum secret sharing and secret splitting with polarized single photons in Ref. [23]. These two QSSCM schemes are secure, but eavesdropping check need to be performed between the sender and any agent, and n photons can generate only one bit of classical secret in Refs. [22,23], here n is the number of the agents. Thus, when n is large, many photons would be wasted in these two QSSCM schemes. Yan and Gao proposed a scheme for quantum secret sharing between multiparty and multiparty without entanglement in Ref. [24] and Schmid et al. gave an experimental single qubit quantum secret sharing in Ref. [25], but the Refs. [26–28] have shown these two QSSCM schemes do not reach the security level of QSSCM. Based on the quantum secure direct communication (QSDC) protocols [29,30], Zhang et al. also proposed a multiparty QSSCM scheme using single photons in Ref. [31]. In the scheme, some special unitary operations (e.g., four Pauli operations) are used to realize the sharing controls. Unfortunately, the scheme is vulnerable to some attacks [32–34]. In order to overcome the flaws in Ref. [31], Han et al. use random phase shift operations instead of some special discrete unitary operations to realize the sharing controls and gave an improvement QSSCM scheme [35]. However, with the development of quantum cryptanalysis, Qin et al. [36] proposed a new attack with quantum teleportation, and any dishonest agent can recover the sender's secret message and introduce no error with this teleportation attack in Han et al.'s scheme.

Therefore, how to design a practical, secure and efficient multiparty QSSCM scheme based on single photons is a urgent and significance problem to be solved. In this paper, we propose a new multiparty QSSCM scheme using single photons and local unitary operations. In this scheme, only two eavesdropping checks are required, and one photon can generate one bit of classical secret message except those chosen for eavesdropping check; in addition, only the sender and one of the agents need to store photons. Thus, this scheme is more practical and efficient. Most important of all, this scheme can resist all the attacks in Refs. [26–28,32–34,36].

Now let us turn to our multiparty QSSCM scheme. For convenience, let us first describe a four-party QSSCM scheme in detail. Suppose Alice wants to send a secret message to three agents, Bob, Charlie and Dick. However, Alice requires the three agents can infer the secret messages only by their mutual assistance. This four-party QSSCM scheme includes the following five steps.

(1) Firstly, according to the bit length of her secret message, Alice prepares the product state of single photons $\otimes_{i=1}^{N}|0\rangle_i$, here N is the bit length of Alice's secret message and $|0\rangle$, $|1\rangle$ denote the horizontal and vertical polarization modes of photons hereafter, respectively. Then, she prepares K sample photons $\otimes_{j=1}^{K}|S_j\rangle$ to detect eavesdropping in the following step (3), here $|S_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\} (j = 1, 2, \ldots, K)$ and $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Finally, she inserts randomly the K sample photons $\otimes_{j=1}^{K}|S_j\rangle$ into the N single photons $\otimes_{i=1}^{N}|0\rangle_i$ and sends all the photons to Bob. Note that any one does not know the initial states and positions of the K sample photons $\otimes_{j=1}^{K}|S_j\rangle$ except Alice.

(2) When Bob receives the photons $\otimes_{i=1}^{N}|0\rangle_i$ and $\otimes_{j=1}^{K}|S_j\rangle$, on each photon, Bob chooses a local unitary operation from I, σ_x, $i\sigma_y$, σ_z and H with probability 12.5%, 12.5%, 12.5%, 12.5% and 50%, respectively, and performs this unitary operation on it. Here $I = (|0\rangle\langle 0| + |1\rangle\langle 1|)$, $\sigma_x = (|1\rangle\langle 0| + |0\rangle\langle 1|)$, $i\sigma_y = (|0\rangle\langle 1| - |1\rangle\langle 0|)$, $\sigma_z = (|0\rangle\langle 0| - |1\rangle\langle 1|)$, $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$. Suppose after Bob's encryption, the photons $\otimes_{i=1}^{N}|0\rangle_i$ and $\otimes_{j=1}^{K}|S_j\rangle$ evolve to $\otimes_{i=1}^{N}U_{B_i}|0\rangle_i$, $\otimes_{j=1}^{K}U_{B_j}|S_j\rangle$, respectively, where U_{B_i} and U_{B_j} denote the local unitary operations that Bob chooses randomly. Then Bob sends the photons $\otimes_{i=1}^{N}U_{B_i}|0\rangle_i$ and $\otimes_{j=1}^{K}U_{B_j}|S_j\rangle$ to Charlie. Charlie does the same procedures as Bob, then he sends the encrypted photons $\otimes_{i=1}^{N}U_{C_i}U_{B_i}|0\rangle_i$ and $\otimes_{j=1}^{K}U_{C_j}U_{B_j}|S_j\rangle$ to Dick, where U_{C_i} and U_{C_j} denote the local unitary operations that Charlie chooses randomly. Dick also does the same procedures as Bob, then he sends the encrypted photons $\otimes_{i=1}^{N}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ and $\otimes_{j=1}^{K}U_{D_j}U_{C_j}U_{B_j}|S_j\rangle$ back to Alice, where $U_{D_i}$and U_{D_j} denote the local unitary operations that Charlie chooses randomly.

(3) After receiving the photons $\otimes_{i=1}^{N}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ and $\otimes_{j=1}^{K}U_{D_j}U_{C_j}U_{B_j}|S_j\rangle$, Alice measures every sample photon $U_{D_j}U_{C_j}U_{B_j}|S_j\rangle$ $(j = 1, 2, \ldots, K)$ with X-basis or Z-basis randomly, here $Z = \{|0\rangle, |1\rangle\}$ and $X = \{|+\rangle, |-\rangle\}$. Then, Alice publics the positions of all sample photons $\otimes_{j=1}^{K}U_{D_j}U_{C_j}U_{B_j}|S_j\rangle$, but she keep their measurement outcomes and initial states secret. In the following, Alice lets the three agents tell her their exact unitary operations U_{B_j},U_{C_j} and U_{D_j} $(j = 1, 2, \ldots, K)$. After that, Alice can determine the error rate according to these K sample photons' initial state $\otimes_{j=1}^{K}|S_j\rangle$, measurement outcomes (Note that there is 50% probability that Alice will choose the wrong measurement basis, so half of the measurement outcomes are useless.) and U_{B_j},U_{C_j},U_{D_j} $(j = 1, 2, \ldots, K)$. If the error rate exceeds the threshold, then the communication is aborted. Otherwise, Alice encodes her secret bits by performing a unitary operation U_{A_i} on the photon $U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ $(i = 1, 2, \ldots, N)$, where $U_{A_i} \in \{I, i\sigma_y\}$ and I ($i\sigma_y$) correspond to the classical bit 0(1). After her encoding, similarly does as the step (1), Alice also prepares K' sample photons $\otimes_{k=1}^{K'}|S'_k\rangle$ and inserts randomly them into the encoded photons $\otimes_{i=1}^{N}U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$. Then she sends the photons$\otimes_{k=1}^{K'}|S'_k\rangle$ and $\otimes_{i=1}^{N}U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ to one of the agents, for example, Bob.

(4) After confirming that Bob has received the photons $\otimes_{i=1}^{N}U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ and $\otimes_{k=1}^{K'}|S'_k\rangle$, Alice tells him the positions and initial states of these K' sample photons $\otimes_{k=1}^{K'}|S'_k\rangle$. Then, Bob measures these K' sample photons with proper measurement basis according to Alice's announcement. After these, they can check whether the encoded photons $\otimes_{i=1}^{N}U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ have been attacked. If they are attacked, the eavesdropper Eve cannot get access to any useful information but interrupts the transmissions. Otherwise, Bob stores the encoded photons $\otimes_{i=1}^{N}U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ and this four-party QSSCM is successfully accomplished.

(5) When Bob, Charlie and Dick approve to recover Alice's secret message, Charlie and Dick tell Bob their exact unitary operations U_{C_i},U_{D_i} $(i = 1, 2, \ldots, N)$. If the number of H in the three unitary operations U_{B_i},U_{C_i},U_{D_i} is odd, Bob performs X-basis measurement on the encoded photon $U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$; otherwise, he performs Z-basis measurement. Thus, they can deduce Alice's unitary operation U_{A_i} on each encoded photon $U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ by their unitary operations U_{B_i},U_{C_i},U_{D_i} and Bob's measurement outcome, and recover Alice's secret message. For example, suppose $U_{B_i} = \sigma_x$, $U_{C_i} = \sigma_Z$ and $U_{D_i} = H$, so Bob knows he should measure the encoded photon $U_{A_i}U_{D_i}U_{C_i}U_{B_i}|0\rangle_i$ with X-basis, and if Bob's measurement outcome is $|+\rangle_i$, the state of the photon $|0\rangle_i$ evolves as follows:

$$|0\rangle_i \Rightarrow U_{B_i}|0\rangle_i = |1\rangle_i \Rightarrow U_{C_i}|1\rangle_i = |1\rangle_i \Rightarrow U_{D_i}|1\rangle_i = |-\rangle_i \Rightarrow U_{A_i}|-\rangle_i \Rightarrow |+\rangle_i.$$

Thus, they can deduce easily $U_{A_i} = i\sigma_y$ and recover the secret bit 1. Otherwise, if Bob's measurement outcome is $|-\rangle_i$, they can deduce $U_{A_i} = I$ and recover the secret bit 0.

So far we have proposed a four-party QSSCM scheme using single photons and local unitary operations. In fact, it is a (3, 3) threshold QSSCM scheme. Now let us discuss the security of this four-party QSSCM scheme. As we know, the security of QSS is more complex than quantum key distribute and QSDC because not all of the legitimate agents in QSS schemes are credible, that is, some of