Efficient Multiparty Quantum Secret Sharing of Secure Direct Communication Based on Bell States and Continuous Variable Operations

Hao Yuan · Jun Zhou · Gang Zhang · Huan Yang · Ling-ling Xing

Received: 19 January 2012 / Accepted: 1 June 2012 / Published online: 9 June 2012 © Springer Science+Business Media, LLC 2012

Abstract By using some ordered Bell states as quantum channel, we propose a protocol for multiparty quantum secret sharing of secure direct communication. The present scheme follows the ideas of dense coding and ping-pong technique. It has a high source capacity as each traveling photon carries two bits of classical secret messages, and has a high intrinsic efficiency because almost all the instances are useful. Since the continuous variable operations instead of the discrete unitary operations used usually are employed to realize the sharing controls, the security of the present protocol is therefore enhanced. Furthermore, due to existing multilevel security checking procedures, the present scheme can prevent against some usual attack strategies.

Keywords Quantum state sharing · Quantum secure direct communication · Continuous variable operations · Dense coding · Ping-pong technique

1 Introduction

In the past two decades, the combination of quantum mechanics with cryptograph has produced a novel and interesting field named quantum cryptograph [1, 2]. Comparing with the classical cryptograph whose security is mainly based on the complexity of computation or...
algorithms, which is strongly challenged by the increasing computational capability, quantum cryptography can achieve theoretically unconditional security guaranteed by the quantum mechanics principles, such as no-cloning theorem, uncertainty principle, entanglement, indistinguishability of nonorthogonal states, nonlocality, and so on. Therefore, quantum cryptography has become a hot research topic in the crossing field between cryptograph and quantum mechanics.

Quantum key distribution (QKD) is the earliest and most mature branch of quantum cryptography, which provides a fancy method for two remote legitimate participants, say Alice and Bob, to commonly establish a secret key through the transmission of quantum signals. By using the key Alice and Bob can encrypt or decrypt the secret messages to realize their mutual secret communications. Its ultimate advantage is the unconditional security, the feat in cryptograph. Therefore, after Bennett and Brassard presented the pioneering work in 1984 [1], a variety of QKD protocols [1–8] have been proposed.

On the other hand, a novel concept in quantum cryptography, quantum secure direct communication (QSDC) has been proposed and actively pursued by some groups [5, 9–19] recently. Different from QKD, whose object is to distribute a random private key between two remote legitimate users of communication, QSDC can transmit the secret messages directly without first generating a key to encrypt them. Incidentally, compared with QKD, the security demands are stricter in QSDC because the transmitted secret messages can never be leaked out no matter whether the eavesdropping would be detected or not. Due to its instantaneous, QSDC may be important in some applications, which have been shown by Bostrom et al. [9] and Deng et al. [12].

In a pure QKD or QSDC protocol, the participants of communication usually consist of two legitimate users, one is the message sender and another is the message receiver, they are all considered honest and never violate the protocol. However, sometimes, Alice wants to send some secret messages to two distant participants, Bob and Charlie. Alice doubts that one of them may be dishonest, and knows if the two participants cooperate with each other, then the honest one will keep the dishonest one from doing any damages, otherwise, neither of them can extract Alice’s secret messages. To complete this kind of task, classical cryptography provides a technique referred to as secret sharing. The basic idea of classical secret sharing in the simplest case is that the message sender Alice splits her secret messages $M_A$ into two pieces, $M_B$ and $M_C$, and then distributes them to Bob and Charlie, respectively. In such a way, only Bob and Charlie collaborate together can they read out the secret messages $M_B \oplus M_C = M_A$. Generalizing the classical secret sharing into a quantum scenario generates a novel concept called quantum secret sharing (QSS). QSS is another important application of quantum mechanic in the realm of cryptography. 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 ancillary states and joint sharing of quantum money, and so on. Therefore, since the pioneering work proposed by Hilery, Bužek and Berthiaume in 1999 [20], QSS has attracted a great deal of attentions in both theoretical and experimental aspects [20–48]. All these works concentrate essentially on two kinds of problem. One deals with the QSS of classical information, and another deals with the QSS of quantum information where the secret message is an arbitrary unknown state. The former is customarily referred to as quantum secret sharing of classical message (QSSCM) [20–24, 26, 27, 29, 30, 36–38, 40–43, 46–48] and the latter as quantum state sharing (QSTS) [25, 28, 31–35, 39, 44, 45]. In more detail, QSSCM can be still divided into two kinds, quantum secret sharing of key distribution (QSS-KD) [20–23, 26, 30, 36, 40, 41, 43, 46–48], and quantum secret sharing of secure direct communication (QSS-SDC) [24, 27, 29, 37, 38, 42]. They mainly focus on distributing a private key and directly sharing a classical secret message among all sharers, respectively.
In recent existing QSS protocols, we noticed that, in 2008, Han et al. proposed a novel QSS-SDC protocol (referred to as HLLZ protocol hereafter) [37] only using single photons. The distinct advantages of the HLLZ protocol are that, only single qubits are used as quantum channel and the phase shift operations employed to realize the sharing controls are completely random. Inspired by the HLLZ protocol, in this paper, we will propose another QSS-SDC protocol based on the same continuous variable operations (CVO) as that used in the HLLZ protocol by employing the dense coding [49] and ping-pong technique [9]. In addition, in the process of establishing the quantum channel, we still use the block transmission method, which was firstly proposed by Long in Ref. [5]. Moreover, It is worthy to emphasize that in our scheme we will use Einstein-Podolsky-Rosen (EPR) photon pairs instead of the single qubits in the HLLZ protocol to establish the quantum channel. Such replacements will make our scheme more efficient than the HLLZ protocol, as each EPR pair can carry two bits of classical secret messages. Moreover, since the secret messages are encoded on the entire EPR pair, while only one qubit in the EPR pair is transmitted in the quantum channel, the communication in our scheme is more secure.

2 Efficient Multiparty QSS of SDC Based on Bell-States and CVOs

Now let us describe our efficient multiparty QSS-SDC scheme detailedly. Suppose a boss, say Alice, wants her $n$ agents, say Bob, Charlie, Dick, . . . , and Zach, who are remote places, to deal with her business according to her messages. Alice suspects that some of them may be dishonest and the number of dishonest agents is less than $n$, but does not know who the dishonest agents are. Alice fears that the business may be destroyed if the dishonest agent manages it independently. However, she knows that if the $n$ agents coexist, the honest agents will keep the dishonest ones from doing any damages. Therefore, Alice only wants to send her secret messages to the agent entity instead of any subset of the agents, and no subset of all the agents is sufficient to extract the boss’s secret messages but the agent entity can with mutual assistances. Alice’s this desire can be achieved by our multiparty QSS-SDC scheme, which consists of the following six steps (Fig. 1).

**Step 1:** Preparing some Bell states and creating two photon sequences, say, home sequence and traveling sequence. Bob generates a sequence of $N$ EPR photon pairs. Each EPR pair is randomly in one of the four Bell-states, i.e.,

$$|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2} = (|hh\rangle - |vv\rangle)/\sqrt{2},$$

$$|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2} = (|hh\rangle - |vv\rangle)/\sqrt{2},$$

$$|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2} = (|hv\rangle + |vh\rangle)/\sqrt{2},$$

$$|\phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2} = (|hv\rangle + |vh\rangle)/\sqrt{2},$$

where $|0\rangle$ and $|1\rangle$ are the up and down eigenstates of the $\sigma_z$, and $|h\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|v\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ are the up and down eigenstates of the $\sigma_x$, respectively. We denote the $N$ ordered EPR pairs with $[(H_1, T_1), (H_2, T_2), \ldots, (H_i, T_i), \ldots, (H_N, T_N)]$. Here $H$ and $T$ represent the two photons in an EPR pair, and the subscript indicates the pair order in the sequence, i.e., the $i$ represents the $i$th entangled photon pair. Bob takes one photon from each EPR pair to form an ordered photon sequence, say $\mathcal{H}$ sequence, denoted by $[H_1, H_2, \ldots, H_i, \ldots, H_N]$. The remaining photons compose another partner photon sequence $[T_1, T_2, \ldots, T_i, \ldots, T_N]$, say $T$ sequence. Bob keeps the $\mathcal{H}$ sequence in his lab and sends the $T$ sequence to Charlie.
Fig. 1  Schematic demonstration of the multiparty QSS of SDC based on Bell-states and CVOs. The two Bobs are the same message agent in two different stages. The bold left-arrows denote the encodings on the photons via CVOs or the four discrete unitary operations. The solid circles denotes the chosen or added check particles. The little solid rectangles represent Bell-state measurement.

Step 2: Defeating the possible Trojan horse eavesdropping attacks and encrypting the control phase angle. In order to prevent from Eve’s possible Trojan horse eavesdropping attacks, i.e., the invisible photon attack [11] and delay-photon attack [50], a filter and a photon number splitter (PBS: 50/50) should be used in this protocol. That is, Charlie inserts a filter in front of his devices to filter out the photon signal with an illegal wavelength. Then he stores the quantum signals and chooses randomly a subset of the quantum signals. Charlie splits the sample signals with a PBS, and measures the two signals with the measuring bases $Z = \{ |0\rangle, |1\rangle \}$ and $X = \{ |h\rangle, |v\rangle \}$ randomly. If there is only one photon in the original signal, Charlie can only get one outcome. Otherwise, he will obtain two outcomes. Charlie analyzes the average probability $P_m$ that there are many photons in each quantum signal sent by Bob. If the multiphoton rate $P_m$ is high, Charlie terminates the communication and repeats it from the beginning. Otherwise, he will encrypt his control phase angles on the remaining photons in the sequence $T$. In detail, for each photon, Charlie performs the CVO which takes the form of

$$
\hat{U}(\theta_C) = \begin{pmatrix}
\cos \theta_C & \sin \theta_C \\
-\sin \theta_C & \cos \theta_C
\end{pmatrix}
$$

in the rectilinear basis $\{ |0\rangle, |1\rangle \}$ on it, where $\theta_C$ is a random angle determined by Charlie and may be different for different photons. For clearly, the encrypted sequence is referred to as sequence $T_C$. After his encryptions, Charlie sends the encrypted sequence $T_C$ to the next agent Dick. Dick also lets all Charlie’s photon pulses pass through his filter and analyzes the average multiphoton rate $P'_m$ of $T_C$ by utilizing his PBS. In the condition of $P'_m$ is very low, Dick performs his CVO $\hat{U}(\theta_D)$ on the remaining photons in the sequence $T_C$ in the same way as Charlie, then sends them to the next agent. The similar procedures are repeated until the last agent, say Zach. After Zach’s encryptions, he sends the encrypted sequence $T_Z$ to the boss Alice.

Step 3: The first security checking, i.e., checking the quantum channel from Bob to Alice. Similarly, before receiving the sequence $T_Z$, Alice uses a filter to prevent from Eve’s invisible photon attack, and after receiving it, Alice utilizes a PBS to detect whether the
quantum channel is eavesdropped by Eve’s decoy-photon attack. Subsequently, Alice selects randomly a fraction of photons from the sequence $T_Z$ and publicly announces their positions. For each of the selected photons, Alice requires all agents one by one to publish their encrypted angles, noting that the agents’ published order is randomly assigned by Alice. Then she performs the reverse CVO $\hat{U}(-\theta_C - \cdots - \theta_Z)$ on it. From the Eq. (5), one can see that $\hat{U}(\Sigma_{k=1}^p \theta_k) = \Pi_{k=1}^p \hat{U}(\theta_k)$ and $\hat{U}(\theta_k)\hat{U}(-\theta_k) = I$. Obviously, after Alice’s performances, each of the selected traveling photons and its partner home photon should be recovered to their original Bell state if the traveling photon is not disturbed during the transmission. According to this principle, Alice can determine the error rate and judge whether the quantum channel is disturbed. The detailed checking process is as follows. For each of the selected photons, say $T_i$, Alice lets Bob perform a measurement on its partner photon $H_i$, either in the measuring basis $Z$ or in the measuring basis $X$, and then tell her the measuring basis and the measurement outcome as well as the initial Bell state. After these, Alice performs a measurement on $T_i$ using the same basis as Bob used. According to Eqs. (1)–(4), their measurement results should be completely correlated if no eavesdropping exists. By comparing their measurement outcomes, Alice can then evaluate the error rate of the traveling sequence dying the entire transmission process from Bob to Alice. If the error rate exceeds the threshold, they discard the transmission and repeat the procedure from the beginning. Otherwise, they continue to the next step.

**Step 4: Encoding secret messages.** Alice performs one of the four unitary operations \{$U_{00}, U_{01}, U_{10}, U_{11}$\} on each of the remaining photons in $T_Z$ sequence to encode her secret information, where

$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$U_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and they correspond to the two bits of classical information 00, 01, 10 and 11, respectively. The nice feature of the operation $U_{ij}$ ($i, j = 0, 1$) is that it flips the state in above four Bell states. For example, $U_{00}|\psi^+\rangle = |\psi^+\rangle$, $U_{01}|\psi^+\rangle = |\psi^-\rangle$, $U_{10}|\psi^+\rangle = |\phi^+\rangle$, and $U_{11}|\psi^+\rangle = |\psi^-\rangle$. Note that, to guarantee the security of the next transmission, it is necessary for Alice to insert some random bits (called the authentication bits) in the bit string of the secret messages. The encoded sequence is referred as sequence $T_A$. Alice sends the sequence $T_A$ to Bob.

**Step 5: Recovery phase and decoding secret messages.** After Bob receives the sequence $T_A$, he can reconstruct the secret information with the help of other agents. In detail, if other agents will to cooperate with Bob, they tell him their respective encrypted phases. For each photon, say, the photon $T_j$, Bob first performs the reverse CVO $\hat{U}(-\theta_C - \cdots - \theta_Z)$ on it. The decoding sequence is referred as sequence $T'$. After his performances, each EPR pair in the sequences $T'$ and $H$ should be recovered to the encoded Bell-basis state. Next, Bob performs the Bell-basis measurements on them. By comparing his measurement results with the corresponding original states, Bob can deduce Alice’s secret messages. For example, suppose an EPR pair originally prepared by Bob is in $|\phi^-\rangle$, and if Bob’s final measurement result is $|\psi^+\rangle$, then Alice’s secret messages is “11”; if Bob’s final measurement result is $|\psi^-\rangle$, then Alice’s secret messages is “10”; if Bob’s final measurement result is $|\phi^+\rangle$, then Alice’s secret messages is “01”; if Bob’s final measurement result is $|\phi^-\rangle$, then Alice’s secret messages is “00”. On the other hand, if anyone is not willing to collaborate with Bob, then neither of them can get access to Alice’s secret messages.
Step 6: The second security checking, i.e., checking the quantum channel from Alice to Bob. Alice reveals the positions and values of the authentication bits for all agents to check whether the sequence $T_A$ traveling from Alice to Bob has been attacked, which is called message authentication. In fact, once the security of the first transmission (i.e., the transmission from Bob till to Alice) is ensured, then the eavesdropper Eve cannot obtain any useful information but only disturb the communication in this transmission (i.e., the transmission from Alice to Bob). Therefore, the purpose of this step is to detect Eve’s possible disturbance attacks in the quantum channel from Alice to Bob. If too few values of the authentication bits agree, then they abandon the communication and repeat the procedure from the beginning. Otherwise, they triumphantly share all of boss’s secret messages.

So far we have expatiated a multiparty QSS scheme for secure direct communication with a sequence of Bell states. Incidentally, if the quantum channel is lossy or noisy, then the quantum error correction and privacy amplification have to be performed.

3 Security Analyses

Now, let us discuss it’s security briefly. Since the control operations are CVOs randomly chosen by Charlie, Dick, ..., and Zach instead of some special discrete unitary operations, no one can obtain the phase shift values of the CVOs except for themselves. Therefore, as far as the security is considered, the present scheme can come down to three-party communication. That is the quantum resource preparer Bob*, the secret messages controller Zach*, and the secret messages sender Alice. If some of dishonest agents including Bob are the eavesdroppers, then they equal to Bob*, and the remaining honest agents equal to Zach*. Contrarily, if some of dishonest agents except for Bob are the eavesdroppers, then they equal to Zach* and the remaining honest agents including Bob equal to Bob*. Following, we mainly consider some kinds of usual attack strategies and various existing special attack strategies in the simplified three-party communication.

Type 1: Trojan horse attack strategies. There are mainly two kinds of Trojan horse attack strategies. One is the invisible photon eavesdropping (IPE) attack and the other is the delay photon eavesdropping (DPE) attack. Whether Eve is Bob*, Zach* or an outside eavesdropper, she may bethink of such attack strategies firstly. Now, we analyze these kinds of attacks in detail. (I) IPE attack: Eve prepares a sequence of EPR photon pair with a special wavelength in advance, which is close to the legitimate one, and each EPR pair is randomly in one of the four Bell states. She divides them into two sequences named $H_Z'$ sequence and $T_Z'$ sequence, and they are denoted by $[H'_1, H'_2, ..., H'_i, ..., H'_M]$ and $[T'_1, T'_2, ..., T'_i, ..., T'_M]$, respectively. During the process that Zach* sends his quantum signal sequence $T_Z$ to Bob, Eve inserts each her photon $T'_i$ into the legitimate photon $T_i$ signal pulse. Therefore, when Alice performs unitary operations on the sequence $T_Z$, she also performs the operations on Eve’s invisible sequence $T'_Z$. After Alice sends the two encoded sequences $T_A$ an $T'_A$ to Bob*, Eve captures his invisible encoded sequence $T'_A$, and performs Bell-basis measurement on each encoded photon in the sequence $T'_A$ and its partner photon in the sequence $H'_Z$. By comparing her measurement results with the corresponding initial Bell states, Eve can easily extract Alice’s secret messages. Nevertheless, in our scheme, Alice adds a filter in her laboratory in advance. All the photon pulses (including the legitimate photon pulses and Eve’s invisible photon pulses) should pass through the filter before she performs her encoding unitary operations. Only wavelengths extraordinary close to the operation wavelength can be in. Hence, Eve’s invisible photons can be filtered out. Even if some Eve’s invisible photons cannot be filtered out by the filter, then they will still be detected by Alice’s PBS.
(II) DPE attack: Eve prepares a sequence of spy EPR pairs with the same wavelength as the legitimate one in advance, and each spy EPR pair is randomly in one of the four Bell states. She divides it into two sequences named $\mathcal{H}_Z^{\prime\prime}$ sequence and $T_Z^{\prime\prime}$ sequence, and they are denoted by $[H_i^{\prime\prime}, H_2^{\prime\prime}, \ldots, H_n^{\prime\prime}, \ldots, H_M^{\prime\prime}]$ and $[T_i^{\prime\prime}, T_2^{\prime\prime}, \ldots, T_i^{\prime\prime}, \ldots, T_M^{\prime\prime}]$, respectively. When Zach* sends her photon sequence $T_Z$ to Alice, Eve inserts each spy photon after each legal signal pulse with a delay time which is shorter than the time windows of Alice’s optical devices. In such case, Alice will perform the exact same operations on the spy sequence $T_Z^{\prime\prime}$ as that on the legal sequence $T_Z$. During Alice returns the encoded sequences $T_A$ and $T_A^{\prime\prime}$ to Bob*, Eve sorts out her spy encoded sequence $T_A^{\prime\prime}$ while lets the sequence $T_A$ go its way to Bob*. Then Eve performs Bell-basis measurement on each spy photon in the sequence $T_A^{\prime\prime}$ and its partner photon in the sequence $\mathcal{H}_Z^{\prime\prime}$. As the spy photon pair sequence is prepared by Eve, she knows the original state of each spy photon pair in it. Therefore, by comparing her measurement results with the corresponding initial Bell states, Eve can read out Alice’s secret messages directly. Unfortunately, before encoding Alice randomly chooses a subset of the quantum signals and splits them with a PBS. Thus each sampling multiphoton signal (including the legal photon signal, the spy delay photon signal and the invisible photon signal whose wavelength is so close to the legal one that it cannot be filtered out with the filter) will be split into two pieces. By performing two single-photon measurements on the two-pieces signal, Alice will easily find the existing of multiphoton signal. Thus, Eve’s such attack can be effectively forbidden in this protocol.

Type 2: Man-in-the-middle attack strategies. Eve can access quantum channel and might execute her evil action by manipulating it. To steal the secret messages, she may adopt some kinds of man-in-the-middle-attack strategies, such as the intercept-measurement-resend attack and the intercept-replacement-resend attack. (I) The intercept-measurement-resend attack: Eve may only need to estimate the states of the photon pairs immediately before and after Alice’s encoding operations to extract Alice’s secret messages. However, the present scheme employs two correlative sequences as quantum channel, one sequence is retained after Alice’s encoding operations to extract Alice’s secret messages. However, the present scheme employs two correlative sequences as quantum channel, one sequence is retained after Alice’s encoding operations to extract Alice’s secret messages. Hence, all of the outside eavesdroppers and the inside eavesdroppers (i.e., the dishonest ones among the $n$ agents) except Bob* have no chance to eavesdrop the secret messages by using such attack. One may unaffectedly bethink of, if Bob* is assuredly the dishonest agent, can he steal the agent entity’s operation to extract Alice’s secret messages? The key is not can absolutely. The reason is that he can not obtain the phase shift values of Zach*’s CVOs. (II) the intercept-replacement-measurement-resend attack: Eve prepares her own ordered EPR pairs and each EPR pair is randomly prepared in one of the four Bell states. Then she divides the ordered EPR pairs into two correlated particle sequences, say sequences $\mathcal{H}_Z^{\prime\prime}$ and $T_Z^{\prime\prime}$. When Zach* sends his sequence $T_Z$ to Alice, Eve intercepts it and sends her own sequence $T_Z^{\prime\prime}$ to Alice. Subsequently, when Alice sends the encoded sequence $T_A^{\prime\prime}$ to Bob*, Eve intercepts it again and orderly measures each encoded photon pair ($H_i^{\prime\prime}$, $T_i^{\prime\prime}$) using Bell measurement basis. By comparing the initial state and the corresponding measurement result of each EPR pair, Eve can deduce Alice’s secret messages. To escape the security checking, Eve then performs the same unitary operation as Alice used on each photon pair in the sequence $T_A$ and then sends the encoded sequence to Bob*. However, the EPR pair ($H_i^{\prime\prime}$, $T_i^{\prime\prime}$) created by Eve has no correlation with the EPR pair ($H_i$, $T_i$) prepared by Bob*, and the phase shift value of Zach*’s CVOs is secret to anyone else. Therefore, whether the eavesdropper is Bob* or someone else, his eavesdropping action will be easily detected by the checking procedure elaborated in the step 3 of the present scheme.
**Type 3: Denial-of-service attack strategy.** Suppose Eve only wants to destroy the communication while not eavesdropping the secret messages. For such purpose, Eve may intercept the sequence $T_A$ when it is traveling from Alice to Bob. Then she can apply an discretionary operation on each particle in the sequence $T_A$. Subsequently, Eve lets the disturbed sequence $T_A$ go on its way. Obviously, since Eve only monitors the quantum channel from Alice to Bob, his maleficent action can not be detected by the legitimate communicators during the first security checking process. Fortunately, Alice encodes her secret messages as the same time inserts some authentication bits in them. The secret messages are disturbed as the same time the authentication bits are disturbed also. Therefore, when Alice reveals the positions and values of the authentication bits, the legitimate agents can easily find Eve’s such attack.

From the above analyses, one can see that the present scheme is immune to some usual attack strategies. Just as the literature cite [37] goes, the security of the most existing QSS protocols which employ some special discrete unitary operations to realize the sharing controls are unreliable. On the contrary, the present scheme employs the CVOs to realize the control action. Currently, the CVOs can not be decoded efficiently. In such sense, the present scheme is relative secure undoubtedly. On the other hand, as the secret messages are encoded on the EPR pairs in the present scheme instead of the single particle sequence in Ref. [37], and only one particle in an EPR pair is transmitting in the quantum channel. Hence, although both are based on the CVOs to achieve the purpose of secure sharing control, the present scheme may be more secure than Ref. [37]. Incidentally, Ref. [37] was reexamined with a special participant attack strategy by Qin et al. [38] later. However, recently, Yen et al. [42] found some errors existing in the Qin’s attack and showed it could not attack the HLLZ protocol successfully. Since the HLLZ protocol has no security hole, the present scheme should also be secure.

**4 Summary**

To summarize, in this paper, by utilizing the CVOs as control operations and EPR pairs as quantum channel, we have proposed a new novel multiparty QSS-SDC scheme. The present scheme follows the ideas of dense coding and ping-pong technique. It has a high source capacity as each traveling photon carries two bits of classical secret messages, and has a high intrinsic efficiency because almost all the instances are useful. Due to existing multilevel checking measures, the present scheme is preventible to some usual attack strategies. The extensively using of filters and PBSs can effectual hold back the IPE and DPE attacks, the alternating implement of two conjugate measurement bases in the first checking procedure can protect the communication against some man-in-the-middle eavesdropping attacks, such as the intercept-measurement-resend attack and the intercept-replacement-measurement-resend attack, and the message authentication method in the second checking procedure can protect the communication against any kind of denial-of-service attack.

**Acknowledgements**  This work is supported by the Key Project of the Education Department of Anhui Province under Grant No. KJ2010A323, the Talent Project of the Anhui Province for Outstanding Youth under Grant Nos. 2009SQRZ190, 2010SQR186, 2010SQR187 and 2011SQR147, the Natural Science Research Programme of the Education Department of Anhui Province under Grant Nos. KJ2009B018Z and KJ2011B208.
References

1. Bennett, C.H., Brassard, G.: In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processings, Bangalore, India, p. 175. IEEE, New York (1984)
2. Bennett, C.H., Brassard, G., Mermin, N.D.: Phys. Rev. Lett. 68, 557 (1992)
3. Cabello, A.: Phys. Rev. Lett. 85, 5635 (2000)
4. Cabello, A.: Phys. Rev. A 61, 052312 (2000)
5. Long, G.L., Liu, X.S.: Phys. Rev. A 65, 032302 (2002)
6. Deng, F.G., Long, G.L.: Phys. Rev. A 68, 042315 (2003)
7. Kye, W.H., Kim, C.M., Kim, M.S., Park, Y.J.: Phys. Rev. Lett. 95, 040501 (2005)
8. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A 78, 022321 (2008)
9. Boström, K., Felbinger, T.: Phys. Rev. Lett. 89, 187902 (2002)
10. Wójcik, A.: Phys. Rev. Lett. 90, 157901 (2003)
11. Cai, Q.Y.: Phys. Lett. A 351, 23 (2006)
12. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A 68, 042317 (2003)
13. Deng, F.G., Long, G.L.: Phys. Rev. A 69, 052319 (2004)
14. Wang, C., Deng, F.G., Long, G.L.: Opt. Commun. 253, 15 (2005)
15. Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Phys. Rev. A 71, 044405 (2005)
16. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Phys. Lett. A 359, 359 (2006)
17. Long, G.L. et al.: Front. Phys. China 2, 251 (2007)
18. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Phys. Rev. A 78, 022321 (2008)
19. Hillery, M., Buzk, V., Berthiaume, A.: Phys. Rev. A 59, 042311 (1999)
20. Gottesman, D.: Phys. Rev. A 61, 042311 (2000)
21. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Ping, K.L.: Phys. Rev. Lett. 92, 177903 (2004)
22. Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Phys. Rev. A 69, 052307 (2004)
23. Chau, H.F.: Phys. Rev. A 66, 060302 (2002)
24. Bagherinezhad, S., Karimpour, V.: Phys. Rev. A 67, 044302 (2003)
25. Lance, A.M., Symul, T., Bowen, W.P., Sanders, B.C., Ping, K.L.: Phys. Rev. Lett. 92, 177903 (2004)
26. Zhao, Z.J., Yang, J., Man, Z.X., Li, Y.: Eur. Phys. J. D 33, 133 (2005)
27. Zhang, Z.J., Jin, X.R., Zhang, S.: Phys. Lett. A 341, 380 (2005)
28. Lance, A.M., Symul, T., Bowen, W.P.: Phys. Rev. A 71, 033814 (2005)
29. Zhao, Z.J.: Opt. Commun. 261, 199 (2006)
30. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Phys. Rev. A 72, 044301 (2005)
31. Hsu, L.Y., Li, C.M.: Phys. Rev. A 71, 022321 (2005)
32. Deng, F.G., Long, G.L., Zhou, H.Y.: Phys. Lett. A 340, 43 (2005)
33. Zhang, J.Z., Yang, J., Man, Z.X., Li, Y.: Eur. Phys. J. D 33, 133 (2005)
34. Zhao, J.Q., Jin, X.R., Zhang, S.: Phys. Lett. A 341, 380 (2005)
35. Lance, A.M., Symul, T., Bowen, W.P.: Phys. Rev. A 71, 033814 (2005)
36. Zhao, Z.J.: Opt. Commun. 261, 199 (2006)
37. Deng, F.G., Li, X.H., Li, C.Y., Zhou, P., Zhou, H.Y.: Eur. Phys. J. D 39, 459 (2006)
38. Zhou, P., Li, X.H., Liang, Y.J., Deng, F.G., Zhou, H.Y.: Physica A 381, 164 (2007)
39. Han, L.F., Liu, Y.M., Liu, J., Zhang, Z.J.: Opt. Commun. 281, 2690 (2008)
40. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Opt. Commun. 281, 5472 (2008)
41. Xiao, L., Wang, C., Zhang, W., Huang, H.D., Peng, J.D., Long, G.L.: Phys. Rev. A 77, 042315 (2008)
42. Lin, S., Wen, Q.Y., Qin, S.J., Zhu, F.C.: Opt. Commun. 282, 4455 (2009)
43. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Opt. Commun. 282, 3647 (2009)
44. Yen, C.A., Horng, S.J., Goan, H.S., Kao, T.W.: Opt. Commun. 283, 3202 (2010)
45. Gu, B., Mu, L.L., Ding, L.G., Zhang, C.Y., Li, C.Q.: Opt. Commun. 283, 3099 (2010)
46. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Opt. Commun. 283, 2762 (2010)
47. Hou, K., Li, Y.B., Shi, S.H.: Opt. Commun. 283, 1961 (2010)
48. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Opt. Commun. 283, 2476 (2010)
49. Hao, L., Li, J.L., Long, G.L.: Sci. China Phys. 53, 491 (2010)
50. Li, X.H., Deng, F.G., Zhou, H.Y.: Phys. Rev. A 74, 054302 (2006)