Int J Theor Phys (2011) 50: 308–313
DOI 10.1007/s10773-010-0524-x

Comment on "Reply to Comment on 'Efficient High-Capacity Quantum Secret Sharing with Two-Photon Entanglement' "

Zhen-Chao Zhu · Yu-Qing Zhang · An-Min Fu

Received: 24 June 2010 / Accepted: 1 October 2010 / Published online: 21 October 2010

Abstract In Deng, Li, and Zhou (Phys. Lett. A 373:399, 2009), the authors propose two improved efficient high-capacity quantum secret sharing schemes to solve the problems existed in the Letter (Phys. Lett. A 372:1957, 2008), they claim that these two schemes are secure and efficient. However, we point out here that these two improved schemes are not secure as one agent can obtain all the information without the help from the other agent. We further modify this three-party quantum secret sharing scheme and make it really secure. In the end, we also give a method to generalize our quantum secret sharing scheme to arbitrary multi-party scheme.

Keywords Quantum secret sharing · Quantum entanglement · Bell state · Non-orthogonal base

In 2008, Deng et al. introduced an efficient high capacity quantum secret sharing (QSS) scheme (DLZ protocol) with quantum dense coding based on two-photon entangled states [1]. In this protocol, the two agents, Bob and Charlie choose the single-photon measurements on the sampling photons with three measuring-base (MBs) randomly for eavesdropping check, and encode their information with four local unitary operations, which make this QSS scheme more convenient for the agents than some other schemes [2, 3]. In DLZ scheme, almost all the entangled photon pairs can be used to exchange the random key and each photon pair can carry two bits of information. The intrinsic efficiency for qubit is double as that in KKI QSS scheme [3], and the source capacity is four times as the latter with the photons running forth and back. However, In 2009, Yang et al. showed that the protocol could not complete the task of secret sharing perfectly when the message sender uses

Z.-C. Zhu · A.-M. Fu
Key Lab of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China

Z.-C. Zhu · Y.-Q. Zhang (✉) · A.-M. Fu
National Computer Network Intrusion Protection Center, Graduate University of Chinese Academy of Sciences, Beijing 100049, China
e-mail: zhangyq@gucas.ac.cn

two non-orthogonal bases for preparing and measuring the quantum information carriers, then they proposed an improved quantum secret sharing protocol (YW protocol) [4] based on DLZ protocol. However, Deng et al. showed that YW protocol was not secure too in the latest paper [5], they admitted that there was a neglect in their original scheme, the scheme would become valid if the sender announces MB of each Einstein-Podolsky-Rosen (EPR) pair after the transmission, the two agents Bob and Charlie should encode their local unitary operations according to the information of the MB of the EPR pair transmitted, we call this improved protocol DLZ^{+}. Deng et al. realized that the above modification would reduce the efficiency unavoidably and then proposed a simplified version of the scheme which we call DLZ^{++} [5], they claimed that the simplified scheme DLZ^{++} was secure and more efficient than that DLZ^{+}. In this comment, we will show that both DLZ^{+} and DLZ^{++} are not secure. We will propose a new protocol for quantum secret sharing. In our protocol, the sharing of the secret is accomplished by coding of the two-particle quantum entanglement states but not the coding of some special discrete unitary operations as that in Refs. [1, 4, 5]. The security of the protocol will be discussed, the scheme has a high intrinsic efficiency for qubits and a high capacity. We also give a method to generalize our scheme to arbitrary multi-party scheme.

Let us give a brief description of the DLZ^{++} protocol [5]. Alice prepares two photons B and C randomly in one of the four entangled states $\{\phi^{\pm}, \psi^{\pm}\}$. Then she sends B to Bob and sends C to Charlie. For preventing the dishonest agent from eavesdropping freely with an opaque attack, Alice sends a decoy photon to each agent with the fixation probability. Bob and Charlie choose the single photon measurements on the sampling photons with the MBs Z, X or Y randomly for eavesdropping check, and encode their random keys on the other photons received with the four unitary operations U_i $(i = 0, 1, 2, 3)$. Then they send the photons back to Alice. Alice takes a Bell-basis measurement on each two correlated photons received from Bob and Charlie with the basis $\{\phi^{\pm}, \psi^{\pm}\}$. The measurement gives out the outcome of the combination of the unitary operations performed by Bob and Charlie, $U_A = U_B \otimes U_C, U_B, U_C \in \{U_i\ (i = 0, 1, 2, 3)\}$. Alice completes the error rate with the helps of her two agents, She requires Bob and Charlie to publish the MBs and the outcomes of the sample photons for which they choose the checking-eavesdropping mode, Alice should also pick out randomly a sufficiently large subset of the outcomes from the Bell-basis measurements on the entangled quantum systems, and analyze its error rate, named it as the second check. If the communication is secure, U_A represents two bits of classical information which can be used as the raw key.

In Ref. [5], the authors thought that the DLZ^{++} protocol was secure and more efficient for only using one set of orthogonal entangled states. However, we will show that the DLZ^{++} protocol is not secure. In the following, we will prove this fact. Suppose that Charlie want to obtain the information without the help from Bob, in the step (3), after receiving the photons C from Alice, Charlie performs on the photons C as a legal agent, however, he intercepts the photons B sent from Bob to Alice, and stores it with a quantum memory. Charlie prepares a fake EPR pair $B'C'$ which is random in one of the following four states $\{\phi^{\pm}, \psi^{\pm}\}$ and sends the photon B' to Alice, instead of the photon B. Charlie sends the photon C' to Alice, instead of the photon C in the step (5), when Alice requires Bob and Charlie to publish the MBs and the outcomes of the sample photons for which they choose the checking-eavesdropping mode, Charlie publics the operations performed on the photon C. It is obvious that Charlie's eavesdropping introduces no errors until now, as this eavesdropping check just monitors the eavesdropper of the quantum channel from Alice to her agents. Let us consider the second check, Alice picks out randomly a sufficiently large subset of the outcomes from the Bell-basis measurements on the entangled quantum systems. Charlie takes a Bell-state

Table 1 Relations among Bell-state measurement on the EPR pair BC, the state of the fake EPR pair $B'C'$ and Charlie's publications, the states of the fake EPR pair $B'C'$ are listed in the first row; Bell-state measurements on the photons EPR pair BC are listed in the first column

	$\|\phi^+\rangle$	$\|\phi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
$\|\phi^+\rangle$	U_0	U_1	U_2	U_3
$\|\phi^-\rangle$	U_1	U_0	U_3	U_2
$\|\psi^+\rangle$	U_2	U_3	U_0	U_1
$\|\psi^-\rangle$	U_3	U_2	U_1	U_0

measurement on the photons BC, Charlie compares the EPR pair BC and the fake EPR pair $B'C'$, for example, if the EPR pair $B'C'$ is in the state $|\phi^+\rangle$ and the measurement on the photons BC is $|\phi^-\rangle$, Charlie publics his operations is U_1. Now, let's think about why Charlie's cheating action is feasible. We can see that, if Charlie does not play the replacing trick, but honestly performs operation on the photon C and then sends it to Alice, the photons received by Alice is $I \otimes U_1|\phi^-\rangle$. Clearly, $I \otimes U_1|\phi^-\rangle$ and $|\phi^+\rangle$ are in the same states, so Charlie's eavesdropping introduces no errors. In the case that Bell-state measurement on the photons BC is $|\phi^+\rangle$, $|\psi^+\rangle$ or $|\psi^-\rangle$, the corresponding publication will be U_0, U_2 or U_3 respectively.

We give the following Table 1 to illustrate Charlie's publications based on the Bell-state measurement on the photons EPR pair BC and the fake EPR pair $B'C'$. The above attacking method is also effective to the DLZ$^+$ protocol, as the only difference between these two protocols is that DLZ^{++} protocol replaces the eight non-orthogonal entangled states $\{\phi^\pm, \psi^\pm, \Phi^\pm, \Psi^\pm\}$ with the four orthogonal states $\{\phi^\pm, \psi^\pm\}$ in the step (2), eight non-orthogonal entangled states belong to two basis sets $\{\phi^\pm, \psi^\pm\}$ and $\{\Phi^\pm, \Psi^\pm\}$. Two different basis sets used in DLZ$^+$ protocol are not orthogonal, which seems to forbid Charlie to copy them perfectly, but the sender (Alice) in DLZ$^+$ protocol announces the MBs of each EPR pair after the transmission, Charlie can choose the fake EPR pair $B'C'$ from sets $\{\phi^\pm, \psi^\pm\}$ or $\{\Phi^\pm, \Psi^\pm\}$ according to the sender (Alice)'s publication, in this case, the second check will be invalid to prevent the dishonest agent from eavesdropping the process from the other agent to Alice freely. We point out that Bob in the DLZ^{++} protocol and DLZ$^+$ protocol can also obtain the information without the help from Charlie with the same attacking strategy.

Through the analysis above, we found that if we want to use the DLZ protocol for secret sharing, it has to be modified. For convenience, we first give the simple case in which there are only three parties, the Boss Alice, two agents, Bob and Charlie. As our protocol is based on the DLZ protocol, to retain the features and the advantages of the original protocol, we just give it a little modification of the original protocol. Now, let us describe the principle of our scheme in detail, which is implemented by the following six steps as follows:

(1) Alice, Bob and Charlie agree that only four local unitary operations will be used in the protocol. Which are

$$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad U_1 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$U_2 = \sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1| \quad \text{and} \quad U_3 = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

(2) Alice prepares a batch of N photons randomly in one of the following eight non-orthogonal entangled states $\{|\phi^\pm\rangle_{BC}, |\psi^\pm\rangle_{BC}, |\Phi^\pm\rangle_{BC}, |\Psi^\pm\rangle_{BC}\}$. She sends B to Bob and sends C to Charlie. For preventing the dishonest agent from eavesdropping freely with an

opaque attack [6], Alice sends a decoy photon [7, 8], which is randomly in one of the six states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle, |+y\rangle, |-y\rangle\}$, to each agent with the probability P_d.

(3) Bob and Charlie choose one of the two modes, a small probability P_c $(< 1/2)$ with the checking eavesdropping mode and a large probability $1 - P_c$ with the coding mode, similar to those in Refs. [9–11]. If Bob (Charlie) chooses the checking-eavesdropping mode, Bob (Charlie) measures his photon by choosing one of the three MBs Z, X and Y randomly; otherwise, Bob (Charlie) performs one of the four unitary operations $\{U_i\}$ $(i = 0, 1, 2, 3)$ on the received photon, Bob (Charlie) records the unitary operations sequence and then sends the photon back to the sender Alice.

(4) Alice takes a measurement on each two correlated photons received from Bob and Charlie with the two photon entanglement basis $\{|\phi^{\pm}\rangle, |\psi^{\pm}\rangle\}$ or $\{|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle\}$, as the same as that she prepares them before the communication. As the operations done by the agents on the quantum system composed of the photons B and C do not change its basis, the measurement done by Alice is deterministic and will give out the outcome of final entangled states which is one of the following eight entangled states $\{U_B \otimes U_C|\phi^{\pm}\rangle, U_B \otimes U_C|\psi^{\pm}\rangle, U_B \otimes U_C|\Phi^{\pm}\rangle, U_B \otimes U_C|\Psi^{\pm}\rangle\}$. If one of the two agents, say Bob, measures his photon and Charlie sends his photon back to Alice, instead of performing one of the four unitary operations $\{U_i\}$ $(i = 0, 1, 2, 3)$ on the received photon, Alice will get nothing with her Bell-basis measurement.

(5) Alice completes the error rate with the helps of her two agents. She requires Bob and Charlie to publish the MBs and the outcomes of the sample photons for which they choose the checking-eavesdropping mode. Alice exploits the refined error analysis technique [11] for checking eavesdropping of the process of the transmission from Alice to her agents. That is, Alice only picks up the decoy photons measured by the agents to check eavesdropping. As the agents measure the decoy photons with the three MBs, Z, Y and X, the probability that the outcomes of the agents' are correlated with those of Alice's is $\frac{1}{3}P_d P_c$. For preventing the dishonest agent from eavesdropping the process from the other agent to Alice freely, Alice should also pick out randomly a sufficiently large subset of the outcomes from the Bell-basis measurements on the entangled quantum systems, and analyzes its error rate, named it as the second check. It is useful for check the security of the quantum channel when the photons run from the two agents back to Alice. For half of these instances, Alice requires Bob first publish his operations and then Charlie, or vice versa.

(6) If all the error rates are lower than the given threshold, Alice publics the initial states of the N non-orthogonal entangled photons, Bob can use the initial states and the unitary operations (while Bob can get Charlie's unitary operation through the interacting with Charlie) to distill the private key which is the coding of the final entangled states; otherwise, they will abandon the outcomes transmitted and repeat the quantum communication from the beginning.

We provide that the final states of the entangled photons $\{|\phi^+\rangle, |\Phi^+\rangle\}$ represent the classical bits 00, $\{|\phi^-\rangle, |\Phi^-\rangle\}$ represent the classical bits 01, $\{|\psi^+\rangle, |\Psi^+\rangle\}$ represent the bits 10 and $\{|\psi^-\rangle, |\Psi^-\rangle\}$ represent the bits 11.

For example, if the initial states of the N non-orthogonal entangled photon is $|\phi^+\rangle$, we give the following table to illustrate our secret sharing protocol. If Alice's final measurement outcome is $|\phi^-\rangle$, through the analysis of Table 2, the unitary operations performed on the photons corresponding to the sequence B and sequence C may be U_0U_1, U_1U_0, U_2U_3 or U_3U_2, no matter which operations are chosen by Bob and Charlie, Alice will deduce the corresponding private key bits are 01; Bob can use the initial states $|\phi^+\rangle$ and the unitary operations (while Bob can get Charlie's unitary operation through the interacting with Charlie) to distill the private key, provided that Bob's unitary operation is U_2, after getting

Table 2 Relations among Bob's local unitary operations, Charlie's local unitary operations and Alice's measurement results in the condition that the photon's initial state prepared by Alice is $|\phi^+\rangle$, Bob's local unitary operation is listed in the first row; Charlie's local unitary operation is listed in the first column

$\|\phi^+\rangle$	$U_0 = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$U_1 = \|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$U_2 = \|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	$U_3 = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$
$U_0 = \|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\|\phi^+\rangle$ 00	$\|\phi^-\rangle$ 01	$\|\psi^+\rangle$ 10	$\|\psi^-\rangle$ 11
$U_1 = \|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\|\phi^-\rangle$ 01	$\|\phi^+\rangle$ 00	$\|\psi^-\rangle$ 11	$\|\psi^+\rangle$ 10
$U_2 = \|1\rangle\langle 0\| + \|0\rangle\langle 1\|$	$\|\psi^+\rangle$ 10	$\|\psi^-\rangle$ 11	$\|\phi^+\rangle$ 00	$\|\phi^-\rangle$ 01
$U_3 = \|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\|\psi^-\rangle$ 11	$\|\psi^+\rangle$ 10	$\|\phi^-\rangle$ 01	$\|\phi^+\rangle$ 00

Charlie's unitary operation U_3 through interacting with Charlie, Bob will deduce the final entangled states and the corresponding private key bits. Charlie can distill the private key with the same method. For the succinctness, the situations for the other seven entangled states $|\phi^-\rangle, |\psi^\pm\rangle, |\Phi^\pm\rangle, |\Psi^\pm\rangle$ are omitted here.

AS that discussed of the DLZ QSS scheme, a dishonest agent, say Bob (or Charlie) can not steal some information with an opaque attack freely and fully [6] for the exploiting the decoy photons, the process of eavesdropping check with decoy photons between Alice and Charlie does not require Bob to participate in it, which will forbid Bob to eavesdrop the quantum channel from Alice to Charlie with an opaque attack strategy [6]. The same process takes place between Alice and Bob. The only potential safety hazard compared to the original DLZ QSS scheme is that the publication of initial states prepared by Alice, however, in our scheme, the security checking before the publication of the initial states will make potential attackers can not get any useful information, for any initial prepared entangled photon is randomly chosen from the following eight non-orthogonal entangled states $\{|\phi^\pm\rangle, |\psi^\pm\rangle, |\Phi^\pm\rangle, |\Psi^\pm\rangle\}$, also the operations operated on the photons by Bob and Charlie are randomly chosen from the four local unitary operations, without the final entangled states the attacker can not get any useful information. As we just give a little modification of the original protocol, the scheme retains most features and advantages of the DLZ protocol. For example, almost all the entangled photon pairs except those used for eavesdropping check can be used to exchange the random key and each photon pair can carry two bits of information. The intrinsic efficiency for qubits is double as that in KKI QSS scheme [3]. The source capacity is four times as the latter with the photons running forth and back.

Compared to YW scheme [4] and DLZ$^+$ scheme [5], Charlie and Bob in our scheme do not need to encode local unitary operations in different way to make sure that the sender Alice can deduce the combination of the keys deterministically, our scheme also does not need that the sender (Alice) announces MB of each EPR pair after the transmission, so our scheme has a higher execution efficiency than the YW scheme [4] and DLZ$^+$ scheme [5]. We admit that DLZ^{++} scheme in Ref. [5] is more efficient than our scheme, but it replaces eight non-orthogonal entangled states with four orthogonal states in DLZ^{++} protocol, this makes the protocol unsecure.

It is easy to generalize our QSS scheme to multi-party QSS scheme. Suppose the sender, Alice, wants to transmit a secret message to the n agents, Bob$_1$, Bob$_2, \ldots,$ Bob$_m$, Charlie$_1$, Charlie$_2, \ldots,$ Charlie$_{n-m}$. In the same time, Alice requires that only all the n agents cooperate together can they obtain her secret message. The most steps of the multi-party QSS scheme are the same as that in the three-party QSS scheme, just when the Bob$_1$ and Charlie$_1$ have finished the step (3), they will send the photons to the Bob$_2$ and Charlie$_2$ respectively, instead of sending the photons to Alice, also for preventing the dishonest agent from eavesdropping freely with an opaque attack [1], Bob$_1$ and Charlie$_1$ prepare two sets of decoy photons [4, 5] which are sufficient for statistical analysis of eavesdropping as the sample sets respectively, the position of each decoy photon is distributed randomly in the sequence. Bob_1 and Charlie_1 tells Bob_2 and Charlie_2 the positions of the decoy photons respectively, Bob_2 and Charlie $_2$ measure the decoy photons by choosing one of the three MBs Z, X and Y randomly, Bob_1 and Charlie_1 compare the results announced by Bob_2 and Charlie_2, if the error rates are lower than the threshold, the protocol will proceeds. Otherwise, they will abandon the outcomes transmitted and repeat the quantum communication from the beginning. While all the Bob_i and Charlie_j $(i = 2, \ldots, m, j = 2, \ldots, n - m)$ have finished the operations as above, Alice will pick out randomly a sufficiently large subset of the outcomes from the Bell-basis measurements on the entangled quantum systems, and analyzes its error rate. Alice randomly requires $\text{Bob}_1, \ldots, \text{Bob}_m$ first publish their operations and then $\text{Charlie}_1, \ldots, \text{Charlie}_{n-m}$, or vice versa. Alice publics the initial states of the N non-orthogonal entangled photons, only all the n agents cooperate together can they obtain Alice's secret message.

Up to now, we have generalized our three-party QSS protocol to multi-party QSS scheme. The security of the proposed multi-party QSS scheme is the same as the security of three parties QSS scheme, only all the n agents cooperate can they recover Alice's secret message.

In conclusion, we have analyzed the security problems existed in two efficient high-capacity QSS schemes and then proposed a secure three-party protocol for secret sharing using two-particle quantum entanglement. In the protocol, the sharing of the secret is accomplished by coding of two-particle quantum entanglement states but not the coding of some special discrete unitary operations. The scheme has a high intrinsic efficiency for qubits and a high capacity. We also give a method to generalize our proposed scheme to arbitrary multi-party scheme.

Acknowledgements The authors would like to thank the anonymous reviewers and editor for their comments that improved the quality of this paper. The first author is grateful to Dr. Rong-Hua Li for her encouragement. This work was supported by the National Science Foundation of China under Grant No. 60773135, No. 90718007 and No. 60970140.

References

1. Deng, F.G., Li, X.H., Zhou, H.Y.: Phys. Lett. A **372**, 1957 (2008). doi:10.1016/j.physleta.2007.10.066
2. Hillery, M., Bužek, V., Berthiaume, A.: Phys. Rev. A **59**, 1829 (1999)
3. Karlsson, A., Koashi, M., Imoto, N.: Phys. Rev. A **59**, 162 (1999)
4. Yang, Y.G., Wen, Q.Y.: Phys. Lett. A **373**, 396 (2009). doi:10.1016/j.physleta.2008.10.055
5. Deng, F.G., Li, X.H., Zhou, H.Y.: Phys. Lett. A **373**, 399 (2009). doi:10.1016/j.physleta.2008.10.056
6. Deng, F.G., Li, X.H., Zhou, H.Y.: arXiv:0705.0279 [quant-ph] (2007)
7. Li, C.Y., Zhou, H.Y., Wang, Y., et al.: Chin. Phys. Lett. **22**, 1049 (2005)
8. Li, X.H., Deng, F.G., Li, C.Y., et al.: J. Korean Phys. Soc. **49**, 1353 (2006)
9. Deng, F.G., Long, G.L., Liu, X.S.: Phys. Rev. A **68**, 042317 (2003)
10. Deng, F.G., Long, G.L.: Phys. Rev. A **69**, 052319 (2004)
11. Lo, H.K., Chau, H.F., Ardehali, M.: J. Cryptology **18**, 133 (2005)