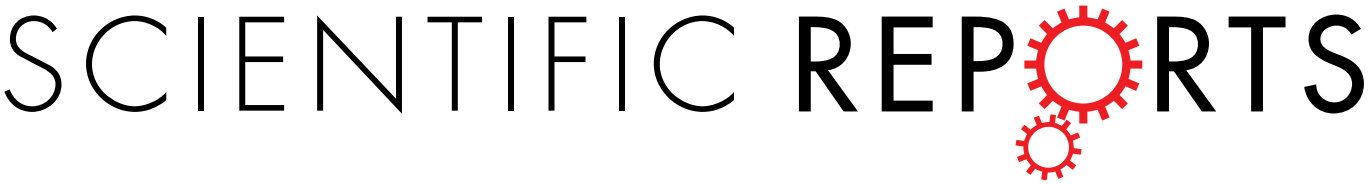

OPEN

Security of a kind of quantum secret sharing with entangled states

Received: 4 January 2017
Accepted: 12 April 2017
Published online: 30 May 2017

Tian-Yin Wang[1,2,3], Ying-Zhao Liu[2], Chun-Yan Wei[2], Xiao-Qiu Cai[2] & Jian-Feng Ma[3]

We present a new collusion attack to a kind of quantum secret sharing schemes with entangled states. Using this attack, an unauthorized set of agents can gain access to the shared secret without the others' cooperation. Furthermore, we establish a general model for this kind of quantum secret sharing schemes and then give some necessary conditions to design a secure quantum secret sharing scheme under this model.

The concept of secret sharing schemes was firstly introduced by Shamir[1] and Blakely[2], respectively, in which a secret S is divided into n pieces in such a way that S can be easily reconstructed from any k pieces, but even complete knowledge of $k-1$ pieces reveals absolutely no information about S. The unique technique of secret sharing enables the construction of robust key management schemes or any other cryptographic schemes that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces[1].

In contrast to classical secret sharing, the security of quantum secret sharing (QSS) is based on the fundamental principles of quantum physics, which allows agents (holders of the shared secret) to share a secret securely even in the presence of an opponent Eve with unlimited computing ability[3]. Owning to the advantage of unconditional security, QSS has attracted much attention and a lot of schemes have been presented both in theoretical and experimental aspects[4–12].

Although an opponent Eve must compromise at least k agents to learn the shared secret, and corrupt more than $n-k$ shares to destroy the information in a (k, n) threshold sharing secret scheme, she has the entire life-time of the secret to mount these attacks. Gradual and instantaneous break-ins into a subset of agents over a long period of time may be feasible for her. Accordingly, the protection provided by traditional secret sharing may be not sufficient. A natural defense is to periodically refresh the secrets, but it is not always possible in some cases such as cryptographic master key and proprietary trade-secret information. As a result, what is actually required to protect the secret of the information is to periodically renew the shares without changing the secret, in such a way that any information learned by Eve about individual shares becomes obsolete after renewing the shares. This is so-called proactive secret sharing, which was firstly introduced by Herzberg *et al.*[13] So far, many proposals for proactive secret sharing have been given in classical cryptography[14,15].

Based on two-step quantum secure direct communication (QSDC)[16], a proactive QSS scheme (named QD-scheme hereafter) was proposed recently[17], in which a dealer Alice prepares Einstein-Podolsky-Rosen (EPR) pairs and then sends all the second particles to every agent in sequence, and the agents code their shares on these particles with four local unitary operations. However, Gao and Wang show that the QD-scheme is not secure in the sense that dishonest participants may collaborate to eavesdrop the secret of the dealer without introducing any error[18].

In this paper, we take the QD-scheme as an example and present a new collusion attack to this kind of QSS scheme based on QSDC, whereby an unauthorized set (the first agent and the last one) can gain access to the dealer's secret without the others' cooperation if they collude with each other. Then we establish a general model for this kind of QSS schemes. Finally, we give some necessary conditions to design a secure QSS scheme under this model.

[1]School of Computer Science and Technology, Xidian University, Xian, 710071, China. [2]School of Mathematical Science, Luoyang Normal University, Luoyang, 471934, China. [3]School of Network and Information Security, Xidian University, Xian, 710071, China. Correspondence and requests for materials should be addressed to X.-Q.C. (email: xiaoqiucai@aliyun.com)

Results

The QD-scheme. In the QD-scheme, $n+1$ participants, i.e., the dealer Alice and n agents Bob_1, Bob_2, …, Bob_n are involved. Suppose that Alice wants to share a secret S among the n agents. The QD-scheme includes the following three phases[17].

Distribution

(1) Alice generates m EPR pairs $|\Psi\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i,y_i}$, $x_i, y_i \in \{0, 1\}$, $i = 1, 2, \ldots, m$, each is randomly in one of the four Bell states:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),\ |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle),$$
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle),\ |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle),$$

hereafter the first particles of all EPR pairs $|\Psi\rangle$ are called $[x]$ sequence and the second are called $[y]$ sequence. Then she prepares some decoy particles $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (BB84 particles) and inserts them into the $[y]$ sequence. After that, she sends the $[y]$ sequence to Bob_1, and keeps a record of the insertion positions and initial states of the decoy particles.

(2) After confirming that Bob_1 has received the $[y]$ sequence, Alice publicly announces the position of the decoy particles and asks Bob_1 to measure these particles with the base $Z = \{|0\rangle, |1\rangle\}$ or $X = \{|+\rangle, |-\rangle\}$ according to their bases and publish his measurement results. Then Alice computes the error rate through comparing the measurement results to the initial states. If the error rate exceeds the preset threshold, she asks Bob_1 to abort the process and start a new one. Otherwise, they continue to perform the protocol.

(3) Bob_1 randomly chooses a binary number $K^1 = (u_1^1, v_1^1, \ldots, u_m^1, v_m^1)$ as his private key and then performs the unitary operation $U_{u_i^1,v_i^1}$ on the i th particle in the $[y]$ sequence, $i = 1, 2, \ldots, m$, where $U_{u_i^1,v_i^1}$ is one of the Pauli operators:

$$U_{00} = I = |0\rangle\langle 0| + |1\rangle\langle 1|,\ U_{01} = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$
$$U_{10} = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|,\ U_{11} = i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|.$$

Note that the $[y]$ sequence is denoted as $[y_1]$ sequence after Bob_1's operation hereafter. Then he prepares some BB84 particles and inserts them into the $[y_1]$ sequence. After that, he sends the $[y_1]$ sequence to Bob_2.

(4) Bob_2 does the similar actions as Bob_1. This process is continued until Bob_n sends $[y_n]$ sequence to Alice.

(5) After confirming the security of the $[y_n]$ sequence, Alice performs a Bell measurement on each EPR pair of the sequence $|\Psi'\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i',y_i'}$, where $|\Psi'\rangle$ is the evolution of $|\Psi\rangle$ after all the agents' operations. According to the measurement outcome, she gets the secret S by computing

$$S = (x_1, y_1, \ldots, x_m, y_m) \oplus (x_1', y_1', \ldots, x_m', y_m'), \tag{1}$$

hereafter $\oplus$ denotes the bitwise exclusive OR.

Updating. (I) In the first updating period, Bob_1 randomly generates m EPR pairs $|\overline{\Psi}\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{\overline{x}_i,\overline{y}_i}$, $\overline{x}_i, \overline{y}_i \in \{0, 1\}$, $i = 1, 2, \ldots, m$, the first and the second particles of them are called $[\overline{x}]$ sequence and $[\overline{y}_1]$ sequence, respectively. Then Bob_1 sends the $[\overline{y}_1]$ sequence to Bob_2 after similarly processing in the distribution phase.

(II) Bob_2 randomly chooses a binary number $C^2 = (a_1^2, b_1^2, \ldots, a_m^2, b_m^2)$ and performs the unitary operation $U_{a_i^2,b_i^2}$ on the i th particle in the $[\overline{y}_1]$ sequence, $i = 1, 2, \ldots, m$. Then Bob_2 updates his key by computing $K^2 \oplus C^2$.

(III) The $[\overline{y}_1]$ sequence is denoted as $[\overline{y}_2]$ sequence after Bob_2's actions. Bob_2 sends the $[\overline{y}_2]$ sequence to Bob_3, and Bob_3 performs the similar operation on the $[\overline{y}_2]$ sequence as Bob_2. This process is continued until Bob_n sends $[\overline{y}_n]$ sequence to Bob_1.

(IV) After confirming the security of the $[\overline{y}_n]$ sequence, Bob_1 performs a Bell measurement on each EPR pair of $|\overline{\Psi}'\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{\overline{x}_i',\overline{y}_i'}$, where $|\overline{\Psi}'\rangle$ is the evolution of $|\overline{\Psi}\rangle$ after the agents' operations. After that, Bob_1 updates his key as $K^1 \oplus C^1$, where

$$C^1 = (\overline{x}_1, \overline{y}_1, \ldots, \overline{x}_m, \overline{y}_m) \oplus (\overline{x}_1', \overline{y}_1', \ldots, \overline{x}_m', \overline{y}_m'). \tag{2}$$

(V) After the above steps, the first updating period is over. When the second updating period starts, Bob_2 does the similar actions as Bob_1. The other updating is performed periodically in the same way.

Recovery. To recover the secret S, a trusted DC (designed combiner by the agents) is needed.

(A) DC randomly generates m EPR pairs $|\widehat{\Psi}\rangle = \otimes_{i=1}^{m} |\widehat{\Psi}\rangle_{\widehat{x}_i,\widehat{y}_i}$.

(B) The $[\widehat{y}]$ sequence is sent to each agent Bob_j $(j = 1, 2, \ldots, n)$ in turn. Bob_j performs the unitary operation $U_{u_i^j,v_i^j}$ on the i th $(i = 1, 2, \ldots, m)$ particle in the $[\widehat{y}]$ sequence according to his key $K^j = (u_1^j, v_1^j, \ldots, u_m^j, v_m^j)$.

(C) After finishing his operations, Bob_n sends the $[\widehat{y}]$ sequence to DC.

(D) When receiving the $[\widehat{y}]$ sequence, DC performs a Bell measurement on each EPR pair of $|\widehat{\Psi'}\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{\widehat{x_i'},\widehat{y_i'}}$, where $|\widehat{\Psi'}\rangle$ is the new state of $|\widehat{\Psi}\rangle$ after the agents' operations. Then DC recovers the secret S by computing

$$S = (\widehat{x_1}, \widehat{y_1}, \ldots, \widehat{x_m}, \widehat{y_m}) \oplus (\widehat{x_1'}, \widehat{y_1'}, \ldots, \widehat{x_m'}, \widehat{y_m'}). \tag{3}$$

By the property of the EPR pairs and four encoding operations, we can know $|\Psi'\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i',y_i'} = \otimes_{i=1}^{m} |\Psi\rangle_{x_i \oplus u_i^1 \oplus \cdots \oplus u_i^n, y_i \oplus v_i^1 \oplus \cdots \oplus v_i^n}$, which means $x_i' = x_i \oplus u_i^1 \oplus \cdots \oplus u_i^n$ and $y_i' = y_i \oplus v_i^1 \oplus \cdots \oplus v_i^n$. So, $S = (x_1, \underline{y_1}, \ldots, x_m, \underline{y_m}) \oplus (x_1', y_1', \ldots, x_m', y_m') = K^1 \oplus K^2 \oplus \cdots \oplus K^n$. Similarly, we can get $C^1 = (\overline{x_1}, \overline{y_1}, \ldots, \overline{x_m}, \overline{y_m}) \oplus (x_1', y_1', \ldots, x_m', y_m') = C^2 \oplus \cdots \oplus C^n$. Clearly, after the first updating period of keys, the shared secret is $K^1 \oplus C^1 \oplus K^2 \oplus C^2 \oplus \cdots \oplus K^n \oplus C^n = K^1 \oplus K^2 \oplus \cdots \oplus K^n = S$. The other updating periods of keys are similar to the first, and thus the shared secret S is not changed after the updating of keys. Therefore, the recovered secret by equation (3) is $(\widehat{x_1}, \widehat{y_1}, \ldots, \widehat{x_m}, \widehat{y_m}) \oplus (\widehat{x_1'}, \widehat{y_1'}, \ldots, \widehat{x_m'}, \widehat{y_m'}) = K^1 \oplus K^2 \oplus \cdots \oplus K^n = S$ by deducting.

The collusion scheme. As we know, the security of QSS requires that only an authorized set of agents can recover the secret S distributed by the dealer, but any unauthorized set of agents can gain access to nothing about it. Consequently, the main goal for the security of QSS is to prevent dishonest agents from deceiving. Nevertheless, the dishonest agents have a lot of advantages in contrast to outside opponents. On the one hand, they know partial information legally. On the other hand, they can tell a lie in the process of eavesdropping check to avoid introducing errors. Therefore, it is more complicated to analyse the security of QSS schemes compared with two-party cryptographic schemes[19–21].

From the QD-scheme, it can be seen that the distribution phase, the updating phase and the recovery phase are very similar, all of them are based on QSDC. Here we take the distribution phase as an example to show its insecurity. In the distribution phase, the $[y]$ sequence prepared by Alice is transferred among n agents Bob_1, Bob_2,…, Bob_n in turn, and when it is sent to an agent Bob_j ($j = 1, 2, \ldots, n$), Bob_j encodes his share $K^j = (u_1^j, v_1^j, \ldots, u_m^j, v_m^j)$ to the $[y]$ sequence by performing pauli operations $U_{u_i^j, v_i^j}$, $i = 1, 2, \ldots, m$. Although each agent Bob_j ($j = 1, 2, \ldots, n$) checks the security of quantum channel between him and the previous agent Bob_{j-1}, and Alice checks the security of quantum channel between her and the agent Bob_n, there is also a chance for dishonest agents to deceive. Specifically, the first agent Bob_1 and the last agent Bob_n, an unauthorized set of agents, can gain access to the shared secret S without the cooperation of any other agent if they collude with each other by the following collusion attack.

(i) In the distribution phase, Bob_1 prepares m EPR pairs $|\Psi''\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i'', y_i''}$ in advance, $x_i'', y_i'' \in \{0, 1\}$, $|\Psi\rangle_{x_i'', y_i''} \in \{|\Psi_{00}\rangle, |\Psi_{01}\rangle, |\Psi_{10}\rangle, |\Psi_{11}\rangle\}$, $i = 1, 2, \ldots, m$. The first particles of all EPR pairs $|\Psi''\rangle$ are called $[x'']$ sequence and the second are called $[y'']$ sequence. Then he sends the initial Bell state information $(x_1'', y_1'', \ldots, x_m'', y_m'')$ and the $[x'']$ sequence to Bob_n.

(ii) As does in Steps (2) and (3), Bob_1 performs his actions faithfully except that he inserts BB84 decoy particles into the $[y'']$ sequence and sends it to Bob_2 instead of the $[y_1]$ sequence, and sends the real $[y_1]$ sequence to Bob_n.

(iii) When Bob_n receiving the fake $[y_{n-1}]$ sequence from Bob_{n-1}, i.e., $[y'']$ sequence, he performs a Bell measurement on each EPR pair of $|\Psi'''\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i'', y_i''}$ after checking the security of quantum channel between him and Bob_{n-1}, where $|\Psi'''\rangle$ is the evolution of $|\Psi''\rangle$ after the agents' operations.

(iv) As does in Step (4), Bob_n randomly chooses a binary number $K^n = (u_1^n, v_1^n, \ldots, u_m^n, v_m^n)$ as his private key. Then he computes

$$\begin{aligned} S''' &= (x_1'', y_1'', \ldots, x_m'', y_m'') \oplus (x_1''', y_1''', \ldots, x_m''', y_m''') \\ &= (x_1'''', y_1'''', \ldots, x_m'''', y_m''''). \end{aligned} \tag{4}$$

After that, he performs the operation $U_{u_i^n, v_i^n} U_{x_i''', y_i''''}$ on the i th particle in the real $[y_1]$ sequence received from Bob_1, $i = 1, 2, \ldots, m$.

(v) As does in Step (4), after inserting BB84 decoy particles into $[y_n]$ (the real $[y_1]$ sequence after Bob_n's operation), Bob_n sends it to Alice.

(vi) After the completion of distribution, Bob_1 and Bob_n can recover the shared secret S at any time by computing

$$\tilde{S} = K^1 \oplus S'''' \oplus K^n. \tag{5}$$

Now let us prove the effectiveness of joint attack. Firstly, it is evident that this deception introduces no error and therefore cannot be detected in the process of eavesdropping check from the above attack. Secondly, the EPR pairs generated by Bob_1 in Step (i) are $|\Psi''\rangle = \otimes_{i=1}^{m} |\Psi\rangle_{x_i'', y_i''}$, and the private keys generated by Bob_2, Bob_3,…, Bob_{n-1} are also $K^2 = (u_1^2, v_1^2, \ldots, u_m^2, v_m^2)$, $K^3 = (u_1^3, v_1^3, \ldots, u_m^3, v_m^3)$, …, $K^{n-1} = (u_1^{n-1}, v_1^{n-1}, \ldots, u_m^{n-1}, v_m^{n-1})$, respectively. By the property of EPR pairs and Pauli operators, the EPR pairs $|\Psi''\rangle$ will evolve in the state

$$\begin{aligned}|\Psi'''\rangle &= \otimes_{i=1}^{m}|\Psi\rangle_{x_i'''y_i'''} \\ &= \otimes_{i=1}^{m}|\Psi\rangle_{x_i''\oplus u_1^2\oplus u_1^3\oplus\cdots\oplus u_1^{n-1},y_i''\oplus v_1^2\oplus v_1^3\oplus\cdots\oplus v_1^{n-1}}\end{aligned} \tag{6}$$

after the unitary operations of Bob_2, Bob_3, …, Bob_{n-1}. Therefore, we can get

$$S''' = K^2 \oplus K^3 \oplus \cdots \oplus K^{n-1}, \tag{7}$$

which means

$$\tilde{S} = K^1 \oplus K^2 \oplus \cdots \oplus K^n. \tag{8}$$

Finally, after the unitary operations of Bob_1 and Bob_n, the EPR pairs $|\Psi\rangle = \otimes_{i=1}^{m}|\Psi\rangle_{x_i,y_i}$ prepared by Alice will evolve in the state

$$\begin{aligned}|\Psi'\rangle &= \otimes_{i=1}^{m}|\Psi\rangle_{x_i',y_i'} \\ &= \otimes_{i=1}^{m}|\Psi\rangle_{x_i\oplus u_1^1\oplus x_i'''\oplus u_1^n,y_i\oplus v_1^1\oplus y_i'''\oplus v_1^n} \\ &= \otimes_{i=1}^{m}|\Psi\rangle_{x_i\oplus u_1^1\oplus u_1^2\oplus\cdots\oplus u_1^n,y_i\oplus v_1^1\oplus v_1^2\oplus\cdots\oplus v_1^n}\end{aligned} \tag{9}$$

which means that the secret S also satisfies

$$S = K^1 \oplus K^2 \oplus \cdots \oplus K^n. \tag{10}$$

Obviously, $\tilde{S} = S$. Additionally, as shown in the QD-scheme[17], the shared secret S is not changed after the updating of keys.

As a result, Bob_1 and Bob_n can gain access to the shared secret S at any time without the others' cooperation if they collude with each other, which is in conflict with the security requirement of QSS that only an authorized set of agents can recover the secret S, but the unauthorized set of agents can gain access to nothing about it.

Noted that Bob_1 and Bob_n also can directly gain access to the shared secret S in the recovery phase if they collude with each other by the similar joint attack.

The proposed model. In this section, let us give a general model for this kind of QSS schemes based on QSDC. Let k be the security parameter. The general procedure for this kind of QSS can be rephrased in the following.

1) Alice prepares m quantum states $|\phi\rangle = \otimes_{i=1}^{m}|\phi\rangle_i$ (two-particle or multi-particle entangled states). Then she takes one particle from each entangled states $|\phi\rangle_i$ to form a travel sequence (named T-sequence hereafter). After that, she prepares $2k$ decoy particles and inserts them into the T-sequence before sending it to Bob_1.

2) When receiving the T-sequence, Bob_1 firstly ascertains whether each particle in the T-sequence is sure a single one or not by the similar methods in refs 22–24. If it is so, Alice tells Bob_1 the initial states and positions of k decoy particles and then Bob_1 checks whether the T-sequence is secure or not by the measurement outcomes on them. If it is secure, for each particle in the T-sequence, Bob_1 chooses two unitary operations U, U' and then performs the operation $U'U$ on it, where U is chosen from a set $\widetilde{U}$ according to his sub-secret K^1 and is used to encode his sub-secret, U' is randomly chosen from a set $\widetilde{U'}$ and is used to encrypt his sub-secret. After that, he also prepares k decoy particles and inserts them into the T-sequence before sending it to Bob_2. In other cases, he aborts the protocol and asks Alice to restart.

3) Bob_2 performs the similar actions as Bob_1 does in Step 2) after receiving the T-sequence. This process is repeated until Bob_n sends the T-sequence to Alice.

4) When receiving the T-sequence, Alice also firstly ascertains whether each of them is sure a single particle or not. If it is so, she announces the remaining k decoy particles' positions to the agents and requires them to send their unitary operations $U'U$ performed on these particles to her. Then she judges whether the T-sequence is attacked or not by the measurement outcomes on the k decoy particles. If it is secure, she requires all agents to send her their encryption operations U' and then she performs a projective measurement on each entangled states $|\phi\rangle_i$, $i = 1, 2, \ldots, m$. According to the measurement outcomes and initial states, she can obtain the secret $S = K^1 \oplus K^2 \oplus \cdots \oplus K^n$. In other cases, she aborts the protocol.

By running this program, Alice makes n agents share a secret S that can be reconstructed if and only if they cooperate together.

The proposed conditions. Now let us study the necessary conditions to design a secure QSS scheme under this model. For QSS, the security mainly includes two aspects: the agents' encoding operations (sub-secrets) and the shared secret S.

Firstly, let us analyse the conditions that nobody can obtain a agent's sub-secret except himself. To get an agent Bob_i's sub-secret K^i, there are generally three ways for an opponent Eve: one is intercepting the T-sequence and then learning some information by directly measuring each particle in the T-sequence. The second is sending fake particles to Bob_i as the T-sequence and then intercepting them when they are sent to Bob_{i+1} by Bob_i. After that, Eve tries to learn some information by measuring these fake particles later. The last is sending multi-particle signal to Bob_i, i.e., Trojan horse attack: Eve inserts one or multi spy particles, an invisible particle, or a delay one in each particle of the T-sequence when it is sent to Bob_i, and captures the spy particles when they are sent to the next agent Bob_{i+1} and gets some information by measuring them later. This kind of attacks were introduced in

2005 by Deng *et al.*[22] and have been used to break through a lot of cryptographic schemes[23,24], and therefore we must seriously consider how to deal with them here. Let us analyse whether it is feasible or not by the first way, it can be seen from the proposed model that nobody knows the initial state of $|\phi\rangle_i$ except Alice. In addition, Eve only has one particle of each entangled state $|\phi\rangle_i$. Accordingly, she can learn no information on Bob_i's encoding operation U according to the principle of quantum measurement, which means that nobody can know an agent's sub-secret by this way. If Eve wants to steal Bob_i's sub-secret K^i by the second way, she must escape the security check on the T-sequence between Bob_i and Bob_{i-1} firstly. It is impossible for an outside opponent Eve to do that except with exponentially small probability, but it is not a problem for an inside opponent Bob_{i-1}. Nevertheless, if Bob_{i-1} wants to steal Bob_i's sub-secret K^i by directly measuring these fake particles, he must have the ability to discriminate the encoding operation U from the set $\widetilde{U}$ after the encrypting operation U', which is equivalent to discriminate the unitary operation $U'U$ is in which one of the sets $\widetilde{U'}U, U \in \widetilde{U}$, where

$$\widetilde{U'}U = \{U'U | U' \in U'\}. \tag{11}$$

Nevertheless, the unitary operation $U'U$ is performed on a fake particle (a single particle or one qubit of an entangled state) only once, if the two sets $\widetilde{U'}$ and $\widetilde{U}$ are selected properly, Bob_{i-1} will not discriminate the unitary operation $U'U$ is in which one of the sets $\widetilde{U'}U, U \in \widetilde{U}$ only by measuring the fake particle. To get rid of this restriction, Bob_{i-1} can measure these fake particles after Bob_i publishes his encryption operation U' in Step 4), but it requires his deception must escape the security check between Bob_{i+1} and Bob_i in Step 3), and Alice's security check in Step 4). Obviously, if Bob_{i+1} is also dishonest, that is he colludes with Bob_{i-1}, in this case Bob_{i-1}'s deception can easily escape the security check between Bob_{i+1} and Bob_i. To escape Alice's security check in Step 4), the teleportation attack was proposed in 2008[20,25,26], but how to prevent this attack will be analysed in the following paragraph. To steal Bob_i's sub-secret by the last way, Eve's deception must escape Bob_i's multi-particle signal check. Nevertheless, it is very difficult because this kind of attacks can be prevented by technical measures. Li *et al.*[23] gave a way to filter out invisible photons. Specifically, Bob_i can add a filter in his laboratory first. All photon pulses should pass through his filter first. Only wavelengths close to the operating wavelength can be let in. Thus, Eve's invisible photons can be filtered out by using the filter. Furthermore, if Eve's spy photons cannot be filtered out, Deng *et al.*[22] gave a feasible way to detect them. Specifically, Bob_i chooses some sample signals and splits them with a photon number splitter, and then measures the two signals with Z-basis or X-basis randomly. If both the measurements have an outcome, Bob_i can judge the quantum signal is a multi-photon signal. Therefore, if Bob_i has the ability of discriminating whether each quantum signal only contains a single particle, this way will not be feasible any longer.

Secondly, let us analyse the conditions that nobody can recover the shared secret S except that all the agents cooperate together. Since the shared secret is the module sum of the agents' sub-secrets, i.e., $S = K^1 \oplus K^2 \oplus \cdots \oplus K^n$, the conditions of protecting sub-secrets should be firstly satisfied to maintain its security. To gain access to the shared secret S, one possible way is stealing all the agents' sub-secrets K^1, K^2, …, K^n, whereby the difficulties have been analysed in the above paragraph. Another possible way is using teleportation attack. The basic principle of this attack can be described as the following. In step 2), a dishonest agent (e.g., Bob_1) sends $m+k$ fake particles (each of them is one qubit of a Bell state) instead of the T-sequence to the next agent. At the same time, he stores the real T-sequence and the remaining $m+k$ qubits of the Bell states in his quantum database. In step 4), when Alice announces the remaining k decoy particles' positions, Bob_1 performs a teleportation measurement on the corresponding original decoy particle and the remaining qubit of the corresponding Bell state. By this way, the state of the corresponding original decoy particle can be teleported to the fake one (i.e., the one qubit of the corresponding Bell state sent to Alice in the end) by the principle of teleportation except the lack of a unitary operation, and therefore the dishonest agent can successfully hide his replacing deception by sending the corresponding unitary operation to Alice. The condition to prevent this attack under single particle model has been deeply discussed in ref. 27. By similar analysis, we can find this condition is also suitable for this model. Specifically, the condition is $\overline{U} \nsubseteq \langle \widetilde{U}, \widetilde{U'} \rangle$, where $\overline{U}$ denotes a unitary operation set that consists of the unitary operations corresponding to the teleportation measurement outcomes, and $\langle \widetilde{U}, \widetilde{U'} \rangle$ represents a unitary operation set, which consists of all the elements in $\widetilde{U}$ and $\widetilde{U'}$ and all the possible products of them.

Up to now, we have clarified the conditions to prevent all the present attacks under the proposed model, i.e., (i) the dealer Alice and every agent have the ability to discriminate whether each quantum signal only contains a single particle; (ii) the unitary operation $U'U$ ($U \in \widetilde{U}$, $U' \in \widetilde{U'}$) cannot be discriminated in the set $\widetilde{U'}U$ when it is performed only on a single particle or one qubit of any entangled state; (iii) $\overline{U} \nsubseteq \langle \widetilde{U}, \widetilde{U'} \rangle$.

Discussion

Using the given conditions, we can judge whether a QSS scheme under the proposed model is secure or not, i.e., if a QSS scheme under the proposed model does not satisfy all the conditions i)-iii), this scheme must be not secure, e.g., the QD-scheme is vulnerable to a lot of attacks because it satisfies none of the conditions i), ii) and iii); otherwise, this scheme is immune to all the present attacks in the sense that these attacks will be detected by Alice in the process of eavesdropping detection with probability p. The probability p can be computed by the following equation

$$p = 1 - (1 - p_e)^k, \tag{12}$$

where p_e denotes the least probability that an opponent introduces an error when a decoy particle is checked. Assume a QSS scheme under the proposed model satisfies all the conditions i)-iii), the least probability p_e only depends on the set $\widetilde{U}'\widetilde{U}$ since the multi-particle signal attack and the invisible particle attack have been excluded by the condition i), and thus the least probability p_e is no less than $1/r$ since at least one of the unitary operations corresponding to teleportation measurement cannot be properly announced by the condition iii), where r is the element number of the set $\overline{U}$.

From Eq. (12), it can be seen that p is exponentially close to 1 with the increase of the security parameter k, which means that the opponent's attack will be detected by Alice with probability exponentially close to 1.

It is evident that if the opponent's attack is detected by Alice, he/she will get no information on the shared secret S. Nevertheless, Alice cannot distinguish which one is the attacker when she finds that there is deceiving among the agents in the process of eavesdropping check, which will induce that a dishonest agent may like to take the risk to cheat, because if the cheating is not detected then he will be benefited, while even if it is detected, he will be not blamed by Alice. Furthermore, when k is very small, the dishonest agent may have a chance to escape Alice's detection.

Using the given conditions, we also can judge whether a QSS scheme is not secure if it is similar to the present model, e.g., the QSS scheme in ref. 28 is not secure since it does not satisfy the condition (iii). Nevertheless, we cannot give a full classification on the security of previous schemes by the conditions (i)-(iii) because most of them are far different from the present model.

References

1. Shamir, A. How to shair a secret. *Commun. ACM* **22**(11), 612–613, doi:10.1145/359168.359176 (1979).
2. Blakely, G. Safeguarding cryptographic keys. *Proc. the National Computer Conference* (pp. 313–317. AFIPS, Montvale: IEEE Press: New York, 1979).
3. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**(3), 1829–1834, doi:10.1103/PhysRevA.59.1829 (1999).
4. Tittel, W., Zbinden, H. & Gisin, N. Experimental demonstration of quantum secret sharing. *Phys. Rev. A* **63**(4), 042301, doi:10.1103/PhysRevA.63.042301 (2001).
5. Xiao, L. *et al*. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **69**(5), 052307, doi:10.1103/PhysRevA.69.052307 (2004).
6. Schmid, C. *et al*. Experimental single qubit quantum secret sharing. *Phys. Rev. Lett.* **95**(23), 230505, doi:10.1103/PhysRevLett.95.230505 (2005).
7. Wang, T. Y. *et al*. An efficient and secure multiparty quantum secret sharing scheme based on single photons. *Opt. Commun.* **281**(24), 6130–6134, doi:10.1016/j.optcom.2008.09.026 (2008).
8. Sun, Y. *et al*. Multiparty quantum secret sharing based on Bell measurement. *Opt. Commun.* **282**(17), 3647–3651, doi:10.1016/j.optcom.2009.05.054 (2009).
9. Yang, Y. G. *et al*. Member expansion in quantum (t, n) threshold secret sharing schemes. *Opt. Commun.* **284**(13), 3479–3482, doi:10.1016/j.optcom.2011.03.017 (2011).
10. Shi, R. H. & Zhong, H. Multiparty quantum secret sharing with the pure entangled two-photon states. *Quant. Inf. Process* **11**(1), 161–169, doi:10.1007/s11128-011-0239-9 (2012).
11. Yang, Y. H. *et al*. Quantum secret sharing via local operations and classical communication. *Sci. Rep* **5**, 16967, doi:10.1038/srep16967 (2015).
12. Lu, H. *et al*. Secret sharing of a quantum state. *Phys. Rew. Lett* **117**(3), 030501, doi:10.1103/PhysRevLett.117.030501 (2016).
13. Herzberg, A. *et al*. Proactive secret sharing or how to cope with perpetual leakage. *Proc. the 15th Annual International Cryptology Conference on Advances in Cryptology* (pp. 339–352. Springer: London, 1995).
14. Guo, Y. B. & Ma, J. F. Proactive secret sharing in asynchronous networks with unreliable links. *Acta Electron. Sin* **32**(3), 399–403 (2004).
15. Hyun, S. I., Shin, S. H. & Yoo, K. Y. A proactive secret image sharing scheme over GF(28). *J. Korea Multimedia Society* **16**(5), 577–590, doi:10.9717/kmms.2013.16.5.577 (2013).
16. 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* **68**(4), 042317, doi:10.1103/PhysRevA.68.042317 (2003).
17. Qin, H. W. & Dai, Y. W. Proactive quantum secret sharing. *Quant. Inf. Process* **14**(11), 4237–4244, doi:10.1007/s11128-015-1106-x (2015).
18. Gao, G. & Wang, Y. Comment on Proactive quantum secret sharing. *Quant. Inf. Process* **16**, 74, doi:10.1007/s11128-017-1521-2 (2017).
19. Qin, S. J. *et al*. Cryptanalysis of the Hillery-Bužek-Berthiaume quantum secret-sharing protocol. *Phys. Rev. A* **76**(6), 062324, doi:10.1103/PhysRevA.76.062324 (2007).
20. Wang, T. Y. *et al*. Cryptanalysis and improvement of multiparty quantum secret sharing schemes. *Phys. Lett. A* **373**(1), 65–68, doi:10.1016/j.physleta.2008.11.004 (2008).
21. Wang, T. Y. & Li, Y. P. Cryptanalysis of dynamic quantum secret sharing. *Quant. Inf. Process* **12**(5), 1991–1997, doi:10.1007/s11128-012-0508-2 (2013).
22. Deng, F. G. *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **72**(4), 044302, doi:10.1103/PhysRevA.72.044302 (2005).
23. Li, X. H., Deng, F. G. & Zhou, H. Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A* **74**(5), 054302, doi:10.1103/PhysRevA.74.054302 (2006).
24. Cai, Q. Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **351**(1–2), 23–25, doi:10.1016/j.physleta.2005.10.050 (2006).
25. Gao, F., Wen, Q. Y. & Zhu, F. C. Teleportation attack on the QSDC protocol with a random basis and order. *Chin. Phys. B* **17**(9), 3189–3194, doi:10.1088/1674-1056/17/9/006 (2008).
26. Wang, T. Y. *et al*. Analysis and improvement of mulparty controlled quantum secret direct communication protocol. *Acta Phys. Sin* **57**(12), 7452–7456 (2008).
27. Wang, T. Y. & Wen, Q. Y. Security of a kind of quantum secret sharing with single photons. *Quant. Inf. & Comput* **11**(5–6), 434–443 (2011).
28. Zhang, Z. J. *et al*. Multiparty quantum secret sharing based on the improved Boström-Felbinger protocol. *Opt. Commun.* **269**(2), 418–422, doi:10.1016/j.optcom.2006.08.021 (2007).

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos 61572246, 61602232, 61202317), the National Key Research and Development Plan of China (Grant No. 2016YFE0104600), the Plan for Scientific Innovation Talents of Henan Province (Grant No. 164100510003), and the Key Scientific Research Project in Universities of Henan Province (Grant Nos 16A520021, 16A120007).

Author Contributions

T.Y., C.Y. and X.Q. present the collusion scheme and establish the model for the QSS schemes based on QSDC. T.Y., X.Q. and J.F. give the conditions to design a secure QSS scheme under this model. T.Y. and X.Q. write the main manuscript text. All authors reviewed the manuscript.

Additional Information

Competing Interests: The authors declare that they have no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.