Quantum Inf Process (2016) 15:1689–1701
DOI 10.1007/s11128-015-1221-8

d-Dimensional quantum state sharing with adversary structure

Huawang Qin[1] · **Yuewei Dai**[1]

Received: 5 June 2015 / Accepted: 11 December 2015 / Published online: 23 December 2015

Abstract A quantum secret sharing scheme with adversary structure is proposed. In the proposed scheme, the secret is a d-dimensional quantum state. The dealer can distribute the private keys according to the adversary structure and encode the quantum state through the d-dimensional Pauli unitary operation. The legitimate participants perform the unitary operations on the encrypted quantum state according to their private keys and recover the original quantum state. Compared to the existing QSS schemes, our scheme can be more efficient when only the adversary structure is given.

Keywords Quantum secret sharing · Adversary structure · d-Dimensional · Quantum cryptography

1 Introduction

Since Shamir [1] proposed the first scheme of secret sharing (SS), SS has become a very important topic of cryptography. SS can split the secret information into several parts and distribute them to different participants. Then only the legitimate participants can recover the secret. Quantum secret sharing (QSS) is the combination of SS and quantum scenario. In QSS, the secret (classical information or quantum state) is distributed, transmitted, and recovered through quantum operation, so its security is based on the fundamental principle of quantum physics. Because of the fascinating features different from the classical secret sharing, QSS is attracting more and more interest.

✉ Huawang Qin
qin_h_w@163.com

[1] School of Automatization, Nanjing University of Science and Technology, Nanjing 210094, China

The first QSS scheme was proposed by Hillery et al. [2] in 1999. After that, many kinds of QSS schemes have been proposed [2–29]. The threshold structure is a very important property of QSS. In the existing schemes, most of them are (n, n) structure, that is, the secret can be recovered when all the participants cooperate together, but any part of the participants cannot recover the secret. Some QSS schemes [26,27] are (t, n) structure, that is, any t out of n participants can recover the secret. Compared to the (n, n) structure, the (t, n) structure is more flexible in practice, because that even if some participants are absent the secret can still be recovered. The (n, n) structure can be seen as the special case of the (t, n) structure when $t = n$. Besides the (n, n) and the (t, n) structures, some other QSS schemes are based on the access structure [10,28,29]. In the scheme with access structure, there are some qualified subsets in the participants, and only the qualified subsets can recover the secret. Each qualified subset may have different number of participants, and a participant can belong to several qualified subsets. In practice, the participants may have different rights. For example, the key of a bank safe is shared by some tellers and some managers. The rights of the teller and the manager are different. For this scenario, we cannot design the secret sharing scheme in which any t out of n participants can recover the secret. So the (t, n) structure is not suitable here. However, we can get all the qualified subsets of the participants according to the application requirement, and use the access structure to design this scheme. Therefore, the access structure is more practical than the (t, n) structure, and the (t, n) structure is the special case of the access structure when every qualified subset has t participants.

Sometimes what we can obtain easily is not the access structure, but the adversary structure [30]. The adversary structure is the family of subsets that each cannot recover the secret. The reason of being called adversary structure is that, the secret is safe even if the participants in such subset are all broken by the adversary. For example, a network of secret sharing is composed of many computers, in which some computers have the similar hardware, some computers have the similar operating systems, and some computers have the similar firewalls. The similar properties may lead these computers to be attacked at the same time. So we should try to separate the similar computers into different qualified subsets, that is, put the similar computers into an unqualified subset. In this scenario, we can see that the adversary structure can be obtained directly according to the similarities of computers, but the access structure cannot be obtained easily. We may first convert the adversary structure to the access structure and then adopt the method of access structure to design this scheme. But when the number of the participants is big, the conversion will be complicated. Moreover, an easy adversary structure may generate a complex access structure, and lead the scheme to be inapplicable.

For the above problem, we will propose a QSS scheme with adversary structure in this paper. Our idea is inspired by Zhou's [31] classical secret sharing scheme. Zhou's scheme can only realize the (t, n) structure, but our scheme can realize the adversary structure. The secret of our scheme is a d-dimensional quantum state. By using a novel algorithm, the dealer can distribute the private keys according to the adversary structure. The dealer encodes the quantum state through the d-dimensional Pauli unitary operation. The legitimate participants perform the unitary operations on the encrypted quantum state according to their private keys, and recover the original quantum state. Compared to the existing QSS schemes, the main contribution of our scheme is that the quantum state can be shared according to the adversary structure directly.

The rest of this paper is organized as follows. In Sect. 2, the correlative preliminaries are introduced. Section 3 explicates the design method of the proposed scheme. Section 4 gives a simple example. Section 5 compares our scheme to some of the existing schemes. Section 6 analyzes the security. Finally, in Sect. 7, the conclusion of this paper is given.

2 Preliminaries

2.1 d-Dimensional quantum state and Pauli operation

In d-dimensional Hilbert space, an unknown quantum state can be described as follows.

$$|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$$

where $c_j (j = 0, 1, \ldots, d-1)$ are the complex amplitudes, and satisfy $\sum_{j=0}^{d-1} |c_j|^2{=}1$.

In d-dimensional Hilbert space, the generalized Pauli operation is described as follows.

$$U_{\alpha,\beta} = \sum_{j=0}^{d-1} \omega^{j\alpha} |j\rangle\langle j + \beta|$$

where $\omega = e^{\frac{2\pi i}{d}}, \alpha, \beta \in \{0, 1, \ldots, d-1\}$, and the symbol "+" means the adder modulo d.

2.2 Access structure and adversary structure

We assume that Q is a set including n participants. A qualified subset of Q is that whose participants can recover the original secret. The family of all the qualified subsets is denoted as Γ, which is called the access structure. If $P \in \Gamma$ and for all $P' \subset P$, $P' \notin \Gamma$, then P is termed a minimal qualified subset. The family of all the minimal qualified subsets forms the minimal access structure and is denoted by Γ_0.

An unqualified subset of Q is that whose participants cannot recover the original secret. The family of all the unqualified subsets is denoted as Ω, which is called the adversary structure. If $P \in \Omega$ and for all $P \subset P'$, $P' \notin \Omega$, then P is termed a maximal unqualified subset. The family of all the maximal unqualified subsets forms the maximal adversary structure and is denoted by Ω_0.

3 The proposed scheme

In our scheme, the secret is an unknown d-dimensional quantum state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$. The dealer Alice wants to share $|\Psi\rangle$ among n participants $Q = \{\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n\}$. $\Omega_0 = \{F_1, F_2, \ldots, F_m\}$ is the maximal adversary structure of Q, and F_i $(i = 1, 2, \ldots, m)$ is the maximal unqualified subset. The requirement is that the participants in each F_i cannot recover the quantum state $|\Psi\rangle$, but any qualified subset (F_i plus another participant) can recover the quantum state $|\Psi\rangle$.

3.1 Distribution of private keys

(1) Alice randomly generates m different pairs (α_i, β_i), $i = 1, 2, \ldots, m$, where $\alpha_i, \beta_i \in \{0, 1, \ldots, d-1\}$. Then she generates n same sets $H_i = \{(\alpha_1, \beta_1, 1), (\alpha_2, \beta_2, 2), \ldots, (\alpha_m, \beta_m, m)\}$, $i = 1, 2, \ldots n$.

(2) Alice do the following operations:

```
for ($i = 1; i \leq m; i++$)
{
  $L$ = the number of the participants in $F_i$.
  for ($j = 1; j \leq L; j++$)
  {
      $r$ = the subscript label of NO. $j$ participant in $F_i$. (NO. $j$ participant in $F_i$ is $\mathrm{Bob}_r$.)
      Delete the array $(\alpha_i, \beta_i, i)$ in the set $H_r$.
      }
}
```

(3) Sends $H_i (i = 1, 2, \ldots, n)$ to the participant Bob_i through quantum secure direct communication such as the methods in Refs. [32,33]. H_i is the private key of Bob_i.

The above step (2) is used to delete the array (α_i, β_i, i) of every participant in subset F_i. For example, if $F_2 = \{\mathrm{Bob}_1, \mathrm{Bob}_3, \mathrm{Bob}_4\}$, then the participants Bob_1, Bob_3 and Bob_4 will not have the array $(\alpha_2, \beta_2, 2)$.

3.2 Sharing of d-dimensional quantum state

After the distribution of private keys, Alice can share a d-dimensional quantum state among any qualified subset. We assume the qualified subset is R. Alice does the following steps.

(1) Alice randomly generates a d-dimensional quantum state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$, where $\sum_{j=0}^{d-1} |c_j|^2 = 1$.

(2) Alice performs the unitary operation $U_{A,B} = \sum_{j=0}^{d-1} \omega^{jA} |j\rangle\langle j + B|$ on $|\Psi\rangle$, where $A = d - (\alpha_1 + \alpha_2 + \cdots + \alpha_m)$, $B = d - (\beta_1 + \beta_2 + \cdots + \beta_m)$, and the symbol "+" means the adder modulo d. Then the state $|\Psi\rangle$ becomes $|\Psi'\rangle$.

(3) Alice prepares some decoy particles which are random in the computational Z-basis and X-basis. The Z-basis and X-basis have the following forms:

$$Z = \{|j\rangle, j = 0, 1, \ldots, d-1\}, X = \{|J_j\rangle, j = 0, 1, \ldots, d-1\}, \text{ where } |J_j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kj} |k\rangle.$$

(4) Alice inserts $|\Psi'\rangle$ into the decoy particles. She keeps a record of the insertion position and the initial states of the decoy particles and then sends these particles to the first participant of the qualified subset R.

(5) After confirming that the first participant of R has received the particles, Alice publicly announces the positions and basis of the decoy particles and asks this participant to measure these particles in the Z-basis or X-basis according to their basis. The participant publishes his measurement results. Alice can compute the error rate through comparing the measurement results and the initial states. If the error rate exceeds the threshold value, Alice asks the participant to abort the process and starts a new one. Otherwise, they continue the protocol.

(6) For every array (α_i, β_i, i) in his private key, the first participant of R performs the unitary operation $U_{\alpha_i,\beta_i} = \sum_{j=0}^{d-1} \omega^{j\alpha_i} |j\rangle\langle j+\beta_i|$ on $|\Psi'\rangle$. Then the state $|\Psi'\rangle$ becomes $|\Psi_1'\rangle$. The first participant publishes the "i" of every array (α_i, β_i, i) he used, to show the other participants what array has been used by him.

(7) The first participant of R prepares some decoy particles in the computational Z-basis and X-basis, and inserts $|\Psi_1'\rangle$ into the decoy particles. He sends these particles to the second participant of R. Similarly, the security of their channel is checked through the decoy particles. For every array (α_i, β_i, i) in the private key of the second participant, if (α_i, β_i) has not been used by the first participant, the second participant performs the unitary operation $U_{\alpha_i,\beta_i} = \sum_{j=0}^{d-1} \omega^{j\alpha_i} |j\rangle\langle j+\beta_i|$ on $|\Psi_1'\rangle$. Then the state $|\Psi_1'\rangle$ becomes $|\Psi_2'\rangle$.This process is continued until the last participant of the qualified subset R.

(8) After the last participant of R performed the unitary operations on the quantum state, the quantum state will become the original state $|\Psi\rangle$.

4 Example

In order to explain our scheme more clearly, we will give an example in the following. We assume the dealer Alice wants to share her quantum state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$ among five participants $\{\text{Bob}_1, \text{Bob}_2, \text{Bob}_3, \text{Bob}_4, \text{Bob}_5\}$. There are three maximal unqualified subset $F_1 = \{\text{Bob}_1, \text{Bob}_2\}$, $F_2 = \{\text{Bob}_2, \text{Bob}_5\}$, $F_3 = \{\text{Bob}_3, \text{Bob}_4\}$ in the participants.

First, Alice randomly generates three different pairs (α_1, β_1), (α_2, β_2), (α_3, β_3), where $\alpha_i, \beta_i \in \{0, 1, \ldots, d-1\}$, $i \in \{1, 2, 3\}$. Then she generates five same sets $H_i = \{(\alpha_1, \beta_1, 1), (\alpha_2, \beta_2, 2), (\alpha_3, \beta_3, 3)\}$, $i = 1, 2, \ldots, 5$. Alice performs the operation of step (2) in Sect. 3.1, the five sets become $H_1 = \{(\alpha_2, \beta_2, 2), (\alpha_3, \beta_3, 3)\}$, $H_2 = \{(\alpha_3, \beta_3, 3)\}$, $H_3 = \{(\alpha_1, \beta_1, 1), (\alpha_2, \beta_2, 2)\}$, $H_4 = \{(\alpha_1, \beta_1, 1), (\alpha_2, \beta_2, 2)\}$,

$H_5 = \{(\alpha_1, \beta_1, 1), (\alpha_3, \beta_3, 3)\}$. $H_i (i = 1, 2, \ldots, n)$ is sent to the participant Bob$_i$ as his private key.

Alice performs the unitary operation $U_{A,B} = \sum_{j=0}^{d-1} \omega^{jA} |j\rangle\langle j + B|$ on $|\Psi\rangle$, where $A = d - (\alpha_1 + \alpha_2 + \alpha_3)$, $B = d - (\beta_1 + \beta_2 + \beta_3)$. Alice sends the quantum state to a qualified subset, and we assume this qualified subset is $\{\text{Bob}_4, \text{Bob}_5\}$. The private key of Bob$_4$ is $H_4 = \{(\alpha_1, \beta_1, 1), (\alpha_2, \beta_2, 2)\}$, and the private key of Bob$_5$ is $H_5 = \{(\alpha_1, \beta_1, 1), (\alpha_3, \beta_3, 3)\}$.We can see that this qualified subset have all the three pairs (α_1, β_1), (α_2, β_2), (α_3, β_3). $\{\text{Bob}_4, \text{Bob}_5\}$ use the pairs in their private keys to perform the unitary operations [step (6–8) in Sect. 3.2], and each different pair is only be used one time. Then the unitary operations of $\{\text{Bob}_4, \text{Bob}_5\}$ will make the quantum state become the original state $|\Psi\rangle$.

5 Comparisons

As described in Sect. 1, the (n, n) structure cannot be used in the threshold scenario, and the (t, n) structure cannot be used when the participants are not equal. So the access structure and the adversary structure are more practical.

In a scenario that the adversary structure is easy to be obtained, we can adopt our scheme directly or convert the adversary structure to the access structure, and then adopt the scheme of access structure. But when the number of the participants is big, the conversion will be complicated, and an easy adversary structure may generate a complex access structure. We use the example in Sect. 4 to compare our scheme and the other schemes. In this example, there are five participants: $\{\text{Bob}_1, \text{Bob}_2, \text{Bob}_3, \text{Bob}_4, \text{Bob}_5\}$, and three maximal unqualified subsets: $\{\text{Bob}_1, \text{Bob}_2\}$, $\{\text{Bob}_2, \text{Bob}_5\}$ and $\{\text{Bob}_3, \text{Bob}_4\}$. Obviously, the schemes of (n, n) structure and (t, n) structure cannot be used here. If we use the scheme of access structure, we will get seven minimal qualified subsets: $\{\text{Bob}_1, \text{Bob}_3\}$, $\{\text{Bob}_1, \text{Bob}_4\}$, $\{\text{Bob}_1, \text{Bob}_5\}$, $\{\text{Bob}_2, \text{Bob}_3\}$, $\{\text{Bob}_2, \text{Bob}_4\}$, $\{\text{Bob}_3, \text{Bob}_5\}$ and $\{\text{Bob}_4, \text{Bob}_5\}$. The dealer must distribute the keys for these seven minimal qualified subsets, which is much more than the maximal unqualified subsets. So it is not efficient to use the scheme of access structure in this scenario. In this example, the number of the participants is not big. As mentioned above, if the number of the participants is big, the conversion between access structure and adversary structure may be very complicated, the obtained minimal qualified subsets may be much more than the maximal unqualified subsets, and then our scheme will be much more efficient than the scheme of access structure.

6 Security and proof

6.1 Confidentiality

We assume that $Q = \{\text{Bob}_1, \text{Bob}_2, \ldots, \text{Bob}_n\}$ is the set of the n participants, $\Omega_0 = \{F_1, F_2, \ldots, F_m\}$ is the maximal adversary structure of Q, and F_i $(i = 1, 2, \ldots, m)$ is the maximal unqualified subset.

Theorem 1 *After the distribution in Sect. 3.1, for any subset $X \subseteq Q$, if X does not have the array $(\alpha_i, \beta_i, i),\ i \in \{1, 2, \ldots, m\}$, then $X \subseteq F_i$.*

Proof We adopt apagoge. We first assume that X does not have the array (α_i, β_i, i) but $X \not\subseteq F_i$.

If $X \not\subseteq F_i$, then X at least includes one participant Bob$_j$ who is not in F_i, that is, Bob$_j \in X$ and Bob$_j \notin F_i$. According to the distribution of keys [Step (2) in Sect. 3.1], only the participants in F_i do not have the array (α_i, β_i, i), but other participants all have (α_i, β_i, i). Because Bob$_j \notin F_i$, Bob$_j$ must have (α_i, β_i, i); because Bob$_j \in X$, the subset X must have (α_i, β_i, i) too.

However, we have assumed that X does not have (α_i, β_i, i) in the beginning, so this conclusion violates the above premise. We can get that the assumption is not correct, and Theorem 1 is proved. □

Lemma 1 *A random unqualified subset F cannot get all the m array (α_i, β_i, i), $i = 1, 2, \ldots, m$;*

Proof We adopt apagoge. We first assume that an unqualified subset F can get all the m array $(\alpha_i, \beta_i, i),\ i = 1, 2, \ldots, m$.

If F can get all the m array $(\alpha_i, \beta_i, i),\ i = 1, 2, \ldots, m$, according to Theorem 1, we can get that $F \not\subseteq F_i,\ i = 1, 2, \ldots, m$.

We know that F is an unqualified subset, so we can get that $F \subseteq F_j, j \in \{1, 2, \ldots, m\}$, where F_j is a maximal unqualified subset.

So far, we have got two contrary conclusions. So the assumption is not correct, and Lemma 1 is proved. □

Lemma 2 *A random qualified subset R must have all the m array $(\alpha_i, \beta_i, i),\ i = 1, 2, \ldots, m$.*

Proof We adopt apagoge. We first assume that a qualified subset R does not have the array $(\alpha_j, \beta_j, j),\ j \in \{1, 2, \ldots, m\}$.

If R does not have the array (α_j, β_j, j), according to Theorem 1, we can know that $R \subseteq F_j$. We also know that F_j is the maximal unqualified subset, so R must be an unqualified subset.

But in the beginning, we have assumed that R is a qualified subset. So the conclusion violates the premise, and the assumption is not correct. Lemma 2 is proved. □

Theorem 2 *If an unitary operation $U_{\alpha,\beta} = \sum_{j=0}^{d-1} \omega^{j\alpha} |j\rangle\langle j+\beta|$ is performed on a d-dimensional quantum state $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$, then the quantum state $|\Psi\rangle$ will become a new state $|\Psi'\rangle = \sum_{j=0}^{d-1} \omega^{j\alpha} c_j |j+\beta\rangle$, where $\omega = e^{\frac{2\pi i}{d}}, \alpha, \beta \in \{0, 1, \ldots, d-1\}$, and the symbol "+" means the adder modulo d.*

Proof $|\Psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle = c_0|0\rangle + c_1|1\rangle + \cdots + c_{d-1}|d-1\rangle$

$$\begin{aligned} U_{\alpha,\beta} &= \sum_{j=0}^{d-1} \omega^{j\alpha} |j\rangle\langle j+\beta| \\ &= \omega^{0\cdot\alpha}|0\rangle\langle\beta| + \omega^{1\cdot\alpha}|1\rangle\langle 1+\beta| + \omega^{2\cdot\alpha}|2\rangle\langle 2 \\ &\quad +\beta| + \cdots + \omega^{(d-1)\cdot\alpha}|d-1\rangle\langle d-1+\beta| \end{aligned}$$

Therefore

$$U_{\alpha,\beta}|\Psi\rangle = \omega^{0\cdot\alpha}c_0|\beta\rangle + \omega^{1\cdot\alpha}c_1|1+\beta\rangle + \cdots + \omega^{(d-1)\cdot\alpha}c_{d-1}|d-1+\beta\rangle$$
$$= \sum_{j=0}^{d-1}\omega^{j\alpha}c_j|j+\beta\rangle$$

□

Lemma 3 *A random qualified subset R can recover the original state $|\Psi\rangle$; a random unqualified subset F cannot recover the original state $|\Psi\rangle$.*

Proof From Lemma 2, we know that a qualified subset R must have all the array $(\alpha_i, \beta_i, i),\ i = 1, 2, \ldots, m$. In the recovery, according to the published label "i" [step (6) in Sect. 3.2], each different pair $(\alpha_i, \beta_i),\ i \in \{1, 2, \ldots, m\}$ will only be used one time in the unitary operations. Therefore, every pair $(\alpha_i, \beta_i),\ i \in \{1, 2, \ldots, m\}$ will be used one time in the unitary operations. According to Theorem 2, the recovered state will become $|\Psi_m'\rangle = \sum_{j=0}^{d-1}\omega^{j(A+\alpha_1+\alpha_2+\cdots+\alpha_m)}c_j\langle j+B+\beta_1+\beta_2+\cdots+\beta_m|$ after the last participant of R performed the unitary operation, where the symbol "+" means the adder modulo d. We know that $A = d-(\alpha_1+\alpha_2+\cdots+\alpha_m)$, $B = d-(\beta_1+\beta_2+\cdots+\beta_m)$ [step (2) in Sect. 3.2]. So $|\Psi_m'\rangle = \sum_{j=0}^{d-1}c_j\langle j| = |\Psi\rangle$, and the original state is recovered.

From Lemma 1, we know that an unqualified subset F cannot get all the m array $(\alpha_i, \beta_i, i),\ i = 1, 2, \ldots, m$. Then in the recovery, some pair will be absent in the unitary operations. We know that Alice performs the unitary operation $U_{A,B} = \sum_{j=0}^{d-1}\omega^{jA}|j\rangle\langle j+B|$ to encode the original quantum state $|\Psi\rangle$ into $|\Psi'\rangle$, where $A = d-(\alpha_1+\alpha_2+\cdots+\alpha_m),\quad B = d-(\beta_1+\beta_2+\cdots+\beta_m)$. The absence of any pair will lead that $|\Psi'\rangle$ cannot be decoded. So an unqualified subset cannot recover the original state $|\Psi\rangle$ from the encrypted quantum state. □

6.2 Security of particles transmission

Since the security of particles transmission in our scheme is based on the decoy particles, two well-known attacks: the intercept-and-resend attack and the entangle-and-measure attack will be analyzed in the following.

(1) intercept-and-resend

We assume that an eavesdropper called Eve intercepts the transmitted particles and resends other forged particles in hope to pass the check. We know that the transmitted particles are composed of a useful particle and some decoy particles. Each decoy particle is randomly chosen from the Z-basis or X-basis, and the useful particle is randomly inserted into the decoy particles. Eve cannot know the position, basis and value of each decoy particle. So the attack may cause some errors to the decoy particles. For one decoy particle, the error rate caused by the eavesdropping is $\frac{d-1}{2d}$. Then for l decoy particles, the eavesdropping will be detected with the probability $1-(\frac{d+1}{2d})^l$. When l is large enough, the probability will converge to 1.

(2) entangle-and-measure

Eve uses a unitary operation U_E to entangle an ancillary particle on the transmitted particle and then measures the ancillary particle to steal secret information. Assume that the ancillary particle is $|E\rangle$. If the decoy particle is in the Z-basis, the effect of the unitary operation U_E performed on the decoy particle can be shown as follows.

$$\begin{aligned}
&U_E|0\rangle|E\rangle = a_{00}|0\rangle|e_{00}\rangle + a_{01}|1\rangle|e_{01}\rangle + \cdots + a_{0(d-1)}|d-1\rangle|e_{0(d-1)}\rangle \\
&U_E|1\rangle|E\rangle = a_{10}|0\rangle|e_{10}\rangle + a_{11}|1\rangle|e_{11}\rangle + \cdots + a_{1(d-1)}|d-1\rangle|e_{1(d-1)}\rangle \\
&\ldots \\
&U_E|d-1\rangle|E\rangle = a_{(d-1)0}|0\rangle|e_{(d-1)0}\rangle + a_{(d-1)1}|1\rangle|e_{(d-1)1}\rangle \\
&\quad + \cdots + a_{(d-1)(d-1)}|d-1\rangle|e_{(d-1)(d-1)}\rangle
\end{aligned}$$

where $|e_{ij}\rangle$ $(i, j \in \{0, 1, \ldots, d-1\})$ are the states determined by the unitary operation U_E, and

$$\begin{aligned}
&|a_{00}|^2 + |a_{01}|^2 + \cdots + |a_{0(d-1)}|^2 = 1 \\
&|a_{10}|^2 + |a_{11}|^2 + \cdots + |a_{1(d-1)}|^2 = 1 \\
&\ldots \\
&|a_{(d-1)0}|^2 + |a_{(d-1)1}|^2 + \cdots + |a_{(d-1)(d-1)}|^2 = 1
\end{aligned}$$

In order to avoid the eavesdropping check, Eve has to set:

$$\begin{aligned}
&a_{01} = a_{02} = \cdots = a_{0(d-1)} = 0 \\
&a_{10} = a_{12} = \cdots = a_{1(d-1)} = 0 \\
&\ldots \\
&a_{(d-1)0} = a_{(d-1)1} = \cdots = a_{(d-1)(d-2)} = 0
\end{aligned}$$

Therefore, the effect of U_E performed on the decoy particle can be simplified as follows.

$$\begin{aligned}
&U_E|0\rangle|E\rangle = a_0|0\rangle|e_0\rangle \\
&U_E|1\rangle|E\rangle = a_1|1\rangle|e_1\rangle \\
&\ldots \\
&U_E|d-1\rangle|E\rangle = a_{d-1}|d-1\rangle|e_{d-1}\rangle
\end{aligned}$$

where $a_0 = a_{00}; a_1 = a_{11}; \ldots; a_{d-1} = a_{(d-1)(d-1)}$ and $e_0 = e_{00}; e_1 = e_{11}; \ldots; e_{d-1} = e_{(d-1)(d-1)}$.

If the decoy particle is in the X-basis, the effect of the unitary operation U_E performed on the decoy particle can be shown as follows.

$$\begin{aligned}U_E|J_j\rangle|E\rangle &= U_E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}|k\rangle\right)|E\rangle\\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}U_E|k\rangle|E\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}a_k|k\rangle|e_k\rangle\end{aligned}$$

where $j \in \{0, 1, \ldots, d-1\}$.

We know that $|j\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{-kj}|J_k\rangle$, so

$$\begin{aligned}U_E|J_j\rangle|E\rangle &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{kj}a_k|e_k\rangle\left(\frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}\omega^{-ik}|J_i\rangle\right)\\ &= \frac{1}{d}\left(|J_0\rangle\sum_{k=0}^{d-1}\omega^{k(j-0)}a_k|e_k\rangle\right.\\ &\quad\left.+|J_1\rangle\sum_{k=0}^{d-1}\omega^{k(j-1)}a_k|e_k\rangle+\cdots+|J_{d-1}\rangle\sum_{k=0}^{d-1}\omega^{k(j-(d-1))}a_k|e_k\rangle\right)\end{aligned}$$

In order to avoid the eavesdropping check, Eve has to set $\sum_{k=0}^{d-1}\omega^{k(j-i)}a_k|e_k\rangle = 0$, where $i \in \{0, 1, \ldots, d-1\}$ and $i \neq j$. Then for any $j \in \{0, 1, \ldots, d-1\}$, we can get $d-1$ equations. According to these d-1 equations, we can obtain that $a_0|e_0\rangle = a_1|e_1\rangle = \cdots = a_{d-1}|e_{d-1}\rangle$. Therefore, no matter what the state of the useful particle is, Eve will get the same information from the ancillary particle and cannot steal secret information. So the entangle-and-measure attack is unsuccessful.

6.3 Participant attack

If a QSS scheme is secure for a dishonest participant, then it is secure for any outside eavesdropper. In fact, the participant attack has broken many QSS schemes [34–37]. We now analyze the security of our scheme for a dishonest participant. A dishonest participant can intercept other participant's particles and resend forged particles [34], or entangle ancillary particles on the intercepted particles and steal the secret information through measuring the ancillary particles [35–37]. However, the transmitted particles in our scheme are protected by the decoy particles, which are random in the Z-basis or X-basis and will be disturbed if the transmitted particles are eavesdropped. From the above analysis of "intercept-and-resend attack" and "entangle-and-measure attack", we can know that whether the outside eavesdropper or the dishonest participant will be prevented from measuring the transmitted particles or ancillary particles because of the decoy particles. Therefore, the dishonest participant cannot steal the secret information from the transmitted particles, and our scheme can resist the participant attack.

6.4 Noisy quantum channel

In a noisy quantum channel, the eavesdropper may use the noise to hide his attack. According to the existing results [38–42], the error rate of one qubit caused by the noise is about from 2 to 8.9 %. If the error rate caused by the eavesdropper is smaller than this value, the eavesdropper will be able to hide his attack into the noise. But in our scheme, the error rate of one qubit caused by the eavesdropper is $\frac{d-1}{2d}(d \geq 2)$, which is larger than the error rate caused by the noise. Therefore, the eavesdropper cannot hide his attack into the noise.

In a noisy quantum channel, some transmitted particles may be lost. Our protocol needs to make some modifications to resolve this problem [15,23]. The receiver must inform the sender of the received particles and the lost particles. If the useful particle is lost, the protocol should be terminated and be repeated from the beginning. If some decoy particles are lost, the receiver uses the rest decoy particles to check the eavesdropping. The lost decoy particles become useless, and no useful information can be extracted from these particles.

7 Conclusion

When only the adversary structure is given, the existing QSS schemes with (n, n) structure, (t, n) structure and access structure cannot be used directly. For this requirement, this paper proposed a QSS scheme with adversary structure. By using a novel algorithm, the proposed scheme can share a d-dimensional quantum state according to the adversary structure.

We proved the confidentiality of our scheme and showed that our scheme is secure against the intercept-and-resend attack, the entangle-and-measure attack, the participant attack and the noisy quantum channel.

References

1. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
2. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**, 1829–1834 (1999)
3. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A **59**, 162–168 (1999)
4. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A **61**, 042311 (2000)
5. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A **310**, 247–251 (2003)
6. Deng, F.G., Zhou, H.Y., Long, G.L.: Bidirectional quantum secret sharing and secret splitting with polarized single photons. Phys. Lett. A **337**, 329 (2005)
7. Wang, T.Y., Wen, Q.Y., Chen, X.B., Guo, F.Z., Zhu, F.C.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. **281**, 6130–6134 (2008)
8. Yan, F.L., Gao, T., Li, Y.C.: Quantum secret sharing protocol between multiparty and multiparty with single photons and unitary transformations. Chin. Phys. Lett. **25**, 1187–1190 (2008)
9. Sun, Y., Wen, Q.Y., Gao, F., Chen, X.B., Zhu, F.C.: Multiparty quantum secret sharing based on Bell measurement. Opt. Commun. **282**, 3647–3651 (2009)
10. Sarvepalli, P.K., Klappenecker, A.: Sharing classical secrets with Calderbank–Shor–Steane codes. Phys. Rev. A **80**, 022321 (2009)

11. Li, Q., Long, D.Y., Chan, W.H., Qiu, D.W.: Sharing a quantum secret without a trusted party. Quantum Inf. Process. **10**, 97–106 (2011)
12. Shi, R.H., Huang, L.S., Yang, W., Zhong, H.: Multi-party quantum state sharing of an arbitrary two-qubit state with Bell states. Quantum Inf. Process. **10**, 231–239 (2011)
13. Yang, Y.G., Teng, Y.W., Chai, H.P., Wen, Q.Y.: Verifiable quantum (k, n)-threshold secret key sharing. Int. J. Theor. Phys. **50**, 792–798 (2011)
14. Yang, Y.G., Jia, X., Wang, H.Y., Zhang, H.: Verifiable quantum (k, n)-threshold secret sharing. Quantum Inf. Process. **11**, 1619–1625 (2012)
15. Liu, L.L., Tsai, C.W., Hwang, T.: Quantum secret sharing using symmetric W state. Int. J. Theor. Phys. **51**, 2291–2306 (2012)
16. Dehkordi, M.H., Fattahi, E.: A novel and efficient multiparty quantum secret sharing scheme using entangled states. Sci. China Phys. Mech. Astron. **55**, 1828–1831 (2012)
17. Hao, S.B., Yu, B.: Multiparty quantum secret information sharing in enterprise management based on single qubit with random rotation angle. Int. J. Theor. Phys. **51**, 1674–1679 (2012)
18. Chiawei, T., Tzonelih, H.: Multi-party quantum secret sharing based on two special entangled states. Sci. China Phys. Mech. Astron. **55**, 460–464 (2012)
19. Gao, G.: Secure multiparty quantum secret sharing with the collective eavesdropping-check character. Quantum Inf. Process. **12**, 55–68 (2013)
20. Shi, R.H., Lv, G.L., Wang, Y., Huang, D.Z., Guo, Y.: On quantum secret sharing via Chinese remainder theorem with the non-maximally entanglement state analysis. Int. J. Theor. Phys. **52**, 539–548 (2013)
21. Wang, H.B., Huang, Y.G., Fang, X., Gu, B., Fu, D.S.: High-capacity three-party quantum secret sharing with single photons in both the polarization and the spatial-mode degrees of freedom. Int. J. Theor. Phys. **52**, 1043–1051 (2013)
22. Sun, Y., Xu, S.W., Chen, X.B., Niu, X.X., Yang, Y.X.: Expansible quantum secret sharing network. Quantum Inf. Process. **12**, 2877–2888 (2013)
23. Hsu, J.L., Chong, S.K., Hwang, T., Tsai, C.W.: Dynamic quantum secret sharing. Quantum Inf. Process. **12**, 331–344 (2013)
24. Lau, H.K., Weedbrook, C.: Quantum secret sharing with continuous-variable cluster states. Phys. Rev. A **88**, 042313 (2013)
25. Chen, R.K., Zhang, Y.Y., Shi, J.H., Li, F.G.: A multiparty error-correcting method for quantum secret sharing. Quantum Inf. Process. **13**, 21–31 (2014)
26. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. **83**, 648–651 (1999)
27. Tyc, T., Sanders, B.C.: How to share a continuous-variable quantum secret by optical interferometry. Phys. Rev. A **65**, 042310 (2002)
28. Sarvepalli, P.: Nonthreshold quantum secret-sharing schemes in the graph-state formalism. Phys. Rev. A **86**, 042303 (2012)
29. Wang, M.M., Chen, X.B., Yang, Y.X.: Quantum secret sharing for general access structures based on multiparticle entanglements. Quantum Inf. Process. **13**, 429–443 (2014)
30. Hirt, M., Maurer, U.: Player simulation and general adversary structures in perfect multi-party computation. J. Cryptol. **13**, 31–60 (2000)
31. Zhou, L., Schneider, F., Robbert, R.: APSS: proactive secret sharing in asynchronous systems. ACM Trans. Inf. Syst. Secur. **8**, 259–286 (2005)
32. Cai, Q.Y., Li, W.B.: Deterministic secure communication without using entanglement. Chin. Phys. Lett. **21**, 601–603 (2004)
33. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A **69**, 052319 (2004)
34. Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on “Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection. Phys. Rev. Lett. **101**, 208901 (2008)
35. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery–Buzek–Berthiaume quantum secret-sharing protocol. Phys. Rev. A **76**, 062324 (2007)
36. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: “Quantum exam” [Phys. Lett. A **350** (2006) 174]. Phys. Lett. A **360**, 748–750 (2007)
37. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. Opt. Commun. **382**, 192–195 (2010)
38. Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., Zeilinger, A.: Quantum cryptography with entangled photons. Phys. Rev. Lett. **84**, 4729–4732 (2000)

39. Hughes, R.J., Nordholt, J.E., Derkacs, D., Peterson, C.G.: Practical free-space quantum key distribution over 10km in daylight and at night. New J. Phys. **43**, 1–14 (2002)
40. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G., Zbinden, H.: Quantum key distribution over 67km with a plug&play system. New J. Phys. **41**, 1–8 (2002)
41. Beveratos, A., Brouri, R., Gacoin, T., Villing, A., Poizat, J.P., Grangier, P.: Single photon quantum cryptography. Phys. Rev. Lett. **89**, 187901 (2002)
42. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122km standard telecom fiber. Appl. Phys. Lett. **84**, 3762–3764 (2004)