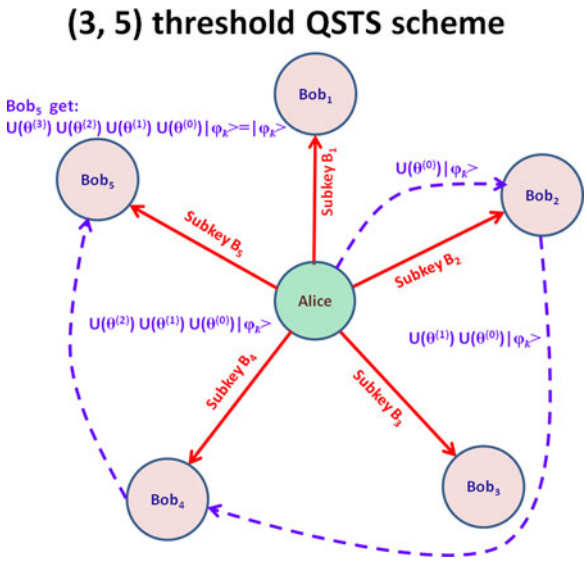
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

(t, n) Threshold Quantum State Sharing Scheme Based on Linear Equations and Unitary Operation

Volume 9, Number 1, February 2017

Cao Hao
Ma Wenping



DOI: 10.1109/JPHOT.2017.2657232
1943-0655

(t, n) Threshold Quantum State Sharing Scheme Based on Linear Equations and Unitary Operation

Cao Hao[1,2] **and Ma Wenping**[1]

[1]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, P. R. China
[2]School of Information and Network Engineering, Anhui Science and Technology University, Chuzhou 233100, China

DOI:10.1109/JPHOT.2017.2657232

Manuscript received August 1, 2016; revised January 18, 2017; accepted January 19, 2017. Date of publication January 24, 2017; date of current version February 13, 2017. This work was supported in part by the National Science Foundation of China under Grant 61373171, in part by the 111 Project under Grant B08038, and in part by the Key Project of Science Research of Anhui Province (Quantum key agreement protocol based on entangled state). Corresponding Author: C. Hao (e-mail:13655505689@163.com).

Abstract: Quantum state sharing (QSTS) plays an important role in transporting, managing, and distributing keys. In this paper, by adopting the linear equation instead of using the Lagrange interpolation, a new idea of constructing (t, n) threshold quantum state sharing scheme is proposed. The best innovation is that a new tool in constructing (t, n) threshold structure is proposed. In this scheme, the dealer who possesses a sequence of one-particle unknown quantum states intends to share it with n participants and authorizes t out of them cooperate to reconstruct the sequence. First, the equations decided by the private key of dealer are constructed. Second, the dealer distributes the private keys of n participants by using the solutions to the equations just mentioned. Finally, the dealer encodes the sequence through a unitary operation, and any t out of the n participants recover the initial quantum state sequence through the unitary operations decided by the solutions to the linear equations. Compared to the existing schemes, the proposed scheme is easily realized in physical experiment, and its successful probability is 100% theoretically.

Index Terms: Quantum secret sharing (QSS), quantum state sharing (QSTS), linear equation, unitary operation.

1. Introduction

Secret sharing is a key technology of data confidentiality in the traditional cryptosystems. In order to resist diversify risk, one can distribute a secret among some agents, and the authorized agents can only cooperate to recover the original secret. Secret sharing plays an important role in the application of electronic commerce, key distribution, secure multi-party computation, and so on. However, the traditional secret sharing schemes will be challenged by the applications of quantum information theory and technology. Quantum cryptography is a new type of secure communication technologies which are based on quantum entanglement and no-cloning theorem of quantum mechanics. It has been proved to be absolutely safe in theory. In 1984, Bennett and Brassard proposed the first quantum cryptography scheme, which is famous for the BB84 [1]. Since then, quantum cryptography strongly attracted attentions from cryptographers and physicists, and several

branchs of quantum cryptography such as quantum key distribution (QKD) [1]–[2], quantum secret sharing (QSS) [3]–[27], quantum direct communication (QDC) [28]–[30], quantum authentication [31], etc., have been proposed. As an important branch of quantum cryptography, quantum secret sharing (QSS) particularly attracted much attention owing to the important applications in quantum computing, multi-party key distribution and unknown quantum state sharing.

Quantum secret sharing mainly includes the QSS scheme, which shares the classical information and QSTS scheme, which shares the quantum information by using the quantum resources. In 1999, Hillery *et al.* put forward the first QSS scheme through the use of Greenberger–Horne–Zeilinger (GHZ) state [3]. That same year, Cleve *et al.* used quantum error correcting code theory to propose a threshold QSS [4]. Since then, QSS and QSTS have gained wide attention, and various schemes have been proposed [5]–[27]. The majority of the current QSS and QSTS schemes, only in all the n participants together with the case, can the secret be recovered. However, any part of the participant could not reconstruct the key [5]–[19], [27]. Some schemes [20]–[26] are (t, n) threshold structure, but these schemes are very complicated. The complicated operations such as quantum error-correcting encoding, continuous-variable quantum state generation or Lagrange interpolation are needed. Hence, searching for new and effective method to construct (t, n) threshold structure is more and more meaningful theoretically and practically.

In this paper, we propose a new and effective method in which the linear equation is used for the first time currently to construct (t, n) threshold structure. The proposed scheme is based on the solutions of the linear equations and unitary transformations, and it possesses the following merits:

1) The private keys of the dealer and n participants are easily generated.
2) The procedure is easily implemented practically.
3) The successful ratio of the implementation is 100%.
4) The private key of the dealer could be reused many times.

The rest of this paper is organized as follows. In Section 2, the design method of the proposed scheme is described in detail. In Section 3, a concrete example of the proposed scheme is shown. Section 4 analyzes the proposed scheme and compares it to other schemes. Finally, in Section 5, the conclusion of this paper is given.

2. Proposed Scheme

Assume that Alice is the dealer who possesses a sequence of 1-particle unknown quantum states as follows:

$$|\varphi_k>=\alpha_k|0>+\beta_k|1> \qquad (k=1,2,\cdots,m) \tag{1}$$

where the complex amplitudes α_k and β_k of $|\varphi_k>$, satisfy the follow equality:

$$|\alpha_k|^2+|\beta_k|^2=1. \tag{2}$$

Alice intends to share the former sequence with the n participants $Bob_1, Bob_2, ..., Bob_n$. If it comes to the pinch, Alice will select arbitrary t participants $Bob_{i_1}, Bob_{i_2}, ..., Bob_{i_t}$ from $Bob_1, Bob_2, ..., Bob_n$, and authorize them cooperate to reconstruct the sequence of 1-particle unknown quantum states.

2.1 Initialization Phase

Alice accomplishes the distribution of private keys among the n participants Bob_i ($i = 1, 2, \ldots, n$) by using the following steps.

1) Alice selects an infinite field F (Rational number field, Real number field, or Complex field).
2) Alice selects n non-zero elements $e_1, e_2, ..., e_n$ from F randomly. The set $\{e_1, e_2, ..., e_n\}$ is the private of Alice.
3) For every $\{e_{i_1}, e_{i_2}, ..., e_{i_t}\} \subseteq \{e_1, e_2, ..., e_n\}$, where $1 \le i_1 \le i_2 \le \cdots \le i_t \le n$, Alice defines a t-variable equation as follows:

$$e_{i_1}x_{i_1}+e_{i_2}x_{i_2},...e_{i_t}x_{i_t}=1. \tag{3}$$

Alice selects a solution $X_{i_1 i_2 \cdots i_t} = (x_{s(i_1)}, x_{s(i_2)}, \ldots x_{s(i_t)})$ to the proposed equation, and the solutions to all the equations satisfy that the values corresponding to the same variable are different in different equations and every $x_{s(i_j)} \neq 0$. The subscript of $x_{s(i_j)}$, $s(i_j) = i_j i_1 i_2 \cdots i_{j-1} i_{j+1} \cdots i_t$ is consisted of i_j with the natural order of $i_1, i_2, \cdots, i_{j-1}, i_{j+1}, \cdots, i_t$. For example, if we select $i_1 = 1$, $i_2 = 3$, $i_3 = 4$, $i_4 = 5$, and $i_5 = 8$, then we have

$$\begin{aligned} s(i_1) &= s(1) = i_1 i_2 i_3 i_4 i_5 = 13458 \\ s(i_2) &= s(3) = i_2 i_1 i_3 i_4 i_5 = 31458 \\ s(i_3) &= s(4) = i_3 i_1 i_2 i_4 i_5 = 41358 \\ s(i_4) &= s(5) = i_4 i_1 i_2 i_3 i_5 = 51348 \\ s(i_5) &= s(8) = i_5 i_1 i_2 i_3 i_4 = 81345. \end{aligned}$$

Hence, the corresponding solution of the just mentioned equation is $X_{13458} = (x_{13458}, x_{31458}, x_{41358}, x_{51348}, x_{81345})$.

4) Alice selects a non-zero element $\delta \in F$ randomly and defines

$$B_i = \{\delta \cdot e_i \cdot x_{i j_1 j_2 \cdots j_{t-1}} | i \neq j_1, j_2, \cdots, j_{t-1} \text{ and } 1 \leq j_1 \leq j_2 \leq \cdots \leq j_{t-1} \leq n\}. \quad (4)$$

The B_i is the private key of Bob_i. Alice sends B_i to Bob_i by quantum secure direct communication method [28]–[30].

2.2 Sharing of Quantum State Phase

Alice generates the sequence of unknown quantum state $\{|\varphi_k> = \alpha_k|0> + \beta_k|1> | (k = 1, 2, \cdots, m)\}$. Next, Alice performs an unitary transform $U(\theta^{(0)})$ (where $\theta^{(0)} = 2\pi - \delta$) on every quantum state in that sequence as just mentioned. $U(\theta)$ is defined by the following 2×2 matrix on the variable θ:

$$U(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \quad (5)$$

Apparently, $U(\theta)$ is an unitary transformation on 1-qubit state. Alice gets the qubit state sequence $\{|\varphi_k{}^0> | k = 1, 2, \cdots, m\}$, where $|\varphi_k{}^0> \equiv U(\theta^{(0)})|\varphi_k>$. If t participants $Bob_{i_1}, Bob_{i_2}, \ldots, Bob_{i_t}$ ($1 \leq i_1 \leq i_2 \leq \cdots \leq i_t \leq n$) out of the n participants $Bob_1, Bob_2, \ldots, Bob_n$ request to Alice reconstructing the initial quantum state sequence $\{|\varphi_k>\}$. Then, Alice could share the sequence of unknown states $|\varphi_1>, |\varphi_2>, \cdots, |\varphi_m>$ by performing the follow step:

1) Alice chooses some decoy particles randomly from the states $\{|0>, |1>, |+>, |->\}$, where $|+> = \frac{1}{\sqrt{2}}(|0> + |1>)$ and $|-> = \frac{1}{\sqrt{2}}(|0> - |1>)$, and inserts them into the sequence. She records the initial state and corresponding positions of every decoy particle. Alice transmits the sequence $\{|\varphi_k{}^0>\}$ with decoy particles to Bob_{i_1}. Next, Alice will announce the positions and the corresponding measuring bases $\{|0>, |1>\}$ or $\{|+>, |->\}$ of the decoy particles after Bob_{i_1}'s confirmation of received the sequence. Bob_{i_1} measures those decoy particles in the bases $\{|0>, |1>\}$ or $\{|+>, |->\}$ and publishes his measurement results. Alice can calculate the error probability by comparing the measurement results with the initial states. If the error ratio is lower than the threshold value, Alice declares that the process is effective, and the process continues. Otherwise, Alice asks Bob_{i_1} to discard the sequence and starts a new one. This process is called Security Checking.

After successfully passed the Security Checking, Bob_{i_1} extracts the sequence $\{|\varphi_k{}^0>\}$ from the received sequence by deleting the decoy particles. Then Bob_{i_1} selects $\theta^{(1)} = \delta e_{i_1} x_{i_1 i_2 \cdots i_t}$ from his private B_{i_1}, and performs the unitary transform $U(\theta^{(1)})$ on every quantum state in the sequence $\{|\varphi_k{}^0>\}$. Then Bob_{i_1} gets the quantum state sequence $\{|\varphi_k{}^1> | k = 1, 2, \cdots, m\}$, where $|\varphi_k{}^1> \equiv U(\theta^{(1)})|\varphi_k{}^0>$.

2) Similar to (1), Bob_{i_1} chooses some decoy particles randomly from the states $\{|0>, |1>, |+>, |->\}$, and inserts them into the sequence $\{|\varphi_k{}^1>\}$. He or She records the initial state and corresponding positions of every decoy particle, and then transmits the sequence $\{|\varphi_k{}^1>\}$ with decoy particles to Bob_{i_2}.

Bob_{i_1} and Bob_{i_2} perform Security Checking similar to Alice. If failed to passed the Security Checking, the process terminates and starts a new one. Or else, the process continues.

After successfully passed the Security Checking, Bob_{i_2} extracts the sequence $\{|\varphi_k{}^1>\}$ from the received sequence by deleting the decoy particles. Then Bob_{i_2} selects $\theta^{(2)} = \delta e_{i_2} x_{i_2 i_1 i_3 \cdots i_t}$ from his private B_{i_2}, and performs the unitary transform $U(\theta^{(2)})$ on every quantum state in the sequence $\{|\varphi_k{}^1>\}$. Then Bob_{i_2} gets the quantum state sequence $\{|\varphi_k{}^2> | k = 1, 2, \cdots, m\}$, where $|\varphi_k{}^2> \equiv U(\theta^{(2)})|\varphi_k{}^1>$.

This procedure continues until the participant Bob_{i_t}.

Note: The order of transmitting sequence could be arbitrary as long as the recipient receives sequence in the last step.

3) After successfully passed the Security Checking, Bob_{i_t} extracts the sequence $\{|\varphi_k{}^{t-1}>\}$ from the received sequence by deleting the decoy particles. Bob_{i_t} can reconstruct the initial quantum state sequence $\{|\varphi_k>\}$ after performing the unitary transform $U(\theta^{(t)})$ on the quantum state $\{|\varphi_k{}^{t-1}> | k = 1, 2, \cdots, m\}$, where $\theta^{(t)} = \delta e_{i_t} x_{i_t i_1 i_2 \cdots i_{t-1}}$.

2.3 Correctness of the Proposed Scheme

First, it is obvious that $X_{i_1 i_2 \cdots i_t} = (x_{i_1 i_2 \cdots i_t}, x_{i_2 i_1 i_3 \cdots i_t}, \ldots, x_{i_t i_1 i_2 \cdots i_{t-1}})$ is a solution of the equation $e_{i_1} x_{i_1} + e_{i_2} x_{i_2}, \ldots e_{i_t} x_{i_t} = 1$, and therefore, $e_{i_t} x_{i_t i_1 \cdots i_{t-1}} + e_{i_{t-1}} x_{i_{t-1} i_1 \cdots i_{t-2} i_t} + \cdots e_{i_1} x_{i_1 i_2 \cdots i_t} = 1$.

Second, it is a piece of cake to verified that the equation $U(\theta)U(\gamma)|\varphi_k> = U(\theta+\gamma)|\varphi_k>$ holds for any θ and γ.

The initial quantum state sequence $\{|\varphi_k>\}$ is transformed $t+1$ times by using $t+1$ unitary transforms from $Alice, Bob_{i_1}, Bob_{i_2}, \ldots,$ *and* Bob_{i_t} separately. The correctness of the procedure can be expressed by

$$
\begin{aligned}
&U(\theta^{(t)})U(\theta^{(t-1)}) \cdots U(\theta^{(1)})U(\theta^{(0)})|\varphi_k> \\
&= U(\theta^{(t)} + \theta^{(t-1)} + \cdots + \theta^{(1)} + \theta^{(0)})|\varphi_k> \\
&= U(\delta \cdot e_{i_t} x_{i_t i_1 \cdots i_{t-1}} + \delta \cdot e_{i_{t-1}} x_{i_{t-1} i_1 \cdots i_{t-2} i_t} + \cdots \delta \cdot e_{i_1} x_{i_1 i_2 \cdots i_t} + (2\pi - \delta))|\varphi_k> \\
&= U(\delta \cdot (e_{i_t} x_{i_t i_1 \cdots i_{t-1}} + e_{i_{t-1}} x_{i_{t-1} i_1 \cdots i_{t-2} i_t} + \cdots e_{i_1} x_{i_1 i_2 \cdots i_t}) + (2\pi - \delta))|\varphi_k> \\
&= U(\delta + (2\pi - \delta))|\varphi_k> \\
&= U(2\pi)|\varphi_k> \\
&= |\varphi_k> .
\end{aligned}
$$

Hence, Bob_{i_t} can get the initial quantum state sequence $\{|\varphi_k>\}$, and the proposed scheme is correct.

3. Concrete Example of the Proposed Scheme

In order to exhibit the whole process of the proposed scheme more clearly, a concrete example of quantum (3, 5) threshold is proposed.

Example of quantum (3, 5) threshold: Suppose the scheme is executed on the Rational number field, and the dealer Alice selects n = 5, t = 3, $e_1 = 2$, $e_2 = 4$, $e_3 = 5$, $e_4 = 8$, and $e_5 = 10$. e_1, e_2, e_3, e_4, e_5 is the private of Alice.

1) For every $\{e_{i_1}, e_{i_2}, e_{i_3}\} \subseteq \{e_1, e_2, e_3, e_4, e_5\} (i_1 \le i_2 \le i_3)$, Alice constructs a 3-variable equation $e_{i_1} x_{i_1} + e_{i_2} x_{i_2} + e_{i_3} x_{i_3} = 1$. Then Alice select a solution $X_{i_1 i_2 i_3} = (x_{s(i_1)}, x_{s(i_2)}, x_{s(i_3)})$ of the equation satisfies that the values corresponding to the same variable is different in different equations and every $x_{s(i_j)} \neq 0$.

If $i_1 = 1$, $i_2 = 2$, $i_3 = 3$, then Alice selects a solution from the solution set of the equation $e_1x_1 + e_2x_2 + e_3x_3 = 1$ randomly. Suppose $X_{123} = (x_{123}, x_{213}, x_{312}) = (1, 1, -1)$.

If $i_1 = 1$, $i_2 = 2$, $i_3 = 4$, then Alice selects $X_{124} = (x_{124}, x_{214}, x_{412}) = (\frac{1}{10}, \frac{1}{15}, \frac{1}{15})$.
If $i_1 = 1$, $i_2 = 2$, $i_3 = 5$, then Alice selects $X_{125} = (x_{125}, x_{215}, x_{512}) = (\frac{1}{16}, \frac{1}{16}, \frac{1}{16})$.
If $i_1 = 1$, $i_2 = 3$, $i_3 = 4$, then Alice selects $X_{134} = (x_{134}, x_{314}, x_{413}) = (\frac{2}{27}, \frac{1}{9}, \frac{1}{27})$.
If $i_1 = 1$, $i_2 = 3$, $i_3 = 5$, then Alice selects $X_{135} = (x_{135}, x_{315}, x_{513}) = (3, -5, 2)$.
If $i_1 = 1$, $i_2 = 4$, $i_3 = 5$, then Alice selects $X_{145} = (x_{145}, x_{415}, x_{514}) = (\frac{1}{2}, \frac{1}{4}, -\frac{1}{5})$.
If $i_1 = 2$, $i_2 = 3$, $i_3 = 4$, then Alice selects $X_{234} = (x_{234}, x_{324}, x_{423}) = (\frac{1}{12}, -\frac{1}{3}, \frac{7}{24})$.
If $i_1 = 2$, $i_2 = 3$, $i_3 = 5$, then Alice selects $X_{235} = (x_{235}, x_{325}, x_{523}) = (-1, \frac{1}{3}, \frac{1}{3})$.
If $i_1 = 2$, $i_2 = 4$, $i_3 = 5$, then Alice selects $X_{245} = (x_{245}, x_{425}, x_{524}) = (\frac{1}{2}, \frac{1}{24}, -\frac{2}{15})$.
If $i_1 = 3$, $i_2 = 4$, $i_3 = 5$, then Alice selects $X_{345} = (x_{345}, x_{435}, x_{534}) = (\frac{1}{5}, \frac{1}{10}, -\frac{2}{25})$.

2) Alice selects a non-zero element $\delta \in F$ randomly. Suppose $\delta = 1/40$. Next Alice distributes the private keys of the 5 participants. The keys are defined by the following equation:

$$B_i = \{\delta \cdot e_i \cdot x_{ij_1j_2} | i \neq j_1, j_2 \text{ and } 1 \leq j_1 \leq j_2 \leq 5\}.$$

Therefore

$$B_1 = \{\delta e_1 x_{123}, \delta e_1 x_{124}, \delta e_1 x_{125}, \delta e_1 x_{134}, \delta e_1 x_{135}, \delta e_1 x_{145}\} = \left\{\frac{1}{20}, \frac{1}{200}, \frac{1}{320}, \frac{1}{270}, \frac{3}{20}, \frac{1}{40}\right\}$$

$$B_2 = \{\delta e_2 x_{213}, \delta e_2 x_{214}, \delta e_2 x_{215}, \delta e_2 x_{234}, \delta e_2 x_{235}, \delta e_2 x_{245}\} = \left\{\frac{1}{10}, \frac{1}{150}, \frac{1}{160}, \frac{1}{120}, -\frac{1}{10}, \frac{1}{20}\right\}$$

$$B_3 = \{\delta e_3 x_{312}, \delta e_3 x_{314}, \delta e_3 x_{315}, \delta e_3 x_{324}, \delta e_3 x_{325}, \delta e_3 x_{345}, \} = \left\{-\frac{1}{8}, \frac{1}{72}, -\frac{5}{8}, -\frac{1}{24}, \frac{1}{24}, \frac{1}{40}\right\}$$

$$B_4 = \{\delta e_4 x_{412}, \delta e_4 x_{413}, \delta e_4 x_{415}, \delta e_4 x_{423}, \delta e_4 x_{425}, \delta e_4 x_{435}, \} = \left\{\frac{1}{75}, \frac{1}{135}, \frac{1}{20}, \frac{7}{120}, \frac{1}{120}, \frac{1}{50}\right\}$$

$$B_5 = \{\delta e_5 x_{512}, \delta e_5 x_{513}, \delta e_5 x_{514}, \delta e_5 x_{523}, \delta e_5 x_{524}, \delta e_5 x_{534}, \} = \left\{\frac{1}{64}, \frac{1}{8}, -\frac{1}{20}, \frac{1}{12}, -\frac{1}{30}, -\frac{1}{50}\right\}.$$

3) If the 3 participants Bob_2, Bob_4, Bob_5 request to Alice reconstructing the initial quantum state sequence $\{|\varphi_k>\}$. Then, Alice, Bob_2, Bob_4, *and* Bob_5 will execute the unitary operations $U(\theta_0), U(\theta_1), U(\theta_2)$, *and* $U(\theta_3)$ on the sequence $\{|\varphi_k>\}$ separately if regardless of the decoy states. In this case, $\theta_0 = 2\pi - \frac{1}{40}, \theta_1 = \delta e_2 x_{245} = \frac{1}{20}, \theta_2 = \delta e_4 x_{425} = \frac{1}{120}$, and $\theta_3 = \delta e_5 x_{524} = -\frac{1}{30}$. Finally, Bob_5 could recover $\{|\varphi_k>\}$ by

$$\begin{aligned}
&U(\theta_3)U(\theta_2)U(\theta_1)U(\theta_0)|\varphi_k> \\
&= U(\theta_3 + \theta_2 + \theta_1 + \theta_0)|\varphi_k> \\
&= U\left(2\pi - \frac{1}{40} + \frac{1}{20} + \frac{1}{120} - \frac{1}{30}\right)|\varphi_k> \\
&= U(2\pi)|\varphi_k> \\
&= |\varphi_k> .
\end{aligned}$$

4. Comparative Analysis

Successful ratio: In the proposed scheme, any t out of the n participants could recover the initial unknown state sequence successfully, if the dealer and the t participants cooperate honestly.

Efficiency: Compared to the existing (t, n) threshold schemes, the proposed scheme possesses First, it is easy to produce the private key of the dealer because it is selected from the infinite field

randomly. Second, the privately keys of the n participants are also easily selected because they are decided by the linear equations. Thirdly, the unitary operations are also executed easily. Hence, the procedure of the proposed scheme is easily implemented practically. And more importantly, because of the randomness of selecting the sub keys and the randomness of the secret elements δ, anybody can not recover the master key unless the n participants share their private subkeys. Therefore, the master key could be reused for many times. Comparatively, most of (t, n) threshold schemes [19]–[25] contain complicated operations. For example, quantum error-correcting encoding, continuous-variable quantum state generation or Lagrange interpolation is needed. Furthermore, the master key should be discarded once used, and this is a waste of resource.

Security: First, the proposed scheme can resist intercept-and-resend attack. Assume that the attacker Eve intercepts some particles sent by the dealer Alice or any participant Bobi, and resends a sequence with forged particles. Because of the existence of the decoy particles randomly chosen from $\{|0>, |1>, |+>, |->\}$ in our scheme, and therefore, Eve would surely cause some errors owing to his complete ignorance of the positions, bases and values of the decoy particles. Then the Eve will be detected with the probability $1-(3/4)^m$ which will converge to 1 when m is large enough. Secondly, the scheme could resist photon-number-splitting attack, if the t participants test sequence sample using the technology of photon number splitter when they receive particles. Third, the scheme can also resist man-in-the-middle attack similarly, if the technology of quantum identity authentication is used [31].

Notes in realistic situation: First, due to the lack of the ideal single photon state source used in the proposed scheme, the technology of measurement-device-independent and the weak coherent state source [2] can be used. Second, considering the presence of noise in realistic communication channel, the quantum state amplification [32] can be used to prevent the photon loss. Furthermore, we also can use the entanglement purification [33], [34], spatial entanglement or frequency entanglement [35] to correct the errors.

5. Conclusion

In summary, a new and effective method of constructing (t, n) threshold quantum state sharing scheme is proposed. In this method, the linear equation is used for the first time currently to construct (t, n) threshold structure. The proposed scheme is based on the solutions of the linear equations and unitary transformations, and possesses several merits such as simple operation, high efficiency, and easy to implement compared to the current schemes.

Acknowledgment

The authors would to thank the anonymous reviewers for their valuable suggestions.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process.*, 1984, pp. 175–179.
[2] C. M. Zhang, M. Li, Z. Q. Yin, H. W. Li, W. Chen, and Z. F. HAN, "Decoy-state measurement-device-independent quantum key distribution with mismatched-basis statistics," *Sci. China Phys., Mech. Astron.*, vol. 58, no. 9, 2015, Art. no. 590301.
[3] M. Hillery, V. Buzek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A*, vol. 59, no. 3, 1999, Art. no. 1829.
[4] R. Cleve, D. Gottesman, and H. K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, 1999, Art.no. 648.
[5] F. Deng, X. Li, C. Li, P. Zhou, and H. Y. Zhou, "Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pair," *Phys. Rev. A*, vol. 72, no. 4, 2005, Art. no. 044301.
[6] F. Deng, X. Li, C. Li, P. Zhou, and H. Y. Zhou, "Quantum state sharing of an arbitrary two-qubit state with two-photon entanglements and Bell-state measurements," *Eur. Physical J. D, Atomic, Mol., Opt. Plasma Phys.*, vol. 39, no. 3, pp. 459–464, 2006.
[7] L. Han, Y. Liu, H. Yuan, and Z. Zhang, "Efficient multiparty-to-multiparty quantum secret sharing via continuous variable operations," *Chin. Phys. Lett.*, vol. 24 , no. 12, pp. 3312–3315, 2007.

[8] T. Gao, F. L. Yan, and Y. C. Li, "Quantum secret sharing between m-party and n-party with six states," *Sci. China G, Phys., Mech. Astron.*, vol. 52, no. 8, pp. 1191–1202, 2009.
[9] X. Sun, X. Zha, J. Qi, and Q. Lan, "High-efficient quantum state sharing via non-maximally five-qubit cluster state," *Acta Physica Sinica*, vol. 62, no. 23, 2013, Art. no. 230302.
[10] W. Wang and H. Cao, "An improved multiparty quantum secret sharing with Bell states and Bell measurement," *Int. J. Theor. Phys.*, vol. 52, no. 6, pp. 2099–2111, 2013.
[11] C. Liao, C. Yang, and T. Hwang. "Dynamic quantum secret sharing scheme based on GHZ state," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1907–1916, 2014.
[12] Y. Nie, Y. Xu, Y. Li, and M. Sang, "Quantum state sharing of an arbitrary three-atom state by using five-atom cluster state in cavity QED," *Int. J. Theor. Phys.*, vol. 53, no. 4, pp. 1299–1307, 2014.
[13] C. H. Liao, C. W. Yang, and T. Hwang, "Dynamic quantum secret sharing scheme based on GHZ state," *Quantum Inf. Process.*, vol. 13, no. 8, pp. 1907–1916, 2014.
[14] H. Xing, Y. Liu, C. Xie, Q. Ji, and Z. Zhang, "Four-party deterministic operation sharing with six-qubit cluster state," *Quantum Inf. Process.*, vol. 13, no. 7, pp. 1553–1562, 2014.
[15] Z. Huang, "Quantum state sharing of an arbitrary three-qubit state by using a seven-qubit entangled state," *Int. J. Theor. Phys.*, vol. 54, no. 9, pp. 3438–3441, 2015.
[16] S. Mishra, C. Shukla, A. Pathak, R. Srikanth, and A. Venugopalan, "An integrated hierarchical dynamic quantum secret sharing scheme," *Int. J. Theor. Phys.*, vol. 54, no. 9, pp. 3143–3154, 2015.
[17] Y. Wei and M. Jiang, "Multi-qudit state sharing via various high-dimensional Bell channels," *Quantum Inf. Process.*, vol. 14, no. 3, pp. 1091–1102, 2015.
[18] J. Y. Peng, M. Bai, and Z. W. Mo, "Bidirectional quantum states sharing," *Int. J. Theor. Phys.*, vol. 55, no. 5, pp. 2481–2489, 2016.
[19] H. Qin and Y. Dai, "d-Dimensional quantum state sharing with adversary structure," *Quantum Inf. Process.*, vol. 15, no. 4, pp. 1689–1701, 2016.
[20] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Phys. Rev. A*, vol. 59, no. 1, 1999, Art. no. 162.
[21] Q. Li, D. Y. Long, W. H. Chan, and D. W. Qiu, "Sharing a quantum secret without a trusted party," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 97–106, 2011.
[22] Y. G. Yang, Y. W. Teng, H. P. Chai, and Q. Y. Wen, "Verifiable quantum (k, n)-threshold secret key sharing," *Int. J. Theor. Phys.*, vol. 50, no. 3, pp. 792–798, 2011.
[23] Y. G. Yang, X. Jia, H. Y. Wang, and H. Zhang, "Verifiable quantum (k, n)-threshold secret sharing," *Quantum Inf. Process.*, vol. 11, no. 6, pp. 1619–1625, 2012.
[24] H. Qin, X. Zhu, and Y. Dai, "(t, n) Threshold quantum secret sharing using the phase shift operation," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 2997–3004, 2015.
[25] L. Hong, O. A. Mehmet, X. Jing-Hua, P. Josef, and X. Li-Yin, "Dynamic (2, 3) threshold quantum secret sharing of secure direct communication," *Commun. Theor. Phys.*, vol. 63, no. 4, pp. 459–465, 2015.
[26] X. Song and Y. Liu, "Cryptanalysis and improvement of verifiable quantum (k, n) secret sharing, " *Quantum Inf. Process.*, vol. 15, no. 2, pp. 851–868, 2016.
[27] H. Abulkasim, S. Hamad, K. El Bahnasy, and S. Z. Rida, "Authenticated quantum secret sharing with quantum dialogue based on Bell states," *Physica Scripta*, vol. 91, no. 8, 2016, Art. no. 085101.
[28] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Phys. Rev. A*, vol. 69, no. 5, 2004, Art. no. 052319.
[29] D. Costa, N. G. De Almeida, and C. J. Villas-Boas, "Secure quantum communication using classical correlated channel," *Quantum Inf. Process.*, vol. 15, no. 10, pp. 4303–4311, 2016.
[30] S. Mi, T. Wang, G. Jin, and C. Wang, "High-capacity quantum secure direct communication with orbital angular momentum of photons," *IEEE Photon. J.*, vol. 7, no. 5, Oct. 2015, Art. no. 7600108.
[31] X. L. Zhang, "One-way quantum identity authentication based on public key," *Chin. Sci. Bull.*, vol. 54, no. 12, pp. 2018–2021, 2009.
[32] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, "Heralded photon amplification for quantum communication," *Phys. Rev. A*, vol. 86, no. 2, 2012, Art. no. 023815.
[33] Y. Sheng and L. Zhou, "Deterministic polarization entanglement purification using time-bin entanglement," *Laser Phys. Lett.*, vol. 11, no. 8, 2014, Art. no. 085203.
[34] L. Zhou and Y. Sheng, "Purification of logic-qubit entanglement," *Sci. Rep.*, vol. 6, 2016, Art. no. 28813.
[35] F. G. Deng, "One-step error correction for multipartite polarization entanglement," *Phys. Rev. A*, vol. 83, no. 6, 2011, Art. no. 062316.