IET Information Security

Research Article

Quantum secret sharing by using Fourier transform on orbital angular momentum

ISSN 1751-8709
Received on 1st September 2017
Revised 21st April 2018
Accepted on 24th September 2018
E-First on 16th November 2018
doi: 10.1049/iet-ifs.2018.5149
www.ietdl.org

Huawang Qin[1] ✉, *Raylin Tso*[2], *Yuewei Dai*[1]

[1] *School of Automatization, Nanjing University of Science and Technology, Nanjing 210094, People's Republic of China*
[2] *Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan*
✉ *E-mail: qin_h_w@163.com*

Abstract: A quantum secret sharing scheme based on orbital angular momentum (OAM) is proposed. The dealer generates single particles in OAM basis or angular position (ANG) basis randomly. The participants encode their private keys into the particles through performing quantum Fourier transforms. Then the dealer can use the single-particle measurements to get the shared secret. In the authors' scheme, the secret is protected by the distinguishability of OAM basis and ANG basis. Compared to the traditional two-dimensional schemes, the authors' scheme can use the higher dimension of OAM to increase the detecting rate of eavesdropping, and enhance the security in practice. Besides, only the single particles are needed in their scheme. Compared to the schemes based on entangled particles, the authors' scheme will be more practical with the present technology.

1 Introduction

Quantum secret sharing (QSS) is the extension of classical secret sharing [1] into the quantum area. It uses the quantum operations to spit a quantum state or a classical secret into several parts, and distributes to different participants. Then the qualified participants can cooperate to reconstruct the original quantum state or classical secret. Different from the classical secret sharing, the security of QSS relies on the quantum theory such as uncertainty principle and no-cloning theorem [2, 3].

Since Hillery *et al.* [2] used the GHz state to propose the first scheme, QSS has attracted lots of interests, and many kinds of schemes have been proposed [3–18]. The traditional QSS schemes usually use the two-dimensional polarisation or spin of particles to bring the secret information. Besides the polarisation and spin, the orbital angular momentum (OAM) of a particle can also be used to bring secret information. Compared to the polarisation or spin, the OAM has higher dimension in the Hilbert space. Recently, the technology of OAM has got a rapid development. For example, the optical beams carrying single OAM states have been produced by using planar plasmonic interfaces [19]. Distinctive scattering resonances in nanoplasmonic Vogel spiral arrays have also been demonstrated to carry OAM modes [20]. Besides, it has been analytically demonstrated that Vogel spiral arrays can generate multiple OAM states encoding well-defined numerical sequences in their far-field radiation patterns [21].

In this paper, we will use the OAM to propose a QSS scheme. The dealer generates the single particles in the OAM basis or the angular position (ANG) basis randomly. The participants perform the quantum Fourier transforms on the particles to encode their private keys. Then the dealer obtains the shared secret through measuring these single particles. In our scheme, we use the distinguishability of OAM basis and ANG basis to protect the secret. The dimension of the Hilbert space for OAM is higher than, for instance, polarisation or spin, and the proposed scheme can use the high dimension to increase the detecting rate of eavesdropping and enhance the security in practice. Besides, our scheme does not need the entangled particles, and only needs the single particles. Compared to the schemes based on the entangled particles, our scheme will be more practical with the present technology.

The rest of this paper is organised as follows. In Section 2, we give some correlative preliminaries. In Section 3, the design method of the proposed scheme is explicated. In Section 4, an example is given to explain the protocol more clearly. In Section 5, the correctness is proved. In Section 6, the security is analysed. Section 7 demonstrates the efficiency. Section 8 compares our scheme with some existing schemes. Finally, in Section 9, the conclusion of this paper is given.

2 Preliminaries

(1) *OAM basis*

The OAM with different values of photon can form a group of orthogonal basis, and the basis can be expressed as $\{|j\rangle,\ j = -N, \ldots, 0, \ldots, N\}$, where N is a positive integer.

(2) *ANG basis*

The ANG of photon can be expressed as $\{|\bar{j}\rangle,\ j = 0, 1, \ldots, 2N\}$, where $|\bar{j}\rangle = (1/\sqrt{2N+1})\sum_{k=-N}^{N}\omega^{-kj}|k\rangle$ and $\omega = \mathrm{e}^{(2\pi i/2N+1)}$.

Now we show that the ANG also forms a group of orthogonal basis. The proof has been done in many existing papers, for example, [22]

$$
\begin{aligned}
\langle\bar{j}|\bar{j}'\rangle &= \frac{1}{\sqrt{2N+1}}\sum_{k=-N}^{N}\omega^{kj}\langle k|\frac{1}{\sqrt{2N+1}}\sum_{k'=-N}^{N}\omega^{-k'j'}|k'\rangle \\
&= \frac{1}{2N+1}\sum_{k,k'=-N}^{N}\omega^{kj-k'j'}\langle k|k'\rangle \\
&= \frac{1}{2N+1}\sum_{k=-N}^{N}\omega^{k(j-j')}
\end{aligned}
$$

We know that $\omega = \mathrm{e}^{(2\pi i/2N+1)}$, so $\sum_{k=-N}^{N}\omega^{k} = 0$. Then $\langle\bar{j}|\bar{j}'\rangle = (1/2N+1)\sum_{k=-N}^{N}\omega^{k(j-j')} = 0$, and we can see that the ANG $\{|\bar{j}\rangle,\ j = 0, 1, \ldots, 2N\}$ can form a group of orthogonal basis.

Now, we show that the OAM basis and the ANG basis are mutually unbiased bases (MUBs), and the proof can also be found in [22] and many other papers

$$
\begin{aligned}
|\langle j|\bar{j}'\rangle| &= \left|\left\langle j\left|\frac{1}{\sqrt{2N+1}}\sum_{k=-N}^{N}\omega^{-kj'}|k\rangle\right.\right\rangle\right| \\
&= \left|\frac{1}{\sqrt{2N+1}}\omega^{-jj'}\right|
\end{aligned}
$$

$$= \left| \frac{1}{\sqrt{2N+1}} \right|$$

We can see that the OAM basis $\{|j\rangle,\ j = -N, \ldots, 0, \ldots, N\}$ and the ANG basis $\{|\bar{j}\rangle,\ j = 0, 1, \ldots, 2N\}$ are MUBs, so we can use their distinguishability to prevent the eavesdropping.

(3) *Quantum Fourier transform*

For the quantum state $|j\rangle$ in the OAM basis, the quantum Fourier transform performed on $|j\rangle$ can be described as $f(|j\rangle) = (1/\sqrt{2N+1})\sum_{k=-N}^{N} \omega^{-kj}|k\rangle$, where $\omega = \mathrm{e}^{(2\pi i/2N+1)}$, $j \in \{-N, \ldots, 0, \ldots, N\}$.

(4) *Implementation of quantum Fourier transform on OAM*

In practice, the photons with the OAM state can be generated with a beta barium borate (BBO) crystal [15], that is, a pump pulse of ultraviolet light passes through a BBO crystal and produces the photons into the OAM mode. The quantum Fourier transform and the measurements with two non-orthogonal bases in the OAM state can be realised with single-photon detectors, assisted with linear optical elements and linear polarising beam splitters (PBSs) or circular PBSs [15, 23, 24].

The OAM state can also be realised from two special Gaussion modes: Hermite–Gauss mode and Laguerre–Gauss mode, and the spatial mode interleaver can operate a quantum Fourier transform through the phase change [25]. Besides, the OAM state and its quantum Fourier transform can be implemented through the nanoplasmonic Vogel spiral arrays [21].

3 Proposed scheme

We assume the dealer Alice wants to share the secret among n participants $\{\mathrm{Bob}_1, \mathrm{Bob}_2, \ldots, \mathrm{Bob}_n\}$. The secret is $S = (s_1, s_2, \ldots, s_m)$, where $s_1, s_2, \ldots, s_m \in \{0, 1\}$. Alice uses the following steps to distribute her secret (see Fig. 1).

i. Alice generates m particles $\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ in the OAM basis or the ANG basis randomly. We assume the dimension of the basis is $(2N+1)$, that is, the state in the OAM basis can be expressed as $\{|j\rangle,\ j = -N, \ldots, 0, \ldots, N\}$, and the state in the ANG basis can be expressed as $\{|\bar{j}\rangle,\ j = 0, 1, \ldots, 2N\}$, where $|\bar{j}\rangle = (1/\sqrt{2N+1})\sum_{k=-N}^{N}\omega^{-kj}|k\rangle$ and $\omega = \mathrm{e}^{(2\pi i/2N+1)}$. The generated particles are not in the state $|0\rangle$ or $|\bar{0}\rangle$.

ii. Alice sends the m particles $\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ to Bob_1. Bob_1 randomly selects his private key $K_1 = (k_{11}, k_{12}, \ldots, k_{1m})$ and public information $V_1 = (v_{11}, v_{12}, \ldots, v_{1m})$. Then Bob_1 performs the operations as follows:

- if $k_{1l} = 0$ and $v_{1l} = 0$, he performs no operation on the particle φ_l;
- if $k_{1l} = 0$ and $v_{1l} = 1$, he performs one quantum Fourier transform on φ_l;
- if $k_{1l} = 1$ and $v_{1l} = 0$, he performs two quantum Fourier transforms on φ_l;
- if $k_{1l} = 1$ and $v_{1l} = 1$, he performs three quantum Fourier transforms on φ_l.

Where $l = 1, 2, \ldots, m$.

iii. Bob_1 sends the particles $\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ to Bob_2, and Bob_2 performs the similar operations as Bob_1,…, this process is continued until Bob_n. After Bob_n performs his operations, he sends the particles to Alice.

iv. When Alice receives the particles $\{\varphi_1, \varphi_2, \ldots, \varphi_m\}$, she asks all the participants to publish their public information $\{V_1, V_2, \ldots, V_n\}$ in random order.

v. Alice computes $v_l = 4 - [(v_{1l} + v_{2l} + \cdots + v_{nl}) \bmod 4]$, and then performs v_l quantum Fourier transforms on φ_l, $l = 1, 2, \ldots, m$. Alice measures the particle φ_l on its original basis. If the measurement result is the same as its original state, Alice sets the subsecret $s_l = 0$, otherwise, she sets $s_l = 1$. Then Alice can get the shared secret $S = (s_1, s_2, \ldots, s_m)$. In Section 5, we will prove that $S = K_1 \oplus K_2 \oplus \ldots \oplus K_n$, where $\oplus$ denotes the bitwise exclusive-OR.

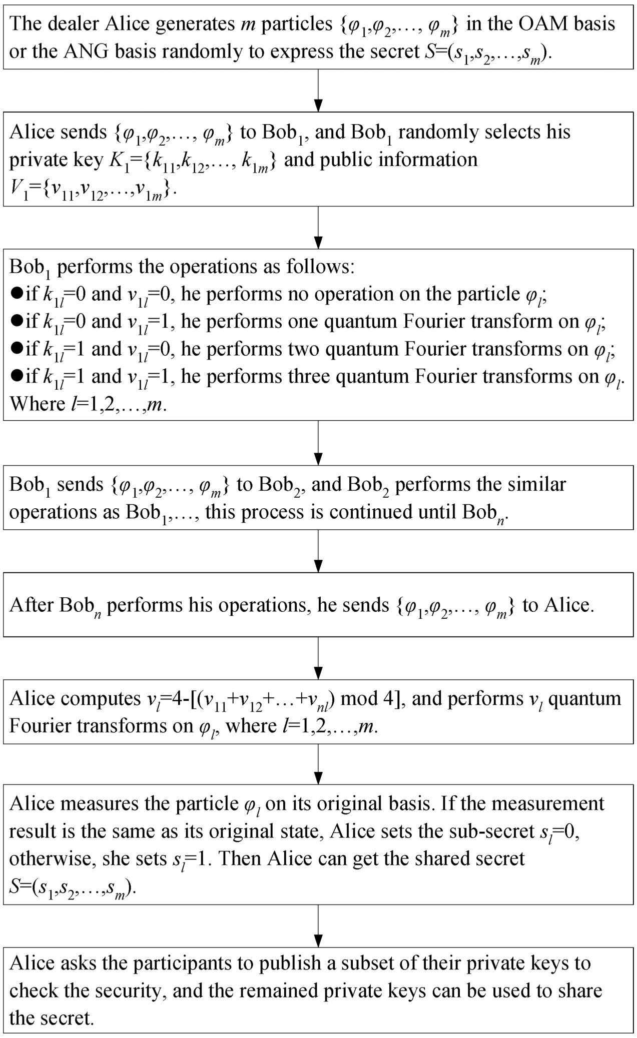
vi. Alice asks the participants to publish a subset of their private keys to check the security, and the remained private keys can be used to share the secret.

4 Example

Now, we give an example to explain our protocol more clearly. Assume Alice wants to share a 3 bit secret $S = (s_1, s_2, s_3)$ among three participants $\{\mathrm{Bob}_1, \mathrm{Bob}_2, \mathrm{Bob}_3\}$, where $m = 3$, $n = 3$. We also assume the dimension of the OAM basis is $(2N+1) = 3$. So, the quantum state in the OAM basis can be denoted as $|j\rangle,\ j \in \{-1, 0, 1\}$, and the quantum state in the ANG basis can be denoted as $|\bar{j}\rangle,\ j \in \{0, 1, 2\}$.

First, Alice generates three particles $\{\varphi_1, \varphi_2, \varphi_3\}$ in the OAM basis or the ANG basis randomly, and we assume the particles are $\varphi_1 = |-1\rangle, \varphi_2 = |\bar{1}\rangle, \varphi_3 = |\bar{2}\rangle$. Then she sends the particles to Bob_1.

Bob_1 randomly selects his private key K_1 and public information V_1. We assume $K_1 = (001)$ and $V_1 = (010)$. Then Bob_1 performs no operation on φ_1, performs one quantum Fourier transform on φ_2, and performs two quantum Fourier transforms on φ_3. The three particles will become $\varphi_1 = |-1\rangle, \varphi_2 = |-1\rangle, \varphi_3 = |\bar{1}\rangle$. Then Bob_1 sends the particles to Bob_2.



The dealer Alice generates m particles $\{\varphi_1,\varphi_2,\ldots,\varphi_m\}$ in the OAM basis or the ANG basis randomly to express the secret $S=(s_1,s_2,\ldots,s_m)$.

Alice sends $\{\varphi_1,\varphi_2,\ldots,\varphi_m\}$ to Bob_1, and Bob_1 randomly selects his private key $K_1=\{k_{11},k_{12},\ldots,k_{1m}\}$ and public information $V_1=\{v_{11},v_{12},\ldots,v_{1m}\}$.

Bob_1 performs the operations as follows:
●if $k_{1l}=0$ and $v_{1l}=0$, he performs no operation on the particle φ_l;
●if $k_{1l}=0$ and $v_{1l}=1$, he performs one quantum Fourier transform on φ_l;
●if $k_{1l}=1$ and $v_{1l}=0$, he performs two quantum Fourier transforms on φ_l;
●if $k_{1l}=1$ and $v_{1l}=1$, he performs three quantum Fourier transforms on φ_l.
Where $l=1,2,\ldots,m$.

Bob_1 sends $\{\varphi_1,\varphi_2,\ldots,\varphi_m\}$ to Bob_2, and Bob_2 performs the similar operations as Bob_1,…, this process is continued until Bob_n.

After Bob_n performs his operations, he sends $\{\varphi_1,\varphi_2,\ldots,\varphi_m\}$ to Alice.

Alice computes v_l=4-[$(v_{11}+v_{12}+\ldots+v_{nl})$ mod 4], and performs v_l quantum Fourier transforms on φ_l, where $l=1,2,\ldots,m$.

Alice measures the particle φ_l on its original basis. If the measurement result is the same as its original state, Alice sets the sub-secret $s_l=0$, otherwise, she sets $s_l=1$. Then Alice can get the shared secret $S=(s_1,s_2,\ldots,s_m)$.

Alice asks the participants to publish a subset of their private keys to check the security, and the remained private keys can be used to share the secret.

Fig. 1 *Main steps of our protocol*

Bob$_2$ randomly selects his private key $K_2 = (110)$ and public information $V_2 = (101)$. Then Bob$_2$ performs three quantum Fourier transforms on φ_1, performs two quantum Fourier transforms on φ_2, and performs one quantum Fourier transform on φ_3. The particles will become $\varphi_1 = |\bar{1}\rangle, \varphi_2 = |1\rangle,\ \varphi_3 = |-1\rangle$. Then Bob$_2$ sends the particles to Bob$_3$.

Bob$_3$ randomly selects his private key $K_3 = (010)$ and public information $V_3 = (110)$. Then Bob$_3$ performs one quantum Fourier transform on φ_1, performs three quantum Fourier transforms on φ_2, and performs no operation on φ_3. The particles will become $\varphi_1 = |-1\rangle, \varphi_2 = |\bar{2}\rangle, \varphi_3 = |-1\rangle$. Then Bob$_3$ sends the particles to Alice.

When Alice receives the particles, she asks {Bob$_1$, Bob$_2$, Bob$_3$} to publish their public information $\{V_1, V_2, V_3\}$. Alice computes $v_1 = 4 - [(v_{11} + v_{21} + v_{31}) \bmod 4] = 2$, and performs two quantum Fourier transforms on φ_1; computes $v_2 = 4 - [(v_{12} + v_{22} + v_{32}) \bmod 4] = 2$, and performs two quantum Fourier transforms on φ_2; computes $v_3 = 4 - [(v_{13} + v_{23} + v_{33}) \bmod 4] = 3$, and performs three quantum Fourier transforms on φ_3. Then the three particles will become $\varphi_1 = |1\rangle, \varphi_2 = |\bar{1}\rangle, \varphi_3 = |\bar{1}\rangle$.

We can see that the three particles have all been in their original basis. Alice measures each particle in its original basis. She will find the states of φ_1 and φ_3 have changed, but the state of φ_2 does not change. So, Alice sets the subsecrets $s_1 = 1$, $s_2 = 0$, $s_3 = 1$, and gets the shared secret $S = (s_1, s_2, s_3) = (101)$. We can see that $S = K_1 \oplus K_2 \oplus K_3$.

5 Correctness

Theorem 1: For the quantum state in the OAM basis $\{|j\rangle,\ j = -N, \dots, 0, \dots, N\}$ and quantum Fourier transform $f(|j\rangle) = (1/\sqrt{2N+1})\sum_{k=-N}^{N} \omega^{-kj}|k\rangle$, it can be obtained that $f^2(|j\rangle) = |-j\rangle$ and $f^4(|j\rangle) = |j\rangle$.

Proof:

$$f^2(|j\rangle) = \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{-kj} \left(\frac{1}{\sqrt{2N+1}} \sum_{k'=-N}^{N} \omega^{-k'k} |k'\rangle \right)$$

$$= \frac{1}{2N+1} \sum_{k=-N}^{N} \sum_{k'=-N}^{N} \omega^{-kj-k'k} |k'\rangle$$

$$= \frac{1}{2N+1} \sum_{k'=-N}^{N} \sum_{k=-N}^{N} \omega^{-k(j+k')} |k'\rangle$$

We know $\omega = e^{(2\pi i/2N+1)}$. If $j + k' \neq 0$, and we assume $j + k' = x$, then $\sum_{k=-N}^{N} \omega^{-k(j+k')} = \sum_{k=-N}^{N} \omega^{-kx} = 0$. If $j + k' = 0$, then $\sum_{k=-N}^{N} \omega^{-k(j+k')} = 2N + 1$. Therefore, only the item which satisfies $j + k' = 0$ can be retained, and the other items will disappear. So, $f^2(|j\rangle) = |-j\rangle$. Then we can continue to get $f^4(|j\rangle) = f^2[f^2(|j\rangle)] = |j\rangle$.

Lemma 1: For the quantum state in the ANG basis $\{|\bar{j}\rangle,\ j = 0, 1, \dots, 2N\}$ and quantum Fourier transform $f(|j\rangle) = (1/\sqrt{2N+1})\sum_{k=-N}^{N} \omega^{-kj}|k\rangle$, it can be obtained that $f^2(|\bar{j}\rangle) = |\overline{2N+1-j}\rangle$ and $f^4(|\bar{j}\rangle) = |\bar{j}\rangle$.

Proof: We will prove this Lemma in two cases.

(1) $j \in \{0, 1, \dots, N\}$

From the definitions of ANG basis and quantum Fourier transform in Section 2, we can know $|\bar{j}\rangle = f(j)$ when $j \in \{0, 1, \dots, N\}$. So from Theorem 1, we can get $f(|\bar{j}\rangle) = f^2(|j\rangle) = |-j\rangle$. Then

$$f^2(|\bar{j}\rangle) = f(|-j\rangle)$$

$$= \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{-k(-j)} |k\rangle$$

$$= \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{-k(2N+1-j)} |k\rangle$$

$$= |\overline{2N+1-j}\rangle$$

Therefore, $f^4(|\bar{j}\rangle) = f^2(|\overline{2N+1-j}\rangle) = |\overline{2N+1-(2N+1-j)}\rangle = |\bar{j}\rangle$.

(2) $j \in \{N+1, N+2, \dots, 2N\}$

When $j \in \{N+1, N+2, \dots, 2N\}$, we can get

$$|\bar{j}\rangle = \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{-kj} |k\rangle$$

$$= \frac{1}{\sqrt{2N+1}} \sum_{k=-N}^{N} \omega^{-k[j-(2N+1)]} |k\rangle$$

$$= f(|j-(2N+1)\rangle)$$

Then from Theorem 1, we can get $f(|\bar{j}\rangle) = f^2(|j-(2N+1)\rangle) = |2N+1-j\rangle$. From the definitions of ANG basis and quantum Fourier transform in Section 2, we can continue to get $f^2(|\bar{j}\rangle) = f(|2N+1-j\rangle) = |\overline{(2N+1-j)}\rangle$. So, $f^4(|\bar{j}\rangle) = f^2(|\overline{2N+1-j}\rangle) = |\overline{2N+1-(2N+1-j)}\rangle = |\bar{j}\rangle$.

Lemma 2: $S = K_1 \oplus K_2 \oplus \dots \oplus K_n$, where $S = (s_1, s_2, \dots, s_m)$ is the shared secret and $K_i = (k_{i1}, k_{i2}, \dots, k_{im})$ is the private key of Bob$_i$, $i \in \{1, 2, \dots, n\}$.

Proof: From Theorem 1 and Lemma 1, we know that the state of the particle φ_l ($l \in \{1, 2, \dots, m\}$) will not change if it has been performed on four quantum Fourier transforms. In step (5) of Section 3, Alice computes $v_l = 4 - [(v_{1l} + v_{2l} + \dots + v_{nl}) \bmod 4]$ and performs v_l quantum Fourier transforms on φ_l. So, the effects of public information $(v_{1l}, v_{2l}, \dots, v_{nl})$ on φ_l will be eliminated, and then we can only take into account the effects of $(k_{1l}, k_{2l}, \dots, k_{nl})$.

Without considering v_{il}, Bob$_i$ will perform no operation on φ_l when $k_{il} = 0$, and perform two quantum Fourier transforms on φ_l when $k_{il} = 1$. If $k_{1l} \oplus k_{2l} \oplus \dots \oplus k_{nl} = 0$, then the times that the participants {Bob$_1$, Bob$_2$, …, Bob$_n$} have performed quantum Fourier transform on φ_l is multiple of four, so the state of φ_l will not change, and Alice will set the subsecret $s_l = 0$ after the measurement, that is, $s_l = k_{1l} \oplus k_{2l} \oplus \dots \oplus k_{nl}$. If $k_{1l} \oplus k_{2l} \oplus \dots \oplus k_{nl} = 1$, then the times that the participants have performed quantum Fourier transform on φ_l is multiple of two, but not multiple of four. We know that φ_l is not in the state $|0\rangle$ or $|\bar{0}\rangle$, then from Theorem 1 and Lemma 1, we can know the state of φ_l has changed, but its basis does not change. So, Alice will set the subsecret $s_l = 1$ after the measurement, that is, $s_l = k_{1l} \oplus k_{2l} \oplus \dots \oplus k_{nl}$.

Through combining all the m subsecrets, we can get that $S = K_1 \oplus K_2 \oplus \dots \oplus K_n$.

6 Security

For a secure QSS scheme, it must satisfy the confidentiality, that is, each participant can keep his private key confidential, and the unqualified participants cannot get any information about the shared secret. In Section 6.1, we will analyse the confidentiality of our scheme. Besides, the secure QSS scheme should resist the attack from outside attackers or inside dishonest participants. In Section 6.2, we will show that our scheme can resist the collusion attack of dishonest participants. In Sections 6.3 and 6.4, we will show that the eavesdropping attack and the entangle-and-measure attack from outside are invalid to our scheme. In practice, the quantum channel is not ideal, so the attacker may use the imperfections of channel and device to steal the secret. In Sections 6.5 and 6.6, we will describe the security of our scheme in practice, and analyse the security for noisy quantum channel and Trojan horse attack.

6.1 Confidentiality

In our scheme, the participant performs quantum Fourier transforms on the particles according to his private key and public information. There is no correlation between the private key and the public information, and others cannot deduce his private key according to his public information. Besides, each particle may be in the OAM basis or the ANG basis randomly, and may be in the state from $\{|-N\rangle, \dots, |0\rangle, \dots, |N\rangle\}$ or $\{|\bar{0}\rangle, |\bar{1}\rangle, \dots, |\overline{2N}\rangle\}$ with the same probability. The attacker cannot know the participant's operations on the particles through measuring the particles.

The shared secret is obtained by taking the exclusive-OR of the bits of all the private keys, that is, the secret can be recovered only all the n participants are available, and even if n–1 participants cannot get any information about the secret. So, our scheme can meet the confidentiality of QSS.

6.2 Security for collusion attack

Some dishonest participants may cooperate to steal secret information of other participants. Without loss of generality, we assume Bob$_{i-1}$ and Bob$_{i+1}$ want to steal the private key of Bob$_i$. Bob$_{i-1}$ forges some particles and sends them to Bob$_i$. After Bob$_i$ performs quantum Fourier transforms and sends the particles to Bob$_{i+1}$, Bob$_{i-1}$ tells Bob$_{i+1}$ the original basis and states of the particles. Then Bob$_{i+1}$ can get the private key of Bob$_i$ through measuring these particles. What is more, if Bob$_1$ and Bob$_n$ collaborate, they can get the shared secret.

However, in our scheme, this collusion will not succeed. When Bob$_i$ receives the particles, if $v_{il} = 1$, he will change the basis of the particle φ_l through quantum Fourier transform; if $v_{il} = 0$, he will not change the basis of φ_l. So, Bob$_{i+1}$ cannot know the basis of φ_l after the operations of Bob$_i$, and cannot steal the private key of Bob$_i$ through measuring φ_l.

6.3 Security for eavesdropping attack

Alice generates the original particles in the OAM basis or the ANG basis randomly. So, the attacker or the dishonest participant cannot know the basis of each particle. From Section 2, we know that the OAM basis and the ANG basis are MUBs. If the attacker measures the particle with a random basis, he will select the wrong basis with the probability 1/2, and then the dealer Alice will get the wrong value with the probability $2N/2N + 1$. So, the error rate of one particle for eavesdropping is $N/2N + 1$. Through checking the public subset of secret, Alice can find the eavesdropping easily.

In the traditional two-dimensional scheme, the error rate of one particle caused by the eavesdropping is only 1/4 [18]. We can see that the particle in our scheme has higher detecting rate for eavesdropping, and this can enhance the security in practice.

6.4 Security for entangle-and-measure attack

In this kind of attack, the attacker entangles an ancillary particle on the secret particle, and then measures the ancillary particle to steal information. For example, the attacker generates an ancillary particle $\psi = |i\rangle$ in the OAM basis, and then he performs a quantum SUM gate on φ_l and ψ, where the control particle is φ_l and the target particle is ψ. Then φ_l and ψ will compose an entangled state. If φ_l is in the OAM basis, and we assume its state is $\varphi_l = |j\rangle$, then the ancillary particle will become $\psi = |i + j\rangle$ after the quantum SUM gate. The attacker can get the state of φ_l through measuring ψ, and does not leave any trace on φ_l. However, if φ_l is in the ANG basis, the attacker will not get the state of φ_l, and he will commit the error rate $2N/2N + 1$ on φ_l. In summary, the error rate caused by the entangle-and-measure attack is $N/2N + 1$, which is the same as the eavesdropping. So, Alice can find this attack through checking the public subset of secret.

6.5 Security for noisy quantum channel

In practice, there is noise in the quantum channel, and the noise may bring some errors into the transmitted particles. If the error rate caused by the eavesdropping is lower than the error rate caused by the noise, the attacker will be able to hide his eavesdropping into the noise, and then the scheme will not be secure. According to the existing results [26–30], the noise in practical quantum channel is about from 2 to 8.9%. However, as described in Section 6.3, in our scheme, the error rate of one particle caused by the eavesdropping is $N/2N + 1$, which is much higher than the error rate caused by the noise. Therefore, the attacker cannot hide his eavesdropping into the noise, and our scheme will be secure in the noisy environment.

6.6 Security for Trojan horse attack

As described in Section 2, in practice, the particles used in our scheme can be the photons, and then the attacker may launch two kinds of Trojan horse attacks: the multiple photon attack and the invisible photon attack. In the multiple photon attack, Bob$_{i-1}$ sends a state with more than one photon so that Bob$_{i+1}$ can measure in different basis to find which operations Bob$_i$ performed. In the invisible photon attack, Bob$_{i-1}$ sends a state with invisible photons (which cannot be detected by Bob$_i$), and Bob$_{i+1}$ can measure the invisible photons to find the operations Bob$_i$ performed.

In order to resist the multiple photon attack, the participant must judge each received photon is a single photon or a multi-photon. He can use the technology of photon number splitter (PNS) to realise it. The participant will randomly select a subset of the received photon signals as sample signals, and split each sampling signal with a PNS. Then he measures the two signals with the OAM basis or the ANG basis randomly. If there is a multiple photon attack, the multi-photon rate will be unreasonably high. For stopping the invisible photon attack, the participant can add a filter before his receiving device. The filter only allows the photon signals whose wavelengths are close to the operating one to come through, and the hidden invisible photons will be filtered out.

7 Efficiency

In our scheme, the dealer needs to generate m particles to share an m-bit secret, and the participants do not need to generate particles. The dealer sends the particles to the participants, and then the particles can be transmitted among the participants without the supervision of the dealer. The particles need to be transmitted $n + 1$ times when there are n participants. The utilisation efficiency of the particles is 100%, which is much higher than the schemes based on the BB84 protocol.

The participant selects his private key by himself, and then performs quantum Fourier transforms according to his private key and public information. The number of quantum Fourier transforms one participant needs to perform is from 0 to 3 m, that is, one participant needs to perform an average of $3m/2$ quantum Fourier transforms.

The dealer needs to perform m single-particle measurements to get the shared secret. Only single particles are needed in our scheme, and the generation or measurement for entangled state is not needed. Compared to the schemes based on the entangled state, our scheme will be more practical with the present technology.

8 Comparison

Wang *et al.* [15] used the OAM state to design a three-party QSS scheme. In their scheme, one participant generates the particles, and the other participant measures the particles with the two bases randomly as BB84 protocol. The dealer is in the middle of two participants and uses the unitary operations to encode the secret on the particles, and share his secret among the two participants. Wang's scheme can only share the secret among two participants, and it cannot be extended to a multi-party scheme. So, its application will be limited in practice. Like BB84 protocol, Wang's scheme only uses about half of the particles to transmit the secret, and the other particles are used to check the eavesdropping. So, the utilisation efficiency of the particles is low.

Guo and Zhao [31] used the Chinese remainder theory and the OAM in multi-dimensional Hilbert space to propose another QSS scheme. Guo's scheme needs the OAM entangled state, and the generation of the OAM entangled state is very complicated, that is, the dealer generates the spin angular momentum (SAM) and OAM hybrid-entanglement state, and then performs the entanglement measurement on SAM to generate the OAM entangled state. The dealer uses the OAM entangled state to distribute the secret to two participants. The two participants perform the OAM BELL-state measurement and use the Chinese remainder theory to recover the secret. The generation and measurement for the OAM entangled state in Guo's scheme are not easy with the present technology. Besides, if Guo's scheme is extended to multi-party, the multi-particle GHz hybrid-entanglement state will be needed. The generation and measurement of this state will be more difficult, and it will seriously influence the practicability of the scheme.

Our scheme does not need the entangled state. The dealer only needs to generate and measure the single particles, and it will be more efficient with the present technology. Besides, our scheme can realise the multi-party QSS easily, and it will be more practical than Wang's and Guo's three-party schemes.

9 Conclusion

In this paper, we have proposed a QSS scheme based on the OAM and quantum Fourier transform. The participants use the quantum Fourier transform to encode their private keys, and the dealer uses the single-particle measurement to obtain the shared secret. The secret is protected by the distinguishability of OAM basis and ANG basis. The higher dimension of OAM basis can increase the detecting rate of eavesdropping. Besides, in our scheme, only the single particles are needed, so it will be more practical than the schemes based on the entangled particles.

10 References

[1] Shamir, A.: 'How to share a secret', *Commun. ACM*, 1979, **22**, pp. 612–613

[2] Hillery, M., Buzek, V., Berthiaume, A.: 'Quantum secret sharing', *Phys. Rev. A*, 1999, **59**, pp. 1829–1834

[3] Cleve, R., Gottesman, D., Lo, H.K.: 'How to share a quantum secret', *Phys. Rev. Lett.*, 1999, **83**, pp. 648–651

[4] Tyc, T., Sanders, B.C.: 'How to share a continuous-variable quantum secret by optical interferometry', *Phys. Rev. A*, 2002, **65**, p. 042310

[5] Yang, Y.G., Jia, X., Wang, H.Y., *et al.*: 'Verifiable quantum (k, n)-threshold secret sharing', *Quantum Inf. Process.*, 2012, **11**, pp. 1619–1625

[6] Li, Q., Long, D.Y., Chan, W.H., *et al.*: 'Sharing a quantum secret without a trusted party', *Quantum Inf. Process.*, 2011, **10**, pp. 97–106

[7] Gao, G.: 'Secure multiparty quantum secret sharing with the collective eavesdropping-check character', *Quantum Inf. Process.*, 2013, **12**, pp. 55–68

[8] Shi, R.H., Lv, G.L., Wang, Y., *et al.*: 'On quantum secret sharing via Chinese remainder theorem with the non-maximally entanglement state analysis', *Int. J. Theor. Phys.*, 2013, **52**, pp. 539–548

[9] Tseng, H.Y., Tsai, C.W., Hwang, T., *et al.*: 'Quantum secret sharing based on quantum search algorithm', *Int. J. Theor. Phys.*, 2012, **51**, pp. 3101–3108

[10] Lau, H.K., Weedbrook, C.: 'Quantum secret sharing with continuous-variable cluster states', *Phys. Rev. A*, 2013, **88**, p. 042313

[11] Chen, R.K., Zhang, Y.Y., Shi, J.H., *et al.*: 'A multiparty error-correcting method for quantum secret sharing', *Quantum Inf. Process.*, 2014, **13**, pp. 21–31

[12] Xiao, H.L., Gao, J.L.: 'Multi-party d-level quantum secret sharing scheme', *Int. J. Theor. Phys.*, 2013, **52**, pp. 2075–2082

[13] Wei, Y.Z., Jiang, M.: 'Multi-qudit state sharing via various high-dimensional Bell channels', *Quantum Inf. Process.*, 2015, **14**, pp. 1091–1102

[14] Sarvepalli, P.K., Klappenecker, A.: 'Sharing classical secrets with Calderbank-Shor-Steane codes', *Phys. Rev. A*, 2009, **80**, p. 022321

[15] Wang, H.B., Huang, Y.G., Fang Gu, X.B., *et al.*: '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.*, 2013, **52**, pp. 1043–1051

[16] Liu, L.L., Tsai, C.W., Hwang, T.: 'Quantum secret sharing using symmetric W state', *Int. J. Theor. Phys.*, 2012, **51**, pp. 2291–2306

[17] Wang, J.T., Xu, G., Chen, X.B., *et al.*: 'Local distinguishability of Dicke states in quantum secret sharing', *Phys. Lett. A*, 2017, **381**, pp. 998–1002

[18] Hsu, J.L., Chong, S.K., Hwang, T., *et al.*: 'Dynamic quantum secret sharing', *Quantum Inf. Process.*, 2013, **12**, pp. 331–344

[19] Yu, N., Genevet, P., Kats, M.A., *et al.*: 'Light propagation with phase discontinuities: generalized laws of reflection and refraction', *Science*, 2011, **334**, pp. 333–337

[20] Trevino, J., Cao, H., Negro, L.D.: 'Circularly symmetric light scattering from nanoplasmonic spirals', *Nano Lett.*, 2011, **11**, pp. 2008–2016

[21] Negro, L.D., Trevino, J., Lawrence, N.: 'Analytical light scattering and orbital angular momentum spectra of arbitrary Vogel spirals', *Opt. Express*, 2012, **20**, pp. 18209–18223

[22] Durt, T., Englert, B.G., Bengtsson, I., *et al.*: 'On mutually unbiased bases', *Int. J. Quantum Inf.*, 2010, **8**, pp. 535–640

[23] Sheng, Y.B., Deng, F.G.: 'One-step deterministic polarization-entanglement purification using spatial entanglement', *Phys. Rev. A*, 2010, **82**, p. 044305

[24] Gu, B., Fei, X., Ding, L.G., *et al.*: 'High-capacity three-party quantum secret sharing with hyperentanglement', *Int. J. Theor. Phys.*, 2012, **51**, pp. 3559–3566

[25] Zhou, K.H., Wang, Y., Wang, T.J., *et al.*: 'Implementation of high capacity quantum secret sharing using orbital angular momentum of photons', *Int. J. Theor. Phys.*, 2014, **53**, pp. 3927–3934

[26] Jennewein, T., Simon, C., Weihs, G., *et al.*: 'Quantum cryptography with entangled photons', *Phys. Rev. Lett.*, 2000, **84**, pp. 4729–4732

[27] Hughes, R.J., Nordholt, J.E., Derkacs, D., *et al.*: 'Practical free-space quantum key distribution over 10 km in daylight and at night', *New J. Phys.*, 2002, **43**, pp. 1–14

[28] Stucki, D., Gisin, N., Guinnard, O., *et al.*: 'Quantum key distribution over 67 km with a plug&play system', *New J. Phys.*, 2002, **41**, pp. 1–8

[29] Beveratos, A., Brouri, R., Gacoin, T., *et al.*: 'Single photon quantum cryptography', *Phys. Rev. Lett.*, 2002, **89**, p. 187901

[30] Gobby, C., Yuan, Z.L., Shields, A.J.: 'Quantum key distribution over 122 km standard telecom fiber', *Appl. Phys. Lett.*, 2004, **84**, pp. 3762–3764

[31] Guo, Y., Zhao, Y.Q.: 'High-efficient quantum secret sharing based on the Chinese remainder theorem via the orbital angular momentum entanglement analysis', *Quantum Inf. Process.*, 2013, **12**, pp. 1125–1139