# Quantum Secret Sharing Scheme with Credible Authentication based on Quantum Walk

**Xue-Yang Li[1], Yan Chang[1*] and Shi-Bin Zhang[1]**
[1] School of Cyberspace Security, Chengdu University of Information Technology
Chengdu 610225, Sichuan, China
[e-mail: cyttkl@cuit.edu.cn]
*Corresponding author: Yan Chang

*Received March 4, 2020; revised May 6, 2020; accepted June 2, 2020; published July 31, 2020*

## Abstract

Based on the teleportation by quantum walk, a quantum secret sharing scheme with credible authentication is proposed. Using the Hash function and quantum local operation, combined with the two-step quantum walks circuit on the line, the identity authentication and the teleportation of the secret information in distribution phase are realized. Participants collaborate honestly to recover secret information based on particle measurement results, preventing untrusted agents and external attacks from obtaining useful information. Due to the application of quantum walk, the sender does not need to prepare the necessary entangled state in advance, simply encodes the information to be sent in the coin state, and applies the conditional shift operator between the coin space and the position space to produce the entangled state necessary for quantum teleportation. Security analysis shows that the protocol can effectively resist intercept/resend attacks, entanglement attacks, participant attacks, and impersonation attacks. In addition, the quantum walk circuit used has been implemented in many different physical systems and experiments, so this quantum secret sharing scheme may be achievable in the future.

***Keywords:*** Quantum Secret Sharing, Authentication, Quantum Walk, Teleportation, Qubit

## 1. Introduction

Quantum Secret Sharing (QSS) is a combination of classical secret sharing and quantum theory, which allows secret information (classical information or quantum encoded information) to be distributed, transmitted, and restored through quantum operations. Imagining Alice wants to hand over a secret plan to Bob and Charlie in the distance, but she is not completely trusting Bob and Charlie. Secret sharing protocols play an important role in the above scenarios, and the security of QSS is based on the fundamentals of quantum mechanics, which makes QSS safer than traditional secret sharing. The earliest QSS scheme was proposed by Hillery et al in 1999[1], they used the Greenberger-Horne-Zeilinger (GHZ) entangled state to complete secret sharing. With the development of quantum information, numerous quantum protocols and algorithms have been presented with entanglement and without entanglement[2-9], and the QSS protocols are no exception[10-13].

In reality, there is a situation where an illegal imposter pretends to impersonate Alice to issue a fake command, directing Bob and Charlie to complete an illegal task. However, in the various schemes mentioned above, it is presupposed that “Alice is legal, at least one of Bob and Charlie is credible”, only the segmentation of the message is discussed regardless of the identity authentication. Recently, Qin et al[14] proposed a QSS scheme using phase shift operation, they pointed out that identity authentication should be applied to avoid man-in-the-middle attacks in QSS scheme. This shows that identity authentication is needed in QSS schemes to prevent internal and external attacks. In fact, as early as 2008, Yang et al[15] had proposed a multi-party quantum identity authentication protocols to share secret information, the protocol do not use entangled states, but it can not ensure the safety of particle transmission, Zhang and Ji[16] pointed out that the protocol was vulnerable to participant attacks, resulting in the disclosure of secret information. Researchers began to use entangled states to ensure the security of QSS scheme with credible authentication, Yang et al [17] proposed a (t,n) QSS scheme with identity authentication based on GHZ states in 2012, Abulkasim H.[18] proposed a authenticated QSS scheme based on Bell states in 2016.

Quantum walk is the quantum correspondence of classic walk, first proposed by Aharonov etal in 1993[19]. Quantum walks show meaningful applications in many ways[20, 21], and applications in communication protocols are beginning to emerge [22-24]. In the past two years, Wang et al[22] and Shang et al[23] proposed the successful application of different models of quantum walk in teleportation. It pointed out that the necessary entangled states do not need to be prepared in advance, but they can spontaneously produce during walking. Since quantum walk has been proven to be possible in many different physical systems[25-27], and many quantum signature schemes based on quantum walk have been proposed[28, 29].

Therefore, this paper proposes the first QSS scheme based on quantum walk by applying the teleportation based on quantum walk to QSS for secret information transmission. The proposed scheme has the following advantages:

1.The credible authenticated protocol complete identity authentication between parties based on hash functions and quantum operations, avoiding participant attacks.

2.The entangled state does not need to be prepared in advance, the entangled state necessary for teleportation is generated by the single particles in the quantum walk process.

3.The one-dimensional two-step quantum walks circuit used in the paper is achievable, so the proposed QSS scheme may be achievable.

The rest of this manuscript is outlined as follows. Section 2 introduces the preliminaries. Section 3 introduces the proposed scheme. Section 4 analyzes the security of the proposed scheme. Section 5 gives the efficiency of the proposed scheme and the comprehensive comparisons between the proposed scheme and other existing schemes. Finally, section 6 concludes the work.

## 2. Preliminaries

### 2.1 Coding mechanism and multi-photon deception signal detecting device

The preparations required for identity authentication of our QSS scheme is similar to that of Ref[30], that is the participant and the secret distributor shares the participant's identity sequence and a one-way Hash function with an output length of $N$, which is kept secret to any third party. Take participant Bob as an example, Bob's $N$-bit authentication key shared with Alice can be calculated as $h_{Bob}(S_{ID\text{-}Bob})$, where $h_{Bob}()$ is the Hash function negotiated jointly by Bob and Alice, $S_{ID\text{-}Bob}$ is Bob's identity sequence, we do not have to limit the length of each participant's $S_{ID}$ to be equal.

Our QSS scheme uses the Pauli operations and Hadamard operation to encode classical information onto quantum states.

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| \tag{1}$$

$$\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{2}$$

$$\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{3}$$

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|) \tag{4}$$

In addition, in order to detect multi-photon deception signal attack, prevent operations on photons by secret distributor from being stolen, we use photon beam splitter(PBS) to detect multi-particle deception signal attack, the implementation is shown in **Fig. 1**.

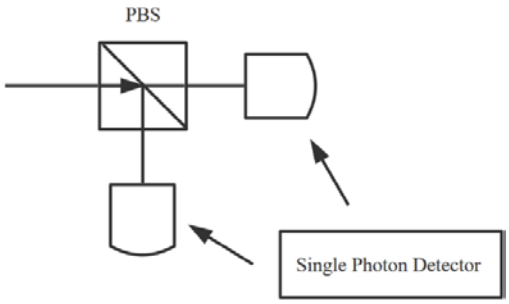


**Fig. 1.** Multi-photon deception signal detecting by using PBS

The secret distributor Alice splits each of the signal used for detection by using PBS and measures it with the single photon detector. If the initial signal before splitting contains only one photon, only one detector will detect photon; if it is a multi-photon signal, it is likely that more than one detector will detect photon. This is the principle of multi-particle deception signal attack detection by using PBS.

### 2.2 One-dimensional quantum walk model on the line

The definition of a coin-based quantum walk model on the line was proposed by Ambainis et al[31] in 2001.

It takes place in a compound Hilbert space consists of two main quantum spaces, position space and coin space, expressed as

$$H = H_{\mathrm{p}} \otimes H_{\mathrm{c}} \tag{5}$$

where $H_{\mathrm{p}}$ represents the position span $\{n, n \in Z\}$, and $H_{\mathrm{c}}$ represents the coin direction of the walk $\{|0\rangle, |1\rangle\}$, each step of the quantum walk can be described as

$$W^{(l)} = E^{(l)} \cdot (I \otimes C) \tag{6}$$

where $E^{(l)} = S \otimes |0\rangle\langle 0| + S^{?} \otimes |1\rangle\langle 1|$ , $S$ is called the shift operator and denoted as $S = \sum_n |n+1\rangle\langle n|$, and $C$ is the coin operator acting on coin space. The walker moves from $|n\rangle$ to $|n+1\rangle$ if the tossed coin is $|0\rangle$ and steps backwards to $|n-1\rangle$ if the tossed coin is $|1\rangle$.

In the past two years, Wang et al[22] and Shang et al[23] have successfully applied quantum walk to the communication protocol of particle teleportation. In detail, the conditional shift operator can introduce entanglement between position space and coin space, this entanglement resource can be used as quantum channel for teleportation. In order to teleport secret information, we use one-dimensional quantum walk model on the line.

Suppose Alice wants to transmit an unkown qubit state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob, where $|\alpha|^2 + |\beta|^2 = 1$, in order to complete the teleportation, Alice prepares particles $A_{\mathrm{p}}$, $A_1$ and $B$, $A_{\mathrm{p}}$ contains the state of the position space, $A_1$ contains the state of the unknown qubit which can also be denoted as Coin1, particle $B$ can be denoted as Coin2. The initial states of particle $A_{\mathrm{p}}$ and $B$ are both $|0\rangle$. After two steps of the walk we can finish the teleportation task.

The first step of the walk can be described as

$$W^{(1)} = E^{(1)} \cdot (A_{\mathrm{p}} \otimes C_1 \otimes B) \tag{7}$$

where $E^{(1)} = S \otimes |0\rangle_1\langle 0| \otimes B + S^{?} \otimes |1\rangle_1\langle 1| \otimes B$, $C_1$ is the coin operation acting on Coin1-$A_1$, in our scheme we choose $I$ operation as $C_1$.

And the second step of the walk can be described as

$$W^{(2)} = E^{(2)} \cdot (A_p \otimes A_1 \otimes H) \tag{8}$$

where $E^{(2)} = S \otimes A_1 \otimes |0\rangle_2\langle 0| + S^{?} \otimes A_1 \otimes |1\rangle_2\langle 1|$, $H$ means the Hadamard operation acting on Coin2-$B$.

After the two-step quantum walks, Alice sends the particle $B$ to Bob. Alice measures particle $A_1$ with basis $X(X=\{|+\rangle, |-\rangle\})$, the measurement results $|+\rangle$ and $|-\rangle$ are marked as 1 and -1 respectively, record the collection of measurement results as $\lambda 1$. After that, Alice measures $A_{\mathrm{p}}$ with basis $|Q\rangle = \{|-2'\rangle, |-1\rangle, |0\rangle, |1\rangle, |2'\rangle\}$ , where $|2'\rangle = 1/\sqrt{2}(|-2\rangle + |2\rangle)$ and $|-2'\rangle = 1/\sqrt{2}(|-2\rangle - |2\rangle)$, $|-2'\rangle$ and $|0\rangle$ and $|2'\rangle$ are marked as -1 and 0 and 1 respectively, record the collection of measurement results as $\lambda 2$.

Alice informs Bob of $\lambda 1$ and $\lambda 2$, Bob performs the corresponding Pauli operations on particle $B$ to get the unknown qubit state of $A_1$ according to **Table 1**.

**Table 1.** The relationship between measurement result and Pauli operation

| $A_1$ | $A_p$ | Revise operation |
|---|---|---|
| 1(-1) | 1(-1) | $I$ |
| 1(-1) | -1(1) | $\sigma_z$ |
| 1 | 0 | $\sigma_x$ |
| -1 | 0 | $\sigma_z \sigma_x$ |

## 3. Quantum secret sharing scheme with credible authentication based on quantum walk

In our QSS scheme, Alice is the secret distributor, Bob and Charlie are the participants. The protocol involves four phases: the particle preparation phase, the identity authentication phase, the secret information encoding phase, the secret information distribution phase and the secret information recovery phase. **Fig. 2** depicts the steps of the proposed scheme, which can be described in detail as follows.

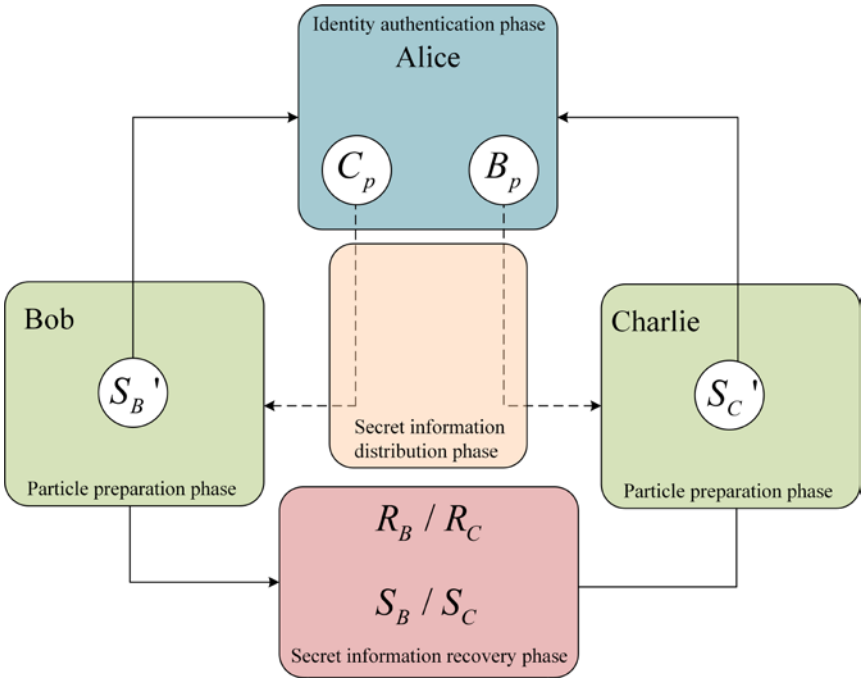


**Fig. 2.** General process of the proposed scheme

### 3.1 Particle preparation phase

1. Bob and Charlie prepare $N$-bit single photons randomly at one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the two qubit sequences formed are denoted as $S_B$ and $S_C$ respectively.
2. Bob performs the following operations on each photon in the $S_B$ according to its own authentication key $h_{Bob}(S_{ID\text{-}Bob})$: if the $i$th value of $h_{Bob}(S_{ID\text{-}Bob})$ is 0, he does an $I$ operation on the $i$th photon of the qubit sequence $S_B$; if the $i$th value of $h_{Bob}(S_{ID\text{-}Bob})$ is 1, he does a $H$ operation on the $i$th photon of the qubit sequence $S_B$. Similarly, Charlie also performs the above operations on each photon of $S_C$ according to his own authentication key $h_{Charlie}(S_{ID\text{-}Charlie})$. Record the $S_B$ and $S_C$ after operation as $S_B$' and $S_C$'.

3. After completing the above operation, Bob and Charlie send $S_B$' and $S_C$' to Alice.

### 3.2 Identity authentication phase

1. When Alice receives $S_B$' and $S_C$', she performs the same operations as the step 2 of the particle preparation phase on the photons in $S_B$' and $S_C$' according to the authentication keys $h_{Bob}(S_{ID\text{-}Bob})$ and $h_{Charlie}(S_{ID\text{-}Charlie})$ she owns. After operation, $S_B$' and $S_C$' revert to $S_B$ and $S_C$.
2. Alice selects enough photons from $S_B$ and $S_C$ as sample particles to detect multi-particle spoofing signal attacks. Assuming the number of samples particles in both qubit sequences is *N-t*, Alice let the samples particles pass through the device shown in *Fig* 1(the split ratio of PBS is 50:50). The measurement bases of the photon detector is randomly selected from the *Z* base and the *X* base. In detecting the result, if the rate of multiple photons is lower than the Pre-determined threshold, Alice announces that the communication is invalid, Alice starts to authenticate Bob and Charlie. Otherwise, Alice informing Bob and Charlie to restart the scheme.
3. Alice announces the location of the sample particles and all measurement results, Bob and Charlie announced which locations do not match the initial states when they were prepared. If the error rate is lower than the predetermined threshold, Bob and Charlie are authenticated by Alice and the quantum channels are considered safe, they proceed to the next phase. Otherwise, Alice decides whether to conduct a new round of secret sharing.

### 3.3 Secret information encoding phase

1. Alice holds the remaining *t* particles of the unknown qubit information sequence $S_B$. It can be described as

$$|S_B\rangle=\{|S_{B1}\rangle,|S_{B1}\rangle,...,|S_{Bi}\rangle,...,|S_{Bt}\rangle\} \tag{9}$$

where $|S_{Bi}\rangle$ ($i$ = 1, 2, · · ·, $n$) represents a single qubit, recorded as

$$|S_{Bi}\rangle=\alpha_i|0\rangle+\beta_i|1\rangle \tag{10}$$

where $\alpha_i$ and $\beta_i$ are complex numbers and satisfy $|\alpha_i|^2+|\beta_i|^2=1$.

Alice prepares another two particle sequences $A_p$ and $B_p$ of length *t*, the initial states of $A_p$ and $B_p$ are both $|0\rangle$. Considering a two-coin-based quantum walk model on the line, Alice uses particles $A_p$, $S_B$ and $B_p$ to build a quantum walk circuit. In the circuit, Alice takes the particles $A_p$ as the displacement space,the particles $S_B$ as the Coin1 space, the particles $B_p$ as the Coin2 space. Take particles $A_{pi}$, $S_{Bi}$(Coin1) and $B_{pi}$(Coin 2) as an example, the general initial state $|\Phi\rangle^{(0)}$ of the walk system is

$$\begin{aligned}|\Phi\rangle^{(0)}&=A_{pi}\otimes S_{Bi}\otimes B_{pi}\\&=|0\rangle_p\otimes(\alpha|0\rangle+\beta|1\rangle)_1\otimes|0\rangle_2\end{aligned} \tag{11}$$

Note that all the particle states in our system are written in the order of $A_p$, $S_B$ and $B_p$ particles.

After the first step of the quantum walk evolutionary operator $W_1$, the initial quantum state of the system based on the conditional phase shift rule evolves to

$$\left|\Phi\right\rangle^{(1)} = \left(\alpha\left|100\right\rangle + \beta\left|-110\right\rangle\right)_{p12} \tag{12}$$

After the second step of the quantum walk evolutionary operator $W_2$, the final state $\left|\Phi\right\rangle^{(2)}$ of the system is also based on the phase shift rule

$$\left|\Phi\right\rangle^{(2)} = \left(\alpha\left|200\right\rangle + \alpha\left|001\right\rangle + \beta\left|010\right\rangle + \beta\left|-211\right\rangle\right)_{p12} \tag{13}$$

After completing the above operation, particles $A_p$, $S_B$ and $B_p$ are entangled.

2. Alice encodes the secrets(length: $t$-bit) she wants to share as Pauli operations: $0\leftrightarrow I$, $1\leftrightarrow\sigma_x$, applying on each particle $S_{Bi}$, record the particles encoded by the secret information as $M_B$. Introduce the two-step quantum walks of $A_p$, $S_B$ and $B_p$ particles and this Pauli operation on $S_B$ particles in detail.

$$\begin{aligned}\left|\Phi\right\rangle^{(1)} &= E^{(1)}\cdot(A_p\otimes C_1\otimes S_B)\\ &= (\left|1\right\rangle_p\left\langle 0\right|\otimes\left|0\right\rangle_1\left\langle 0\right| + \left|-1\right\rangle_p\left\langle 0\right|\otimes\left|1\right\rangle_1\left\langle 1\right|)\otimes\left|0\right\rangle_2\cdot\left(\left|0\right\rangle_p\otimes(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)_1\right)\\ &= (\alpha\left|100\right\rangle+\beta\left|-110\right\rangle)_{p12}\end{aligned} \tag{14}$$

It can be found that after $W^{(1)}$, the position space particle $A_p$ and the coin space particle $S_B$ have been entangled, their composite state changes from $(\alpha\left|0\right\rangle+\beta\left|1\right\rangle)_1\otimes\left|0\right\rangle_p$ to $(\alpha\left|10\right\rangle+\beta\left|-11\right\rangle)_{p1}$.

$$\begin{aligned}\left|\Phi\right\rangle^{(2)} &= E^{(2)}\cdot(I_{p1}\otimes H\otimes B_p)\\ &= E^{(2)}\cdot[(\alpha\left|10\right\rangle+\beta\left|-11\right\rangle)_{p1}\otimes(\left|0\right\rangle+\left|1\right\rangle/\sqrt{2})_2]\\ &= \left(S\otimes\left|0\right\rangle_2\left\langle 0\right| + S^{\dagger}\otimes\left|1\right\rangle_2\left\langle 1\right|\right)\\ &\quad\cdot(\alpha\left|100\right\rangle+\beta\left|-110\right\rangle+\alpha\left|101\right\rangle+\beta\left|-111\right\rangle)_{p12}/\sqrt{2}\\ &= (\left|2\right\rangle_p\left\langle 1\right|\otimes\left|0\right\rangle_2\left\langle 0\right| + \left|0\right\rangle_p\left\langle 1\right|\otimes\left|1\right\rangle_2\left\langle 1\right|)\\ &\quad\cdot(\alpha\left|100\right\rangle+\beta\left|-110\right\rangle+\alpha\left|101\right\rangle+\beta\left|-111\right\rangle)_{p12}/\sqrt{2}\\ &= (\alpha\left|200\right\rangle+\alpha\left|001\right\rangle+\beta\left|010\right\rangle+\beta\left|-211\right\rangle)_{p12}/\sqrt{2}\end{aligned} \tag{15}$$

After $W^{(2)}$, the coin space particles $S_B$ and $B_p$ are also entangled. If Alice does Pauli operation $I$ on $S_{Bi}$, the general state do not change, if Alice does Pauli operation $\sigma_x$ on $S_{Bi}$, the general state evolves to $(\alpha\left|210\right\rangle+\alpha\left|011\right\rangle+\beta\left|000\right\rangle+\beta\left|-201\right\rangle)_{p12}/\sqrt{2}$.

3. For another unknown qubit information sequence $S_C$, the same as steps 1-4 in this phase, Alice prepares additional particles $A_p$ as the displacement space and the particles $C_p$ as the Coin2, takes the particles $S_C$ as the Coin1, uses particles $A_p$, $S_C$ and $C_p$ to build another quantum walk circuit. After two-step quantum walks, Alice applies the same Pauli operations sequence to encode particles $S_C$, gets the secret encoded particles $M_C$.

### 3.4 Secret information distribution phase

1. After completing the above operation, Alice sends particle sequence $B_p$ to Charlie, particle sequence $C_p$ to Bob.

2. Bob and Charlie apprize Alice after receiving $C_{\mathrm{p}}$ and $B_{\mathrm{p}}$. Charlie uses particle $B_{\mathrm{p}}$ to complete the teleportation with Alice's particle $M_{\mathrm{B}}$. Alice measures $M_{\mathrm{B}}$ with basis $X$, the measurement results $\lambda 1$ is recorded as: $|+\rangle \leftrightarrow 1$, $|-\rangle \leftrightarrow$-1. Then, Alice measures $A_{\mathrm{p}}$ with basis $Q$, the measurement results $\lambda 2$ is recorded as: $|-2'\rangle \leftrightarrow$-1, $|0\rangle \leftrightarrow 0$, $|2'\rangle \leftrightarrow 1$. Alice announces $\lambda 1$ and $\lambda 2$ to Charlie.
3. According to $\lambda 1$ and $\lambda 2$, Charlie does the revise Pauli operation on particle string $B_{\mathrm{p}}$ depending on Table1 to recover the target state. After this, Charlie completes the teleportation of unknown qubit state from Alice, the states of $B_{\mathrm{p}}$ convert to the states of $M_{\mathrm{B}}$. Explain in detail the particle state recovery process as follows.
   If Alice does Pauli operation $I$ on $S_{\mathrm{B}i}$ and measures particle $S_{\mathrm{B}i}$, particle $A_{\mathrm{p}i}$ and $B_{\mathrm{p}i}$ will collapse to the corresponding state.

$$\begin{aligned}&(a|200\rangle + a|001\rangle + b\,|\,010\rangle + b\,|\,-211\rangle)_{\mathrm{p}12}\\ &=(|+\rangle_1(a\,|\,20\rangle + a\,|\,01\rangle + b\,|\,00\rangle + b\,|\,-21\rangle)_{\mathrm{p}2} +\\ &\quad |-\rangle_1(a\,|\,20\rangle + a\,|\,01\rangle - b\,|\,00\rangle - b\,|\,-21\rangle)_{\mathrm{p}2})/\sqrt{2}\end{aligned} \tag{16}$$

   When $S_{\mathrm{B}i}$'s measurement result is $|+\rangle$, it can be seen that the entangled state of $A_{\mathrm{p}i}$ and $B_{\mathrm{p}i}$ is $(a\,|\,20\rangle + a\,|\,01\rangle + b\,|\,00\rangle + b\,|\,-21\rangle)_{p2}$, then Alice measures $A_{\mathrm{p}i}$, causing $B_{\mathrm{p}i}$ collapses into the state of $S_{\mathrm{B}i}$, the final general state after collapse is

$$|2'\rangle_{\mathrm{p}}(a\,|\,0\rangle + b\,|\,1\rangle)_2/2 + |\text{-}2'\rangle_{\mathrm{p}}(a\,|\,0\rangle - b\,|\,1\rangle)_2/2 + |0\rangle_{\mathrm{p}}(a\,|\,1\rangle + b\,|\,0\rangle)_2/\sqrt{2} \tag{17}$$

   When $S_{\mathrm{B}i}$'s measurement result is $|-\rangle$, it can be seen that the entangled state of $A_{\mathrm{p}i}$ and $B_{\mathrm{p}i}$ is $(a\,|\,20\rangle + a\,|\,01\rangle - b\,|\,00\rangle - b\,|\,-21\rangle)_{\mathrm{p}2}$, then Alice measures $A_{\mathrm{p}i}$, causing $B_{\mathrm{p}i}$ collapses into the state of $S_{\mathrm{B}i}$, the final general state after collapse is

$$|2'\rangle_{\mathrm{p}}(a\,|\,0\rangle - b\,|\,1\rangle)_2/2 + |\text{-}2'\rangle_{\mathrm{p}}(a\,|\,0\rangle + b\,|\,1\rangle)_2/2 + |0\rangle_{\mathrm{p}}(a\,|\,1\rangle - b\,|\,0\rangle)_2/\sqrt{2} \tag{18}$$

   Based on $\lambda 1$, $\lambda 2$ and Table 1, Bob performs corresponding Pauli operations on Particle $B_{\mathrm{p}i}$, gets the transformed result $\alpha_i|0\rangle + \beta_i|1\rangle$.
   Another situation can be similarly verified: if Alice does Pauli operation $\sigma_x$ on $S_{\mathrm{B}i}$ and measures particle $S_{\mathrm{B}i}$, $A_{\mathrm{p}i}$ in order, the final general state after collapse is

$$|2'\rangle_p(a\,|\,1\rangle + b\,|\,0\rangle)_2/2 + |\text{-}2'\rangle_p(a\,|\,1\rangle - b\,|\,0\rangle)_2/2 + |0\rangle_p(a\,|\,0\rangle + b\,|\,1\rangle)_2/\sqrt{2} \tag{19}$$

or

$$|2'\rangle_p(a\,|\,1\rangle - b\,|\,0\rangle)_2/2 + |\text{-}2'\rangle_p(a\,|\,1\rangle + b\,|\,0\rangle)_2/2 + |0\rangle_p(a\,|\,0\rangle - b\,|\,1\rangle)_2/\sqrt{2} \tag{20}$$

   Charlie performs corresponding Pauli operations on Particle $B_{\mathrm{p}i}$, gets the transformed result $\alpha_i|1\rangle + \beta_i|0\rangle$.

4. Similar to the steps of the teleportation of Alice with Charlie, Alice can teleport the states of $M_{\mathrm{C}}$ to Bob. Denoting this time's basis $X$ and basis $Q$'s measurement results as $\gamma 1$ and $\gamma 2$ respectively, the states of $C_{\mathrm{p}}$ in Bob's hands convert to the states of $M_{\mathrm{C}}$ according to $\gamma 1$ and $\gamma 2$ announced by Alice.

### 3.5 Secret information recovery phase

1. Bob and Charlie collaborate. The two show the initial states of the single particles prepared in the particle preparation phase, select the corresponding basis to measure each particle, and Alice was reversely authenticated by the measurement results according to **Table 2**.

**Table 2.** The correspondence between the initial state of single photons and the particles encoded by secret information

| Measurement Base | *Z* | *Z* | *X* | *X* |
|---|---|---|---|---|
| $S_B/S_C$ | $\|0\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| $M_B/M_C$ | $\|0\rangle, \|1\rangle$ | $\|0\rangle, \|1\rangle$ | $\|+\rangle, \|-\rangle$ | $\|+\rangle, \|-\rangle$ |

   If the error rate is lower than the pre-agreed threshold, Alice is considered legal and can start rebuilding the secret. Otherwise, Alice is considered illegal.
2. Record the measurement result of $M_B(M_C)$ as $R_B(R_C)$, combined with the particles $S_B$ and $S_C$ which Bob and Charlie prepared in the particle preparation phase, Bob and Charlie can get the same Alice's Pauli operation sequence. Bob and Charlie map Pauli operations to *t*-bit secrets: $I \leftrightarrow 0$, $\sigma_x \leftrightarrow 1$, Alice's secret reconstruction is complete.

## 4. Security analysis

### 4.1 Discussion on dishonest participant Bob*

Assuming that the dishonest participant Bob* attempts to take intercept-resend attack or entanglement attack to obtain information carried by Charlie's particles.

- Intercept–resend attack by Bob*

For the intercept-resend attack, suppose Bob* intercepts the particles *S*c' that Charlie sent to Alice and resends the same particles to Alice. Bob* attempts to determine the particle states of *S*c, so that when the states of *C*p in Bob*'s hands convert to the states of $M_C$, he could recover the secret alone.

First, it is impossible for Bob* to obtain authentication key information about Charlie, so he could not restore *S*c' to *S*c without the authentication key $h_{Charlie}(S_{ID\text{-}Charlie})$ and he could not bypass the authentication.

Second, Bob* was unable to get the entire particle states of the *S*c' either, since the state of each particle in sequence *S*c' is randomly at one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Suppose the probability of Bob* correctly measuring the state of each particle is 50%, the probability $P_B$ of correctly measuring the entire particle states of *S*c' can be quantitatively assessed according to statistics.

$$P_B = \binom{N}{k}\left(\frac{1}{2}\right)^k\left(\frac{1}{2}\right)^{N-k} \tag{21}$$

where *k* represents the total number of particle states correctly measured. *N* represents the length of the *S*c'. The probability $P_B$ satisfies the binomial distribution and the binomial coefficient.

$$\binom{N}{k} = \frac{N!}{k!(N-k)!} \tag{22}$$

$P_B$ in dependence on $k$ for the respective $N$ = 256, $N$ = 512 and $N$ = 1024 in **Fig. 3** shows that there exists a maximal value of $P_B$ for different $N$, and it diminishes with the increase of $N$. Therefore, Bob* was unable to get the entire particle states of the $Sc$' and combines the initial particle states of $Sc$ presented by Charlie in the secret recovery phase to infer the authentication key $h_{\text{Charlie}}(S_{\text{ID-Charlie}})$.

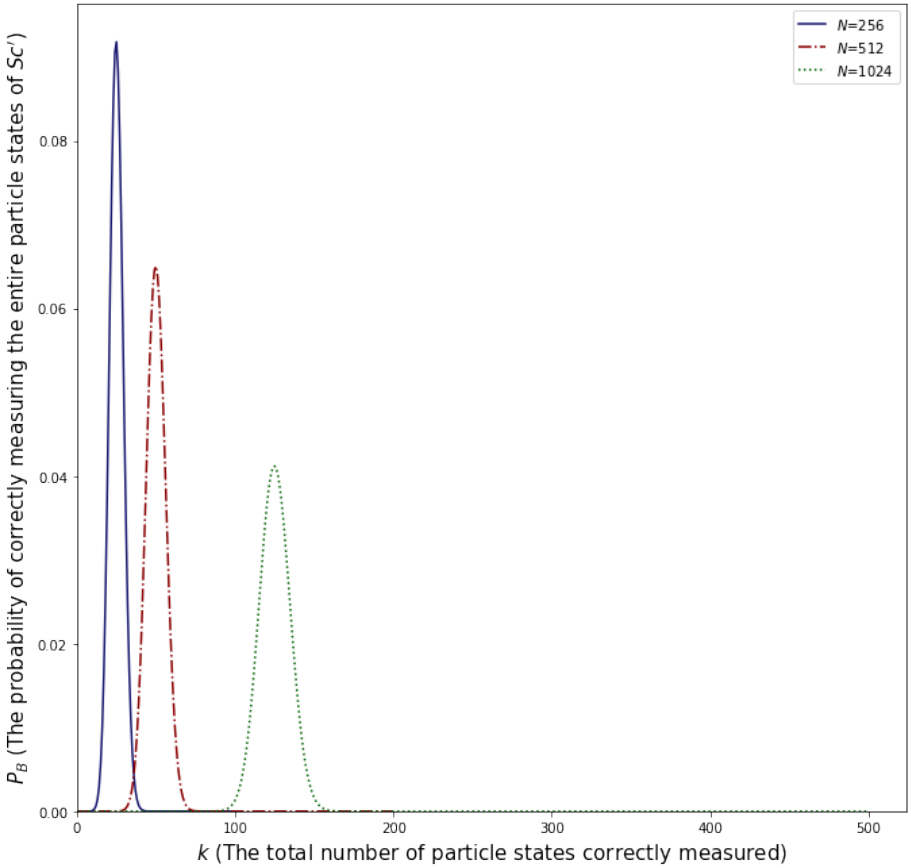


**Fig. 1.** The relationship of $k$ (the total number of particle states correctly measured) and $P_B$ (the probability of Bob* correctly measuring the entire particle states of $S_c$') when $N$=256, 512 and 1024

- Entanglement attack by Bob*

For the entanglement attack, suppose Bob* intercepts the particles $Sc$' that Charlie sent to Alice during transmission and uses unitary operation $E$ to entangle the new particles $e$ with $Sc$' to form a bigger Hilbert space, where $Sc_i$'=$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

$$E \otimes |0e\rangle = a|0e_{00}\rangle + b|1e_{01}\rangle \tag{23}$$

$$E \otimes |1e\rangle = b'|0e_{10}\rangle + a'|1e_{11}\rangle \tag{24}$$

$$\begin{aligned} E\otimes|+e\rangle &= \frac{1}{\sqrt{2}}(a|0e_{00}\rangle + b|1e_{01}\rangle + b'|0e_{10}\rangle + a'|1e_{11}\rangle) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + b'|e_{10}\rangle + a'|e_{11}\rangle) \\ &\quad + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + b'|e_{10}\rangle - a'|e_{11}\rangle)] \end{aligned} \tag{25}$$

$$\begin{aligned} E\otimes|-e\rangle &= \frac{1}{\sqrt{2}}(a|0e_{00}\rangle + b|1e_{01}\rangle - b'|0e_{10}\rangle - a'|1e_{11}\rangle) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle - b'|e_{10}\rangle - a'|e_{11}\rangle) \\ &\quad + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - b'|e_{10}\rangle + a'|e_{11}\rangle)] \end{aligned} \tag{26}$$

The unitary operation matrix $E$ is expressed as

$$E=\begin{pmatrix} a & b' \\ b & a' \end{pmatrix} \tag{27}$$

where $e_{i,j}$ decided by operator $E$ satisfy the normalization condition

$$\sum_{i,j\in\{0,1\}} \langle e_{ij}|e_{ij}\rangle = 1 \tag{28}$$

Since $EE^*=1$, $a$, $b$, $a'$, $b'$ satisfy the following relationship

$$|a|^2 + |b|^2 = 1,\ |a'|^2 + |b'|^2 = 1,\ ab^* = (a')^* b' \tag{29}$$

We can get the result

$$|a|^2 = |a'|^2,\ |b|^2 = |b'|^2 \tag{30}$$

If particle $e$ is in an entangled state, Bob$^*$'s entanglement attack will inevitably introduce an error rate $P_{error}$

$$P_{error} = |b|^2 = 1-|a|^2 = |b'|^2 = 1-|a'|^2 \tag{31}$$

If Bob$^*$ tries to achieve the eavesdropping without being detected, the transmitted qubits and Bob$^*$'s auxiliary particles are in a tensor-product state. However, in direct state there is no correlation between the auxiliary particle $e$ and the whole system, Bob$^*$ could not get any useful information, thus proving that the entanglement attack is futile.

Therefore, it is concluded that the dishonest participant Bob$^*$ can not get any valid information by intercept-resend attack or entanglement attack without introducing errors.

### 4.2 Discussion on eavesdropper Eve

Suppose the eavesdropper Eve wants to acquire the Bob and Charlie's authentication key by intercept-resend attack or entanglement attack and bypassing eavesdropping detection. Before, we have analyzed that the internal dishonest participant Bob$^*$ can not get any valid information by intercept-resend attack or entanglement attack to get the authentication key $h_{\text{Charlie}}(S_{\text{ID-Charlie}})$.

Obviously, Bob* has a greater attack advantage than the external eavesdropper Eve, but Bob*'s two attacks are futile. It can be considered that Eve's intercept-resend attack or entanglement attack to $S_B$'/$S_C$' is also futile. So, we only discuss Eve's intercept-retransmit attack and entanglement attack on particles $B_p/C_p$.

- Intercept-resend attack by Eve

Suppose Eve intercepts the particles $B_p$, which is entangled with particles $A_p$ and $M_B$ in quantum walk system, and gets Alice's measurement results $\lambda 1$, $\lambda 2$ to recover the target states. Since he knows nothing about the states of particle $S_B$, it is unable for him to obtain correct measurement results and resend correct particles to Charlie, he will bring the error rate of 50% for each particle in step1 of the secret information recovery phase.

The detected probability $P_D$ can be quantitatively assessed according to statistics.

$$P_D = 1 - \left( \frac{t!}{k!(t-k)!} \right) \left( \frac{1}{2} \right)^k \left( \frac{1}{2} \right)^{t-k} \tag{32}$$

where $k$ represents the total number of correct measurement results, $t$ represents the length of the $B_p$.

$P_D$ in dependence on $k$ for the respective $t$ = 256, $t$ = 512 and $t$ = 1024 in **Fig. 4** shows that there exists a minimum value of $P_E$ for different $N$, and it increases as $N$ increases.

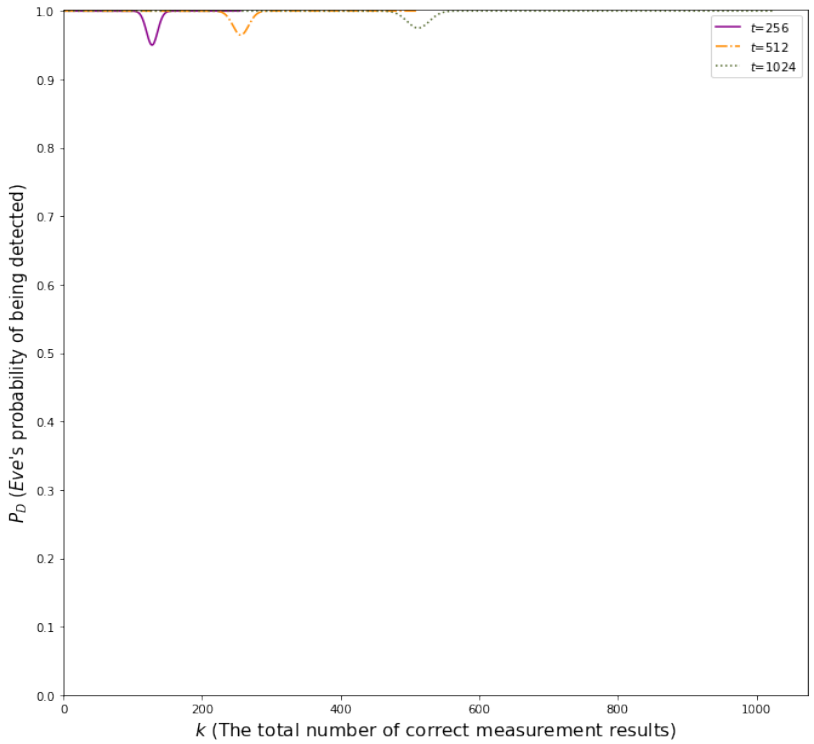


**Fig. 2.** The relationship of $k$ (The total number of correct measurement results) and $P_D$ (Eve's probability of being detected) when N=256, 512 and 1024

- Entanglement attack by Eve

For the entanglement attack, suppose Eve uses unitary operation $E$ to entangle the new particles $e$ with paticle $B_p$ in $|\Phi\rangle^{(2)}$, the unitary operation matrix $E$ and the $e_{i,j}$ decided by operator $E$ are conform to Formula(23-30), and we will not repeat them here.

where $|\Phi\rangle^{(2)} = (\alpha|200\rangle + \alpha|001\rangle + \beta|010\rangle + \beta|-211\rangle)_{p12}$.

The state of the composite system becomes

$$\begin{aligned}|\Phi\rangle_{Eve} &= \alpha|20\rangle_{p1}(a|0e_{00}\rangle + b|1e_{01}\rangle)_{2E} + \alpha|00\rangle_{p1}(b'|0e_{10}\rangle + a'|1e_{11}\rangle)_{2E} \\ &+ \beta|01\rangle_{p1}(a|0e_{00}\rangle + b|1e_{01}\rangle)_{2E} + \beta|-21\rangle_{p1}(b'|0e_{10}\rangle + a'|1e_{11}\rangle)_{2E} \\ &= \alpha|0\rangle_1[(a|20e_{00}\rangle + b|21e_{01}\rangle)_{p2E} + (b'|00e_{10}\rangle + a'|01e_{11}\rangle)_{p2E}] \\ &+ \beta|1\rangle_1[(a|00e_{00}\rangle + b|01e_{01}\rangle)_{p2E} + (b'|-20e_{10}\rangle + a'|-21e_{11}\rangle)_{p2E}]\end{aligned} \tag{33}$$

When Alice measures particle $S_B$, the composite state of particles $A_p$, $B_p$, $e$ converts to $(a|20e_{00}\rangle + b|21e_{01}\rangle)_{p2E} + (b'|00e_{10}\rangle + a'|01e_{11}\rangle)_{p2E}$ if the measurement result is $|0\rangle_1$, and converts to $(a|00e_{00}\rangle + b|01e_{01}\rangle)_{p2E} + (b'|-20e_{10}\rangle + a'|-21e_{11}\rangle)_{p2E}$ if the result is $|1\rangle_1$. We continue the analysis with the measurement result of $|0\rangle_1$, Alice measures particle $A_p$ based on this, the state of the composite particles becomes

$$\begin{aligned}&(a|20e_{00}\rangle + b|21e_{01}\rangle)_{p2E} + (b'|00e_{10}\rangle + a'|01e_{11}\rangle)_{p2E} \\ &= |2\rangle_p(a|0e_{00}\rangle + b|1e_{01}\rangle)_{2E} + |0\rangle_p(b'|0e_{10}\rangle + a'|1e_{11}\rangle)_{2E} \\ &= \tfrac{1}{\sqrt{2}}[|2'\rangle_p(a|0e_{00}\rangle + b|1e_{01}\rangle)_{2E} + |-2'\rangle_p(a|0e_{00}\rangle + b|1e_{01}\rangle)_{2E}] \\ &\quad + |0\rangle_p(b'|0e_{10}\rangle + a'|1e_{11}\rangle)_{2E}\end{aligned} \tag{34}$$

It can be indicated that if particle $e$ is in an entangled state, Eve's will introduce an error rate $P_{error}$

$$P_{error} = |b|^2 = 1 - |a|^2 = |b'|^2 = 1 - |a'|^2 \tag{35}$$

If Eve doesn't want to introduce an error rate, the qubits in quantum walk system and the qubits $e$ must be in a tensor-product state. However, in direct state there is no correlation between them, Eve could not get any useful information, thus the entanglement attack is futile.

Therefore, the eavesdropper Eve can not get any valid information by intercept-retransmit attack and entanglement attack on particles $B_p/C_p$ without introducing errors.

### 4.3 Discussion on the security of Alice certification

Suppose an illegal imposter tries to impersonate Alice.

The scheme firstly lets Bob and Charlie prepare random photons, perform Pauli operations on photons according to their authentication key, then send to Alice. Alice authenticates the received particles and builds quantum walk circuits. Previously, we have analyzed that any third party cannot obtain the authentication keys through intercept-resend attack or entanglement attack. Therefore, the imposter cannot obtain Bob and Charlie's legal authentication keys.

In addition, when Bob and Charlie collaborate to authenticate Alice, because each single photon of $M_B/M_C$ is randomly in the one of $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, Bob and Charlie select the measurement basis according to the initial particle state their prepared to measure $M_{Bi}/M_{Ci}$, the measurement results has two possibilities: the measurement result is the same as the initial particle state, if Alice performs an $I$ operation on $S_{Bi}/ S_{Ci}$, and be opposite if Alice performs a $\sigma_x$ operation on $S_{Bi}/ S_{Ci}$. Therefore, based on the known information and in comparison with Table 2, it can be found whether Alice actually owns the authentication keys of Bob and Charlie, and can determine whether Alice is legal.

## 5. Efficiency analysis and comparisons

According to Cabello[32], information-theoretical efficiency can be defined as $\eta=q_e/(q_t+b_t)$, where $q_u$ is the final effective number of qubits, $q_t$ represents the total number of qubits transmitted through the quantum channel, and $b_t$ is the classical bits for decoding of the qubits. (The quantum resources and the classical resources which are used for identity authentication and security checks are not counted.) The information-theoretical efficiency of the proposed protocol is $2n/(4t+2t)=33.33\%$ which is the same as the efficiency performance computed in most protocols like Ref[41, 42]. However, the proposed protocol is more secure with respect to the feature of identity authentication.

Evaluate the protocol from the quantum resources used, whether it has identity authentication and whether it can against participant attack, the comparison results of between the proposed protocol and some other QSS protocols are listed in **Table 3**.

**Table 3.** Comparisons between the proposed QSS protocol and previous QSS protocols

| | **Preparation of initial photons** | **Photon preparation difficulty** | **Identity authentication** | **Secure against participant attack** |
|---|---|---|---|---|
| Refs. 33, 34 and 35 | Bell state | Hard | No | No |
| Ref. 36 | Six-qubit entangled state | Hard | No | Yes |
| Ref. 37 | Bell state | Hard | No | Yes |
| Ref. 16 | Single photon | Easy | Yes | No |
| Ref. 38 | GHZ state | Hard | No | No |
| Ref. 39 | Single photon and Bell state | Hard | No | No |
| Ref. 40 | GHZ state | Hard | Yes | Yes |
| Ref. 18 | Bell state | Hard | Yes | Yes |
| The proposed scheme | Single photon | Easy | Yes | Yes |

The comparison results shows this scheme is distinguished with the function of identity authentication and secure against participant attack. In addition, the initial phase of the particle preparation only requires single photons, the necessary entangled states do not need to be prepared in advance, they can be spontaneously entangled after the first step of quantum walk. (Comparing with difficult entangled state preparation, this is a big improvement.)

## 6. Conclusion

This paper proposes a quantum secret sharing scheme with credible authentication based on quantum walk. Different from the existing QSS protocols, the proposed scheme is to prepare single photons by Bob and Charlie respectively, and then send it to Alice. Alice authenticates Bob and Charlie, and then encodes the secret onto the quantum states by constructing a quantum walk circuit and performing Pauli operation. Secrets are distributed to Bob and Charlie through quantum teleportation. Eventually, they complete identity authentication for Alice, and collaborate to measure and recover the secret. The scheme realizes the authentication of both parties in the process of secret sharing, and it can effectively prevent an attacker from impersonating Alice to issue fake commands.

In addition, the protocol transmits information securely through quantum teleportation, but does not need to prepare entangled states in initial, it spontaneously generates entangled states between Alice and Bob in the circuit of one-dimensional two-step quantum walks on the line. This quantum circuit causes Alice to collapse the transmission information in the quantum state of Bob(Charlie) after measuring her own quantum state, then Bob(Charlie) performs the corresponding Pauli operation to recover the information, thereby completing the teleportation. Due to the function of identity authentication and the use of quantum walk, the protocol greatly enhances the security of the QSS protocol. At present, Xue et al[43] have successfully confirmed that quantum walk can be applied to quantum communication and can perform quantum walks of more than 20 steps in a one-dimensional space. Due to the limitation of equipment, this paper cannot provide such physical verification for the time being, but the quantum resources that the protocol relies on are satisfyable under the current technology, so it is feasible to implement the QSS protocol proposed in this paper based on the current technology.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (No.61572086, No.61402058), the Key Research and Development Project of Sichuan Province (No. 20ZDYF2324, No. 2019ZYD027, No. 2018TJPT0012), the Innovation Team of Quantum Security Communication of Sichuan Province (No.17TD0009), the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province (No. 2016120080102643), the Application Foundation Project of Sichuan Province(No.2017JY0168), the Science and Technology Support Project of Sichuan Province (No.2018GZ0204, No.2016FZ0112).

## References

[1] M. Hillery, V. Buzek, A. Berthiaume, “Quantum secret sharing,” *Physical Review A*, vol. 59, no. 3, pp. 1829-1834, March 1999. Article (CrossRef Link).

[2] W. Liu, P. Gao, W. Yu, et al, “Quantum Relief algorithm,” *Quantum Information Processing*, vol. 17, no. 10, pp. 280, October, 2018. Article (CrossRef Link).

[3] Y. Chang, S. Zhang, L. Yan, et al, “A Quantum Authorization Management Protocol Based on EPR-Pairs,” *Computers, Materials & Continua*, vol. 59, no. 3, pp. 1005-1014, 2019. Article (CrossRef Link).

[4] W. Liu, P. Gao, Z. Liu, et al, “A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment,” *Security and Communication Networks*, vol. 2019, pp.1-14, 2019. Article (CrossRef Link).

[5] Z. Qu, S. Wu, M. Wang, et al, "Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels," *Quantum Information Processing*, vol. 16, no.12, pp. 306, December, 2017. Article (CrossRef Link).
[6] Z. Qu, Z. Li, G. Xu, et al, "Quantum Image Steganography Protocol Based on Quantum Image Expansion and Grover Search Algorithm," *IEEE Access*, vol. 7, pp. 50849-50857, January, 2019. Article (CrossRef Link).
[7] Z. Qu, Z. Wen, X. Wang, "Matrix Coding-Based Quantum Image Steganography Algorithm", *IEEE Access*, vol. 7, pp. 35684-35698, January, 2019. Article (CrossRef Link).
[8] L. Yan, Y. Chang, S. Zhang, et al, "Measure-Resend Semi-Quantum Private Compari-son Scheme Using GHZ Class States," *Computers, Materials & Continua*, vol. 61, no. 2, pp. 877-887, 2019. Article (CrossRef Link).
[9] S. Zhang, Y. Chang, L. Yan, et al, "Quantum Communication Networks and Trust Management: A Survey," *Computers, Materials & Continua*, vol. 61, no.3, pp.1145-1174, January, 2019. Article (CrossRef Link).
[10] W. Liu, Y. Xu, M. Zhang, et al, "A Novel Quantum Visual Secret Sharing Scheme," *IEEE Access*, vol. 7, pp. 114374-114384, 2019. Article (CrossRef Link).
[11] X. Chen, X. Niu, X. Zhou, et al, "Multi-party quantum secret sharing with the single-particle quantum state to encode the information," *Quantum Information Processing*, vol. 12, no. 1, pp. 365-380, March, 2013. Article (CrossRef Link).
[12] H. Wang, Y. Huang, X. Fang, et al, "High-Capacity Three-Party Quantum Secret Sharing with Single Photons in Both the Polarization and the Spatial-Mode Degrees of Freedom," *International Journal of Theoretical Physics*, vol. 52, no. 4, pp.1043–1051, April, 2013. Article (CrossRef Link).
[13] S. Hao, B. Yu, "Multiparty Quantum Secret Information Sharing in Enterprise Management Based on Single Qubit with Random Rotation Angle," *International Journal of Theoretical Physics*, vol. 51, no. 6, pp. 1674–1679, June, 2012. Article (CrossRef Link).
[14] H. Qin, X. Zhu, Y. Dai, "(t, n) Threshold quantum secret sharing using the phase shift operation," *Quantum Information Processing*, vol. 14, no. 8, pp. 2997–3004, August, 2015. Article (CrossRef Link).
[15] Y. Yang, Q. Wen, X. Zhang, "Multiparty simultaneous quantum identity authentication with secret sharing," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 51, no. 3, pp. 321-327, January, 2008. Article (CrossRef Link).
[16] X. Zhang, D. Ji, "Analysis of a kind of quantum cryptographic schemes based on secret sharing," *Science in China Series G: Physics, Mechanics and Astronomy*, vol. 52, no. 9, pp. 1313–1316, September, 2009. Article (CrossRef Link).
[17] Y. Yang, H. Wang, X. Jia, H. Zhang, "A Quantum Protocol for (t,n)-Threshold Identity Authentication Based on Greenberger-Horne-Zeilinger States," *International Journal of Theoretical Physics*, vol. 52, no. 2, pp. 524–530, 2013. Article (CrossRef Link).
[18] H. Abulkasim, S. Hamad, K. Bahnasy, et al, "Authenticated quantum secret sharing with quantum dialogue based on Bell states," *Physica Scripta*, vol. 91, no. 8, pp. 085101, July, 2016. Article (CrossRef Link).
[19] Y. Aharonov, L. Davidovich, N. Zagury, "Quantum random walks," *Physical Review A*, vol. 48, no. 2, pp. 1687-1690, 1993. Article (CrossRef Link).
[20] J. Kempe, "Quantum random walks - an introductory overview," *Contemporary Physics*, vol. 44, no. 4, pp. 307-327, January, 2003. Article (CrossRef Link).
[21] S.E. Venegas-Andraca, "Quantum walks: a comprehensive review," *Quantum Information Processing*, vol. 11, no. 5, pp. 1015-1106, January, 2012. Article (CrossRef Link).
[22] Y. Wang, Y. Shang, P. Xue, "Generalized teleportation by quantum walks," *Quantum Information Processing*, vol. 16, no. 221, September, 2017. Article (CrossRef Link).
[23] Y. Shang, Y. Wang, M. Li, et al, "Quantum communication protocols by quantum walks with two coins," *Europhysics Letters*, vol. 124, no. 6, pp. 60009, February, 2019. Article (CrossRef Link).
[24] X. Chen, Y. Wang, G. Xu, et al, "Quantum Network Communication With a Novel Discrete-Time Quantum Walk," *IEEE Access*, vol. 7, pp. 13634-13642, January, 2019. Article (CrossRef Link).

[25] X. Zou, Y. Dong, G. Guo, "Optical implementation of one-dimensional quantum random walks using orbital angular momentum of a single photon," *New Journal of Physics*, vol. 8, no. 81, May, 2006. Article (CrossRef Link).
[26] Z. Bian, J. Li, X. Zhan, et al, "Experimental implementation of a quantum walk on a circle with single photons," *Physical Review A*, vol. 95, no. 5, pp. 052338, May, 2017. Article (CrossRef Link).
[27] H. Tang, X. Lin, Z. Feng, et al, "Experimental two-dimensional quantum walk on a photonic chip," *Science Advances*, vol. 4, no. 5, pp.3174, December, 2018. Article (CrossRef Link).
[28] Y. Feng, R. Shi, J. Shi, et al, "Arbitrated quantum signature scheme with quantum walk-based teleportation," *Quantum Information Processing*, vol. 18, no. 5, pp. 15, April, 2019. Article (CrossRef Link).
[29] J. Shi, H. Chen, F. Zhou, et al, "Quantum Blind Signature Scheme with Cluster States Based on Quantum Walk Cryptosystem," *International Journal of Theoretical Physics*, vol. 58, no. 4, pp. 1337-1349, February, 2019. Article (CrossRef Link).
[30] H. Lee, H. Yang, J. Lim, "Quantum Direct Communication with Authentication," *Physical Review A*, vol. 73, no. 4, pp. 543-543, April 2006. Article (CrossRef Link).
[31] A. Ambainis, E. Bachy, A. Nayakz, et al, "One-dimensional quantum walks," in *Proc. of the thirty-third annual ACM symposium on Theory of computing STOC01*, pp. 37-49, 2001. Article (CrossRef Link).
[32] A. Cabello, "Quantum Key Distribution in the Holevo Limit," *Physical Review Letters*, vol. 85, pp. 5635, January, 2000. Article (CrossRef Link).
[33] Y. Du, W. Bao, "Multiparty quantum secret sharing scheme based on the phase shift operations," *Optics Communications*, vol. 308, no. 1, pp. 159-163, November, 2013. Article (CrossRef Link).
[34] Z. Zhu, A. Hu, A. Fu, "Cryptanalysis of a new circular quantum secret sharing protocol for remote agents," *Quantum Information Processing*, vol. 12, no. 2, pp. 1173–1183, February, 2013. Article (CrossRef Link).
[35] R. Shi, L. Huang, W. Yang, et al, "Multiparty quantum secret sharing with Bell states and Bell measurements," *Optics Communications*, vol. 283, no. 11, pp. 2476-2480, June, 2010. Article (CrossRef Link).
[36] G. Gan, "Multiparty Quantum Secret Sharing Using Two-Photon Three-Dimensional Bell States," *Communications in Theoretical Physics*, vol. 52, no. 3, pp. 421-424, September, 2009. Article (CrossRef Link).
[37] M. Dusek, O. Haderka, M. Hendrych, et al, "Quantum identification system," *Physical Review A*, vol. 60, pp. 149, January, 1999. Article (CrossRef Link).
[38] Q. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A*, vol. 351, no. 1-2, pp. 23-25, February, 2006. Article (CrossRef Link).
[39] J. Lin, T. Hwang, "New circular quantum secret sharing for remote agents," *Quantum Information Processing*, vol. 12, no. 1, pp. 685–697, April, 2013. Article (CrossRef Link).
[40] F. Liu, Q. Su, Q. Wen, "Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations," *International Journal of Theoretical Physics*, vol. 53, no. 5, pp. 1730-1737, April, 2014. Article (CrossRef Link).
[41] T. Hwang, C. Hwang, C. Li, "Multiparty quantum secret sharing based on GHZ states," *Physica Scripta*, vol. 83, no. 4, pp. 045004, March, 2011. Article (CrossRef Link).
[42] X. Liu, R. Pan, "Cryptanalysis of quantum secret sharing based on GHZ states," *Physica Scripta*, vol. 84, no. 4, pp. 045015, September, 2011. Article (CrossRef Link).
[43] P. Xue, R. Zhang, H. Qin, et al, "Experimental quantum-walk revival with a time-dependent coin," *Physical Review Letters*, vol. 114, no. 14, pp. 140502, April, 2015. Article (CrossRef Link).

**Xueyang Li** has received his B.S. degree in Electronic Information Engineering from Chengdu University of InformationTechnology in 2013. He is a postgraduate in the School of Cyberspace Security, Chengdu University of InformationTechnology, mainly studying quantum information and information security.

**Yan Chang** received her Ph.D. degree in information security from University of Electronic Science and Technology of China in 2016. She is currently a professor in the Department of Information Security, Chengdu University of Information Technology. Her research interests are quantum information, information security.

**Shibin Zhang** received his Ph.D. degree in information security from Southwest Jiao Tong University of China in 2006. He is currently a professor in Chengdu University of Information Technology. His research interests include applied computer science and technology, quantum information, information security and cryptography.