entropy

MDPI

Article

A Kind of (t, n) Threshold Quantum Secret Sharing with Identity Authentication

Depeng Meng, Zhihui Li *, Shuangshuang Luo and Zhaowei Han

School of Mathematics and Statistics, Shaanxi Normal University, Xi'an 710119, China; mdp@snnu.edu.cn (D.M.)
* Correspondence: lizhihui@snnu.edu.cn; Tel.: +86-13-03-298-9886

Abstract: Quantum secret sharing (QSS) is an important branch of quantum cryptography. Identity authentication is a significant means to achieve information protection, which can effectively confirm the identity information of both communication parties. Due to the importance of information security, more and more communications require identity authentication. We propose a d-level (t, n) threshold QSS scheme in which both sides of the communication use mutually unbiased bases for mutual identity authentication. In the secret recovery phase, the sharing of secrets that only the participant holds will not be disclosed or transmitted. Therefore, external eavesdroppers will not get any information about secrets at this phase. This protocol is more secure, effective, and practical. Security analysis shows that this scheme can effectively resist intercept–resend attacks, entangle–measure attacks, collusion attacks, and forgery attacks.

Keywords: quantum secret sharing; identity authentication; mutually unbiased bases; (t, n) threshold scheme

check for updates

Citation: Meng, D.; Li, Z.; Luo, S.; Han, Z. A Kind of (t, n) Threshold Quantum Secret Sharing with Identity Authentication. *Entropy* **2023**, *25*, 827. https://doi.org/10.3390/e25050827

Academic Editors: Hong-Wei Li, Jin Dong Wang, Qin Wang and Xing-Yu Zhou

Received: 29 March 2023
Revised: 16 May 2023
Accepted: 17 May 2023
Published: 22 May 2023

1. Introduction

Secret sharing is an important research field in cryptography. It has important applications in many aspects, such as network communication, signature checking, and identity verification. In 1979, Shamir [1] proposed the first secret-sharing protocol based on Lagrange interpolation formula. With the rapid development of quantum technology, quantum secret sharing (QSS) has also made great progress. In 1999, Hillery et al. [2] proposed the first QSS protocol using the Greenberger–Horne–Zeilinger (GHZ) state. Since then, more and more relatively complete QSS protocols [3–17] have been proposed by scholars. Like the (n, n) threshold QSS protocol [3–5], the secret is divided into n parts. Only n participants can cooperate to recover the secret. However, due to practical needs and consideration of flexibility, some (t, n) threshold QSS protocols [6–17] have received great attention. The secret is also divided into n parts, but t participants can recover the secret and fewer than t participants cannot recover the secret. In addition, to detect the existence of external attackers and check the integrity of internal participants, some verifiable QSS protocols [11–17] have been proposed. They mainly include message authentication (verify the correctness of the message) and identity authentication (verify the correctness of identity). Identity authentication is a systematic process to verify the identity of legitimate users, components and devices. Therefore, it is the security guarantee of various encryption tasks. In the identity authentication scheme, the sender registers the secret information as his identity information in the receiver's database before communication. Afterwards, the sender proves the secret identification information to the receiver, that is, his identity information. The receiver can prove that the sender is a legitimate user before establishing the communication channel by using an authentication scheme, so he avoids the occurrence of an illegal sender. In quantum cryptography, quantum secret sharing [15–17], quantum key distribution [18–21], quantum secure direct communication [22,23], etc., all require identity authentication. In real life, the importance of identity authentication is also reflected everywhere.

In 2013, Yang et al. [3] constructed an QSS using entangled state and quantum Fourier transform (QFT). In 2015, Tavakoli [4] proposed a d-level QSS based on GHZ state and mutually unbiased bases. The above two schemes are (n, n) threshold. In 2017, Song et al. [7] proposed a d-level (t, n) threshold QSS based on Shamir's secret-sharing scheme and the Lagrange interpolation formula. However, restricted by private secret shares, the scheme is infeasible. In 2020, Sutradhar et al. [8] proposed an QSS without credible participants. Nevertheless, in the actual process, the reconstructor needs to compare secrets and the hash value of secrets, so the reconstructor must be trustworthy. In 2020, Mashhadi [9] pointed out the problems in the protocol of Song et al. [7] and gave an improvement scheme. In this improved protocol, each participant applies the inverse quantum Fourier transform (IQFT) on its own particle. Then, each participant measures and publishes the measurement results. At this time, everyone can recover the original secret, but there is no identity authentication process in the transmission of quantum states, and we cannot guarantee that the corresponding operation is performed by the corresponding participant. In 2021, Hu et al. [17] proposed a dynamic QSS using GHZ state in a high-dimensional quantum system. In this protocol, each participant performs corresponding unitary operations according to its own measurement results.

In this paper, we overcome the above problems. The innovation of this article is to improve [8] by combining relevant knowledge. We mainly add identity authentication content to make the protocol more secure and complete. Our protocol is a d-level (t, n) threshold scheme that both parties can be mutually verified. Each participant can act as a reconstructor to recover the secret. When a participant wants to recover the secret, he can cooperate with participants in an authorized subset to obtain the secret. The direct communication parties will conduct mutual identity authentication through mutually unbiased bases. After passing the authentication, other participants use direct product operation on their own particles and auxiliary particle passed by the reconstructor. Then, the reconstructor measures the final secret after performing the IQFT. Finally, he verifies whether the correct secret is obtained by comparing the secret and the hash value of the secret published by the dealer.

The rest of the article is organized as follows. In Section 2, we give the preliminary knowledge needed for this article. In Section 3, we propose a (t, n) threshold quantum secret sharing scheme with identity authentication. In Section 4, we give the correctness proof of the agreement. In Section 5, we analyze the security of the protocol. In Section 6, we compare and analyze this protocol with some previous protocols. In Section 7, we give a specific example to better understand the protocol. In Section 8, we summarize the full text and draw conclusions.

2. Preliminaries

In this section, we introduce some basic knowledge needed in this article, including quantum measurement, mutually unbiased bases, QFT, IQFT, and $CNOT$ operation.

2.1. Quantum Measurement

Quantum measurement can be described based on a set of measurement operators $\{M_i\}$. These measurement operators satisfy the completeness equation:

$$\sum_i M_i^\dagger M_i = 1. \tag{1}$$

When the quantum state $|\varphi\rangle$ is measured, the probability that the result is i is:

$$p(m) = \langle\varphi|M_i^\dagger M_i|\varphi\rangle. \tag{2}$$

After measurement, the quantum state collapses as follows:

$$|\varphi\rangle' = \frac{M_i|\varphi\rangle}{\sqrt{\langle\varphi|M_i^{\dagger}M_i|\varphi\rangle}}. \tag{3}$$

Therefore, quantum measurement will change the original state of the quantum state.

2.2. Mutually Unbiased Bases

Let d be an odd prime number and Z_d be a finite field. Suppose $V_1 = \{|u_i\rangle\}_{i=1}^{d}$, $V_2 = \{|v_j\rangle\}_{j=1}^{d}$ are two sets of standard orthogonal bases on d-dimensional Hilbert space. If they satisfy:

$$|\langle u_i|v_j\rangle| = \frac{1}{\sqrt{d}}. \tag{4}$$

Then these two groups of bases are called mutually unbiased bases. If any two sets of bases in $V = \{V_1, V_2, \cdots, V_m\}$ are mutually unbiased, V is called mutual unbiased bases set. Additionally, there are at most $d+1$ elements in set V. Specifically, the calculation base $\{|z\rangle\}$, $z \in Z_d$, is one of them. The remaining d groups can be expressed as:

$$|e_l^j\rangle = \frac{1}{\sqrt{d}}\sum_{z=0}^{d-1}\omega^{z(l+jz)}|z\rangle, \tag{5}$$

where $l, j \in \{0, 1, \cdots, d-1\}$, $\omega = e^{\frac{2\pi i}{d}}$, j represents the sequence of bases, and l represents vector sequence in a set of bases. They satisfy the following relation:

$$|\langle e_l^j|e_{l'}^{j'}\rangle| = \frac{1}{\sqrt{d}}, j \neq j'. \tag{6}$$

Additionally, among mutually unbiased bases, the following unitary operation makes them transform each other:

$$X_d = \sum_{u=0}^{d-1}\omega^u|u\rangle, Y_d = \sum_{u=0}^{d-1}\omega^{u^2}|u\rangle, \tag{7}$$

let

$$U_{x,y} = X_d^x Y_d^y. \tag{8}$$

We have

$$U_{x,y}|e_l^j\rangle = |e_{l+x}^{j+y}\rangle. \tag{9}$$

2.3. QFT, IQFT

The QFT in the d-dimensional system can be expressed as follows:

$$F|x\rangle = \frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}\omega^{x\cdot y}|y\rangle. \tag{10}$$

where $\omega = e^{\frac{2\pi i}{d}}$, $x, y \in Z_d$. Similarly, the IQFT can be expressed as:

$$F^{-1}|x\rangle = \frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}\omega^{-x\cdot y}|y\rangle. \tag{11}$$

It is easy to know that both discrete QFT and discrete IQFT are unitary transformations. In addition, by

$$\sum_{q=0}^{d-1} \omega^{sq} = \begin{cases} 0, & s \neq 0 \bmod d, \\ \\ d, & s = 0 \bmod d, \end{cases} \tag{12}$$

We can obtain

$$F^{-1}(F|x\rangle) = |x\rangle. \tag{13}$$

2.4. CNOT Operation

$CNOT$ is a two-qubit gate. In the d-dimensional system, it can be expressed as follows:

$$CNOT(|x_1\rangle, |x_2\rangle) = (|x_1\rangle, |x_1 \oplus x_2\rangle), \tag{14}$$

where $|x_1\rangle$ is control bit, $|x_2\rangle$ is the target bit, $x_1, x_2 \in Z_d$.

3. Proposed Protocol

In this section, we propose a quantum secret-sharing scheme with d-level and (t, n) threshold. Participants can verify each other mutually. Dealer Alice distributes secret shares among the set of participants B = {Bob$_1$,Bob$_2$,$\cdots$,Bob$_n$}. At least t participants can recover the secret. As the participants mutually verify, the protocol is more secure and practical. The entire scheme consists of three stages, namely the secret-sharing stage, identity authentication stage, and secret-recovery stage. The continuous identity authentication is included in the entire secret-recovery phase. Here, we use Figure 1 to briefly represent the entire process. The specific scheme of the protocol is shown below.

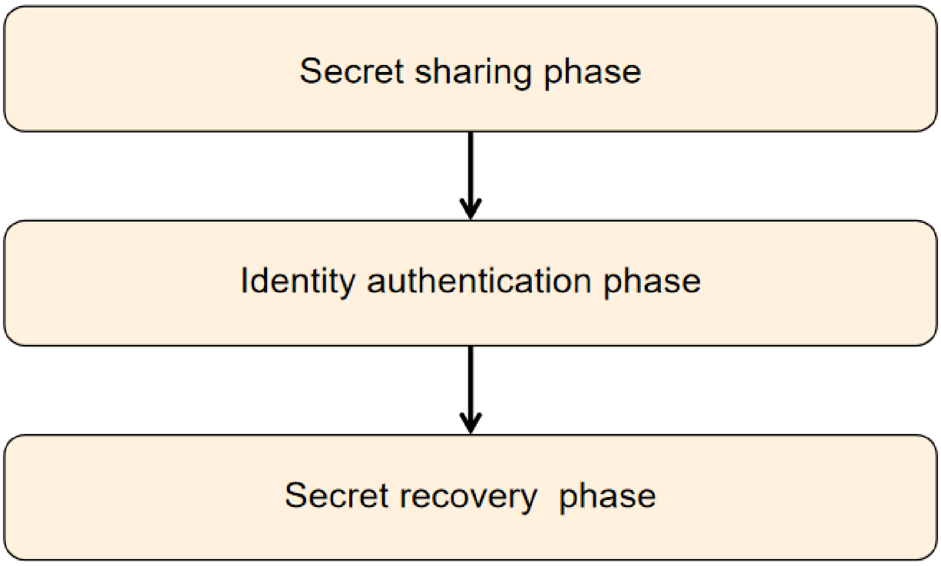

Figure 1. The process of this scheme.

3.1. Secret-Sharing Phase

In this phase, The dealer Alice performs the following operations:

(I) Alice selects a binary symmetric polynomial $F(x, y)$ of degree $(t-1)$ in the Z_d. The $(t-1)$ degree polynomial can be defined as:

$$F(x, y) = S + a_{10}x + a_{01}y + a_{20}x^2 + a_{02}y^2 + a_{11}xy + \cdots + a_{t-1,t-1}x^{t-1}y^{t-1}, \tag{15}$$

where Z_d is a finite field, S is secret, d is an odd prime number, coefficients $a_{ij} \in Z_d$, $a_{ij} = a_{ji}$, $i, j \in \{0, 1, \cdots, t-1\}$.

(II) Alice calculates polynomials F(x_i,y) $(i = 1, 2, \cdots, n)$, respectively, by (15) and sends them to the corresponding participants Bob$_i$ through a secure classical channel, where $x_i \in Z_d$ is the public identity information of the corresponding participant Bob$_i$ with $x_i \neq x_j$ for $i \neq j$.

(III) According to the characteristics of binary symmetric polynomials, we define the following two groups of constants:

$$k_{i,j} = F(x_i, x_j) = F(x_j, x_i) = k_{j,i}, \tag{16}$$

$$sk_{i,j} = F(x_i, x_j) = F(x_j, x_i) = vk_{j,i}. \tag{17}$$

Remark 1. *Here, these four values are the same. However, in the following text, different symbols have different meanings. $k_{i,j}$ and $k_{j,i}$ represent the symmetry keys during encryption and decryption. $sk_{i,j}$ and $vk_{j,i}$ represent one's own identity information, used to indicate one's identity, which can be understood as one's own signature information.*

(IV) Alice chooses a one-way hash function $h()$. Then, Alice discloses the hash algorithm and hash value $H = h(S)$ of the secret S.

3.2. Secret-Recovery Phase

Suppose Bob$_1$ (reconstructor) wants to get the secret S. Then at least another $t-1$ participants need to be selected to form a qualified subset with him to jointly recover the secret S. Let us suppose B$_1$ = {Bob$_1$, Bob$_2$, $\cdots$, Bob$_t$} is a qualified subset from all the qualified subsets. Each participant in the set has the ability to independently produce a single photon. The corresponding participant will perform the following processes to recover the secret:

(I) Each participant Bob$_i$, $i = (1, 2, \cdots, t)$, calculates the shadow (S_i) of the share according to own polynomial and prepares computational basis state $|S_i\rangle$ with d-level.

$$S_i = F(x_i, 0) \prod_{j \neq i}^{t} \frac{x_j}{x_j - x_i} \bmod d. \tag{18}$$

Remark 2. *Here, $\dfrac{1}{x_j - x_i}$ is the modular multiplicative inverse of the integer $(x_j - x_i)$. According to the recent literature, this calculation has a fast calculation method. We will not expand here as readers can refer to [24].*

(II) Bob$_1$ applies QFT on the computational basis state $|S_1\rangle$ and gets the result $|\phi_1\rangle$.

$$|\phi_1\rangle = \mathrm{QFT}(|S_1\rangle) = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle. \tag{19}$$

(III) Bob$_1$ again prepares computational basis state $|0\rangle$ with d-level and performs $CNOT$ operation according to $|\phi_1\rangle$ and $|0\rangle$. $|\phi_1\rangle$ is the control bit and $|0\rangle$ is the target bit. When the operation is completed, Bob$_1$ obtains the entangled state $|\phi_2\rangle$.

$$|\phi_2\rangle = CNOT(|\phi_1\rangle, |0\rangle) = CNOT(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle, |0\rangle) = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle_H |k\rangle_T. \tag{20}$$

The subscript H and T here are used to distinguish two particles.

(IV) Bob$_1$ and Bob$_2$ mutually conduct identity authentication:

Step 1. Bob$_1$ prepares a d-level initial quantum state $|e_0^0\rangle$, two random numbers c_1, p_1, and opens p_1. Bob$_1$ performs the unitary transformation U_{p_1,c_1} on the initial quantum state and obtains a new quantum state $|\Psi_1\rangle = U_{p_1,c_1}|e_0^0\rangle = |e_{p_1}^{c_1}\rangle$. Then according to own polynomial $F(x_1, y)$, Bob$_1$ can obtain $sk_{1,2} = F(x_1, x_2)$. Subsequently, Bob$_1$ performs the unitary transformation $U_{sk_{1,2},0}$ on $|\Psi_1\rangle$ and obtains $|\Psi_{1,2}\rangle = |e_{p_1+sk_{1,2}}^{c_1}\rangle$. Bob$_1$ again determines a random moment $t_{1,2}$. Lastly, Bob$_1$ sends messages $E_{k_{1,2}}(c_1, t_{1,2})$, which has been encrypted, and $|\Psi_{1,2}\rangle$ to Bob$_2$ through secure classical channel and quantum channel, respectively.

Step 2. After Bob$_2$ receives the quantum state and encrypted information, he first calculates $vk_{2,1} = F(x_2, x_1)$ according to the own polynomial $F(x_2, y)$. Afterwards Bob$_2$ performs the unitary transformation $U_{-vk_{2,1},0}$ on $|\Psi_{1,2}\rangle$ and obtains $|\Psi_1\rangle' = |e_{p_1+sk_{1,2}-vk_{2,1}}^{c_1}\rangle$. Then, Bob$_2$ obtains a number pair $(c_1, t_{1,2}) = D_{k_{2,1}}(E_{k_{1,2}}(c_1, t_{1,2}))$ by decrypting the received classic information. Finally, Bob$_2$ uses the basis $\{|e_l^{c_1}\rangle\}(l \in Z_d)$ to measure $|\Psi_1\rangle'$ to obtain the measurement result $(p_1)'$ and compares $(p_1)'$ with the published random number p_1. If $(p_1)' = p_1$; then, Bob$_2$ considers that all the information comes from Bob$_1$. The identity information of Bob$_1$ is authenticated. Otherwise, Bob$_2$ considers that the message does not come from Bob$_1$ or is destroyed in the middle of the process and terminates this agreement.

Step 3. After Bob$_2$ confirms that the message originated from Bob$_1$, he also prepares a d-level initial quantum state $|e_0^0\rangle$, two random numbers c_2, p_2, and opens p_2. Then, Bob$_2$ performs the unitary transformation U_{p_2,c_2} on $|e_0^0\rangle$ and obtains a new quantum state $|\Psi_{2,1}\rangle = U_{p_2,c_2}|e_0^0\rangle = |e_{p_2}^{c_2}\rangle$. Bob$_2$ decides another moment $t_{2,1}$ and sends encrypted message $E_{k_{2,1}}(c_2, t_{2,1})$ to Bob$_1$. Lastly, Bob$_2$ is ready to send $|\Psi_{2,1}\rangle$ to Bob$_1$ at moment $t_{2,1}$.

Step 4. Bob$_1$ decrypts the encrypted classical information to obtain a random number pair $(c_2, t_{2,1}) = D_{k_{1,2}}(E_{k_{2,1}}(c_2, t_{2,1}))$. After receiving the message particle from Bob$_2$ at moment $t_{2,1}$, Bob$_1$ selects the basis $\{|e_l^{c_2}\rangle\}(l \in Z_d)$ to measure $|\Psi_{2,1}\rangle$ to obtain the measurement result $(p_2)'$ and compares $(p_2)'$ with the published random number p_2. If $(p_2)' = p_2$, Bob$_1$ believes that all the information comes from Bob$_2$ and Bob$_2$ has received an own message. So, Bob$_1$ will send the auxiliary state $|k\rangle_T$ in his own hand to Bob$_2$ through the secure quantum channel at moment $t_{1,2}$. The entire identity authentication process is shown in Figure 2 below:

Remark 3. *Here, secure quantum channel refers to a quantum channel that is not subject to external interference. That is, an authenticated quantum channel. Participants can engage in quantum direct communication.*

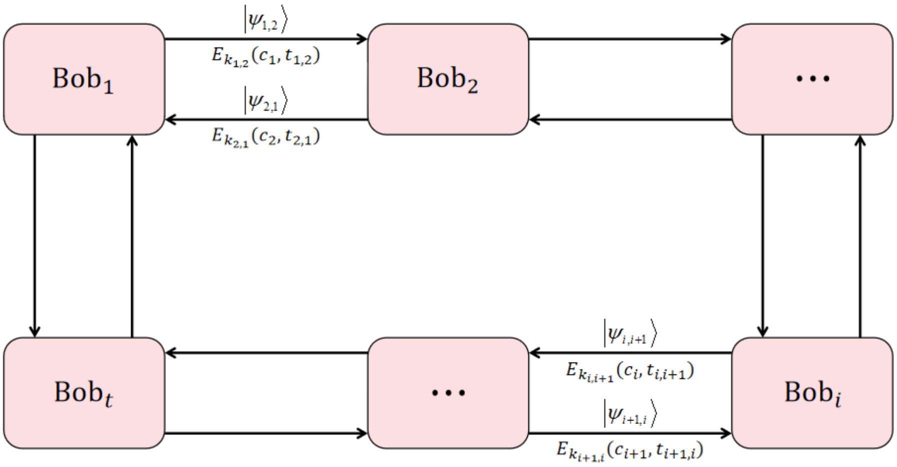

Figure 2. Identity authentication process between participants in this scheme.

(V) After Bob$_2$ receives $|k\rangle_T$ at moment $t_{1,2}$, he treats $|k\rangle_T$ as the control bit and $|S_2\rangle$ as the target bit. Then, Bob$_2$ performs controlled black box operation C_k on these two quantum states, where C_k can be expressed as:

$$C_k : |k\rangle_T |S_2\rangle \rightarrow |k\rangle_T U^k |S_2\rangle. \tag{21}$$

U is a linear transformation and it satisfies $U|S_2\rangle = \omega^{S_2}|S_2\rangle$. That is to say, $|S_2\rangle$ is an eigenvector of U with an eigenvalue of ω^{S_2}. After performing the controlled black box operation, Bob$_2$ next conducts the direct product operation of $|S_2\rangle$ and $|k\rangle_T$. Then, the whole quantum state system becomes $|\phi_3\rangle$.

$$\begin{aligned}
|\phi_3\rangle &= (I \otimes I \otimes C_k)(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle_H |k\rangle_T |S_2\rangle) \\
&= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle_H |k\rangle_T U^k |S_2\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle_H |k\rangle_T \omega^{S_2 k} |S_2\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(S_1+S_2)k} |k\rangle_H |k\rangle_T |S_2\rangle.
\end{aligned} \tag{22}$$

(VI) Each participant, Bob$_i$ and Bob$_{i+1}$, repeat the above mutual authentication and operation process of Bob$_1$ and Bob$_2$. When Bob$_2$ and Bob$_3$ complete mutual authentication, Bob$_2$ will send the auxiliary state $|k\rangle_T$ in his own hand to Bob$_3$ through the secure quantum channel at moment $t_{2,3}$. Bob$_3$ also performs a similar controlled black box operation first. Then, he performs the direct product operation on his quantum state $|S_3\rangle$ and the whole quantum system, and so on, until the last participant Bob$_t$ completes the direct product operation. At this time, the whole quantum system becomes $|\phi_4\rangle$.

$$|\phi_4\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(\sum\limits_{i=1}^{t} S_i)k} |k\rangle_H |k\rangle_T |S_2\rangle |S_3\rangle \cdots |S_t\rangle. \tag{23}$$

(VII) When Bob$_t$ completes the direct product operation, Bob$_t$ completes the identity authentication process with Bob$_1$ in the same way. After completing the authentication operation, Bob$_t$ retransmits the auxiliary state $|k\rangle_T$ back to Bob$_1$ through a secure quantum channel. After Bob$_1$ receives the auxiliary state $|k\rangle_T$ again, he performs $CNOT$ operation on the two particles in his hand, where $|k\rangle_H$ is control bit and $|k\rangle_T$ is target bit. At this time, the whole quantum system becomes $|\phi_5\rangle$.

$$\begin{aligned}
|\phi_5\rangle &= (CNOT(\frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(\sum\limits_{i=1}^{t} S_i)k} |k\rangle_H |k\rangle_T)) |S_2\rangle |S_3\rangle \cdots |S_t\rangle \\
&= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(\sum\limits_{i=1}^{t} S_i)k} |k\rangle_H |0\rangle_T |S_2\rangle |S_3\rangle \cdots |S_t\rangle.
\end{aligned} \tag{24}$$

(VIII) Bob$_1$ uses computational basis to measure the quantum state $|k\rangle_T$ which has been handled by the $CNOT$ operation. If the measurement result is $|0\rangle$, Bob$_1$ believes that his auxiliary particles have not been destroyed or replaced. Bob$_1$ will continue to perform the following steps. Otherwise Bob$_1$ has reason to believe that the auxiliary state is damaged or replaced during the transmission process, thus ending the entire agreement.

(IX) Bob$_1$ applies IQFT on his first quantum state $|k\rangle_H$ and measures the output to obtain the final secret $S' = \sum\limits_{i=1}^{t} S_i \bmod d$.

(X) Bob$_1$ calculates $H' = h(S')$ according to hash function $h()$ released by Alice and compares it with public $H = h(S)$. If $H' = H$, S', the secret obtained by Bob$_1$ is the real secret. If not, Bob$_1$ has reason to believe that there is at least one dishonest participant, thus terminating the agreement.

4. Correctness Analysis

In this section, we show the correctness of the protocol in the secret recovery phase through two theorems.

Theorem 1. *The sum of t shares of participants is the secret to be recovered.*

Proof. According to the Lagrange interpolation formula, we have

$$\begin{aligned}\sum_{i=1}^{t} S_i \bmod d &= F(x_1,0)\prod_{j=2}^{t}\frac{x_j}{x_j-x_1}+\cdots+F(x_t,0)\prod_{j=1}^{t-1}\frac{x_j}{x_j-x_t} \bmod d\\ &= F(0,0)\\ &= S.\end{aligned} \tag{25}$$

□

Theorem 2. *When Bob$_1$ applies the IQFT on the first quantum state $|k\rangle_H$ in his hand and measures the output result, he could gobtain the secret S.*

Proof.

$$\begin{aligned}&\mathrm{IQFT}\otimes I\big(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{(\sum_{i=1}^{t} S_i)k}|k\rangle_H|0\rangle_T\big)\\ =&\big(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{(\sum_{i=1}^{t} S_i)k}\mathrm{IQFT}|k\rangle_H\big)|0\rangle_T\\ =&\big(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{(\sum_{i=1}^{t} S_i)k}\big(\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{-lk}\big)|l\rangle_H\big)|0\rangle_T\\ =&\big(\frac{1}{d}\sum_{k=0}^{d-1}\sum_{l=0}^{d-1}\omega^{(\sum_{i=1}^{t} S_i-l)k}\big)|0\rangle_T\\ =&\big(\frac{1}{d}\sum_{k=0}^{d-1}|\sum_{i=1}^{t} S_i \bmod d\rangle_H+\frac{1}{d}\sum_{l=0,l\neq\sum_{i=1}^{t} S_i}^{d-1}\big(\sum_{k=0}^{d-1}\omega^{(\sum_{i=1}^{t} S_i-l)k}\big)|l\rangle_H\big)|0\rangle_T\\ =&\big(|\sum_{i=1}^{t} S_i \bmod d\rangle_H+\frac{1}{d}\sum_{l=0,l\neq\sum_{i=1}^{t} S_i}^{d-1}0|l\rangle_H\big)|0\rangle_T\\ =&|\sum_{i=1}^{t} S_i \bmod d\rangle_H|0\rangle_T\\ =&|F(0,0)\rangle_H|0\rangle_T\\ =&|S\rangle_H|0\rangle_T.\end{aligned} \tag{26}$$

□

5. Security Analysis

In this section, we analyze the security of our scheme against quantum attacks [25–29].

5.1. Intercept–Resend Attack

Suppose that there is an eavesdropper, Eve, who wants to steal secret information by performing an intercept–resend attack. When Bob$_i$ communicates with Bob$_{i+1}$, there will be three quantum states interacting through the quantum channel. They are $|\Psi_{i,i+1}\rangle = |e^{c_i}_{p_i+sk_{i,i+1}}\rangle$, $|\Psi_{i+1,i}\rangle = |e^{c_{i+1}}_{p_{i+1}}\rangle$, and auxiliary state $|k\rangle_T$. When Eve intercepts $|\Psi_{i,i+1}\rangle$ and $|\Psi_{i+1,i}\rangle$, she needs to obtain information by measuring, but Eve does not know the measurement basis c_i and c_{i+1}. If Eve arbitrarily chooses a set of bases to measure, the probability of success is $\frac{1}{d}$ when $d \rightarrow \infty$, $\frac{1}{d} \rightarrow 0$. Therefore, the possibility of success is negligible. Even if Eve succeeds, $|\Psi_{i,i+1}\rangle$ and $|\Psi_{i+1,i}\rangle$ are also just the quantum states needed for Bob$_i$ and Bob$_{i+1}$ to verify their identities. These two quantum states have no information about secrets. As for auxiliary state $|k\rangle_T$, it is only the control bit in the secret recovery process and also has no information about secrets. Therefore, the intercept–resend attack is not successful.

5.2. Entangle–Measure Attack

In this attack, the eavesdropper Eve prepares an auxiliary state $|e\rangle$. By using unitary transformation to entangle the auxiliary state $|e\rangle$ onto the transmission particle, Eve measures the auxiliary state and compares it with the original result to obtain relevant information about the secret. In our scheme, only particle $|k\rangle_T$ is transferred between participants in the secret recovery phase. Therefore, suppose that when Bob$_1$ transfers particle $|k\rangle_T$ to Bob$_2$, Eve performs the d-level $CNOT$ operation to entangle the auxiliary state $|e\rangle$ to the particle $|k\rangle_T$. At this time, $|\phi_2\rangle$ becomes $|\phi_2\rangle'$.

$$|\phi_2\rangle' = (CNOT(|k\rangle_T, |e\rangle))|\phi_2\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{S_1 k} |k\rangle_H |k\rangle_T |k \oplus e\rangle. \tag{27}$$

When Bob$_2$ completes its own operation and transfers particle $|k\rangle_T$ to Bob$_3$, Eve performs d-level $CNOT$ operation again. Where particle $|k\rangle_T$ is the control bit and auxiliary state $|k+e\rangle$ is target bit. At this time, $|\phi_3\rangle$ becomes $|\phi_3\rangle'$.

$$\begin{aligned} |\phi_3\rangle' &= (CNOT(|k\rangle_T, |k \oplus e\rangle))|\phi_3\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(S_1+S_2)k} |k\rangle_H |k\rangle_T |S_2\rangle |k \oplus k \oplus e\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{(S_1+S_2)k} |k\rangle_H |k\rangle_T |S_2\rangle |e\rangle. \end{aligned} \tag{28}$$

Next, Eve obtains the result e by measuring the auxiliary state particle. She concludes that the particles transmitted between participants are the same. The particle $|k\rangle_T$ has no information about sharing the secret. She cannot obtain any information about the secret. Therefore, the entangle–measure attack is not feasible.

5.3. Collusion Attack

In the collusion attack, some collusive participants want to obtain information about others' sharing of secrets through cooperation. Then, they can obtain the original secret. In our protocol, the sharing of secrets is calculated by each participant Bob$_i$ through the own share polynomial $F(x_i, y)$. Each participant only knows his own share. In addition, the sharing of secrets will not be disclosed or transferred to other participants. As a consequence, it is impossible for participants to obtain the others' sharing of secrets. So collusive attack is not feasible.

5.4. Forgery Attack

Suppose the participant Bob$_i$ wants to perform a forgery attack. Then, in the identity authentication phase, to prove his identity to Bob$_{i-1}$ and Bob$_{i+1}$, Bob$_i$ must use the correct authentication information. He cannot use forged information, or the agreement will end early. In the secret-recovery phase, on the one hand, if Bob$_i$ forges an auxiliary state $|k\rangle_T{}'$ and transmits it to Bob$_{i+1}$, then the measurement result of Bob$_1$ in **(VIII)** will not be $|0\rangle$. Bob$_1$ believes that the auxiliary state has been damaged and terminates the agreement in advance. On the other hand, if Bob$_i$ uses his sharing of S_i to forge a false computational basis state $|S_i\rangle'$, Bob$_1$ will get the wrong secret S' eventually. By comparing $h(S') \neq h(S)$, Bob$_1$ believes that at least one participant is dishonest and ends the agreement. Therefore, our protocol can resist forgery attacks.

6. Scheme Comparison

In this section, we analyze the quantum resources needed by our protocol and compare it with some previous protocols.

The protocol of Yang et al. [3] operates in d-dimensional space; it is a (n, n) threshold scheme. The scheme needs $(n-1)$ message particles and performs n number of QFT operations and n number of measure operations. It uses fewer quantum resources, but the scheme is not flexible enough. This scheme can resist any computational attack, but it cannot resist collusion attacks.

The protocol of Song et al. [7] operates in d-dimensional space, it is a (t, n) threshold scheme. The secret reconstructor prepares t message particles and distributes $(t-1)$ number of them to the other participants. The reconstructor starts with an QFT. Until the other participants complete the operation, the reconstructor performs an IQFT and measures particles to obtain the secret. Finally, the reconstructor verifies it through the hash function. This protocol can resist various common attacks. However, after some calculation and analysis, due to the mutual entanglement between particles, simple IQFT cannot recover the secret.

The protocol of Sutradhar et al. [8] is d level with (t, n) threshold. Using the Lagrange interpolation formula, the reconstructor first applies QFT to a particle. After each participant adds its share to the whole recovery process, the reconstructor uses the IQFT to recover the secret and measures to obtain the secret. The whole secret recovery process is repeated twice using two polynomials to restore the secret and the hash value of the secret, respectively. Through this method, the reconstructor can verify the correctness of the message. However, the protocol must require a trusted reconstructor, so the protocol can not resist collusion attack and can resist other common attacks.

The protocol of Mashhadi et al. [9] is an improvement to the protocol of Song et al. [7]. The protocol points out the inadequacy of its entanglement and proposes an improved scheme. Since the IQFT performed by the reconstructor cannot obtain the secret, t participants are required to perform IQFT in the entanglement system and summarize the measurement results to obtain the initial secret. Therefore, the protocol cannot resist intercept–resend attacks and collusion attacks.

Our protocol is also d level with (t, n) threshold. The dealer uses the binary symmetric polynomial to distribute the share polynomial. Each participant can use its own share polynomial to calculate the secret share and complete the identity authentication process. The protocol uses $2t$ number of message particles to complete the mutual authentication process of both parties. Finally, the reconstructor restores the secret by performing IQFT and obtains the secret through measurement. Although our protocol uses more quantum resources, every step is necessary. The identity authentication process will make the protocol more secure and reliable. Our protocol can also resist some attacks well. The comparison of these protocols is shown in Table 1 below.

Table 1. Comparison of parameters among our protocol and previous protocols.

Protocols	Yang [3]	Song [7]	Sutradhar [8]	Mashhadi [9]	Our
$(t, n)threshold$	N	Y	Y	Y	Y
QFT	n	1	2	1	1
IQFT	-	1	2	t	1
measurement operation	n	1	2	t	$2t+1$
dimensional space	d	d	d	d	d
message particle	$n-1$	t	$t+1$	t	$3t+1$
hash function	2	2	2	2	2
intercept–resend	-	Y	Y	N	Y
entangle–measure	-	Y	Y	Y	Y
collusive attack	N	Y	N	N	Y
forgery attack	-	Y	Y	Y	Y
identity authentication	N	N	N	N	Y

7. Example

In this section, in order to better understand our protocol, we give a quantum secret sharing scheme with (4,6) threshold. In this protocol, t = 4, n = 6, d = 17, S = 2.

7.1. Secret-Sharing Phase

Alice performs the following operations:

(I) Alice selects a binary symmetric polynomial $F(x, y)$ of degree 3 in the Z_{17}.

$$\begin{aligned} F(x, y) =& 2+7x+7y+3x^2+3y^2+9xy+4x^3+4y^3+5x^2y+5xy^2 \\ &+10x^3y+10xy^3+8x^2y^2+3x^3y^2+3x^2y^3+15x^3y^3, \end{aligned} \tag{29}$$

where secret S = 2.

(II) Alice calculates polynomials F(x_i,y) $(i = 1, 2, \cdots, 6)$, respectively, by Equation (29) and sends them to the corresponding participants Bob$_i$ through a secure channel, where $x_i = i$. Here, the polynomial obtained by each Bob$_i$ is:

$$\begin{aligned} &\text{Bob}_1 : F(1, y) = 16+14y+2y^2+15y^3; \\ &\text{Bob}_2 : F(2, y) = 9+6y+y^2+3y^3; \\ &\text{Bob}_3 : F(3, y) = 5+9y+y^2+7y^3; \\ &\text{Bob}_4 : F(4, y) = 11+15y+3y^2+15y^3; \\ &\text{Bob}_5 : F(5, y) = 16y+8y^2+15y^3; \\ &\text{Bob}_6 : F(6, y) = 14+4y+12y^3. \end{aligned} \tag{30}$$

(III) According to the characteristics of binary symmetric polynomial, constants have the following relationship: $sk_{i,j} = vk_{j,i} = k_{i,j} = k_{j,i} = F(x_i, x_j) = F(x_j, x_i)$. According to the selected binary symmetric polynomial and the identity information of each participant, we can obtain:

$$\begin{aligned} &sk_{1,2} = vk_{2,1} = k_{1,2} = k_{2,1} = F(x_1, x_2) = F(x_2, x_1) = 2; \\ &sk_{2,3} = vk_{3,2} = k_{2,3} = k_{3,2} = F(x_2, x_3) = F(x_3, x_2) = 15; \\ &sk_{3,4} = vk_{4,3} = k_{3,4} = k_{4,3} = F(x_3, x_4) = F(x_4, x_3) = 12; \\ &sk_{4,1} = vk_{1,4} = k_{4,1} = k_{1,4} = F(x_4, x_1) = F(x_1, x_4) = 10. \end{aligned} \tag{31}$$

(IV) Alice chooses a one-way hash function $h()$. Then, Alice discloses the hash algorithm and hash value $H = h(2)$ of the secret S = 2.

7.2. Secret-Recovery Phase

Suppose Bob_1(reconstructor) wants to get the secret S. Bob_1 chooses Bob_2, Bob_3, and Bob_4 to help him recover the secret. Each participant has the ability to independently produce a single photon.

(I) Each participant Bob_i, $i = (1,2,3,4)$, calculates the shadow (S_i) of the share according to the own polynomial $F(x_i, y)$.

$$\text{Bob}_1 : S_1 = F(1,0) \cdot \frac{2}{2-1} \cdot \frac{3}{3-1} \cdot \frac{4}{4-1} \bmod 17 = 13. \tag{32}$$

Similarly, S_2 = 14, S_3 = 3, S_4 = 6. Then, they separately prepare a 17-level computational basis state $|13\rangle$, $|14\rangle$, $|3\rangle$, and $|6\rangle$.

(II) Bob_1 applies QFT on the computational basis state $|13\rangle$ and obtains the result $|\phi_1\rangle$.

$$|\phi_1\rangle = \text{QFT}(|13\rangle) = \frac{1}{\sqrt{17}} \sum_{k=0}^{16} \omega^{13k} |k\rangle. \tag{33}$$

(III) Bob_1 again prepares computational basis state $|0\rangle$ with 17-levels and performs $CNOT$ operation according to $|\phi_1\rangle$ and $|0\rangle$. $|\phi_1\rangle$ is the control bit and $|0\rangle$ is the target bit. When the operation is completed, Bob_1 obtains the entangled state $|\phi_2\rangle$.

$$|\phi_2\rangle = CNOT(|\phi_1\rangle, |0\rangle) = CNOT(\frac{1}{\sqrt{17}} \sum_{k=0}^{16} \omega^{13k} |k\rangle, |0\rangle) = \frac{1}{\sqrt{17}} \sum_{k=0}^{16} \omega^{13k} |k\rangle_H |k\rangle_T. \tag{34}$$

(IV) Bob_1 and Bob_2 mutually conduct identity authentication:

Step 1. Bob_1 prepares a 17-level initial quantum state $|e_0^0\rangle$, 2 random numbers c_1 = 6, p_1 = 8, and opens p_1. Bob_1 performs the unitary transformation $U_{p_1,c_1} = U_{8,6}$ on the initial quantum state and obtains a new quantum state $|\Psi_1\rangle = U_{8,6}|e_0^0\rangle = |e_8^6\rangle$. Then, according to the own polynomial $F(1,y)$, Bob_1 can obtain $sk_{1,2} = F(1,2) = 2$. Subsequently, Bob_1 performs the unitary transformation $U_{2,0}$ on $|\Psi_1\rangle$ and obtains $|\Psi_{1,2}\rangle = U_{2,0}|e_8^6\rangle = |e_{10}^6\rangle$. Bob_1 again determines a random moment $t_{1,2} = 9$. Lastly, Bob_1 sends message $E_{k_{1,2}}(6,9)$, which has been encrypted, and $|\Psi_{1,2}\rangle$ to Bob_2 through secure classical channel and quantum channel, respectively.

Step 2. After Bob_2 receives the quantum state and encrypted information, he first calculates $vk_{2,1} = F(2,1) = 2$ according to the own polynomial $F(2,y)$. Afterwards, Bob_2 performs the unitary transformation $U_{-2,0}$ on $|\Psi_{1,2}\rangle$ and obtains $|\Psi_1\rangle' = U_{-2,0}|e_{10}^6\rangle = |e_{10-2}^6\rangle = |e_8^6\rangle$. Then, Bob_2 obtains a number pair $(6,9) = D_{k_{2,1}}(E_{k_{1,2}}(6,))$ by decrypting the received classic information. Finally, Bob_2 uses the basis $\{|e_l^6\rangle\}(l \in Z_{17})$ to measure $|\Psi_1\rangle'$ to obtain the measurement result $(p_1)'$ and compares $(p_1)'$ with the published random number $p_1 = 8$. If $(p_1)' = 8$, then Bob_2 considers that all the information comes from Bob_1. The identity information of Bob_1 is authenticated. Otherwise, Bob_2 considers that the message does not come from Bob_1 or is destroyed in the middle of the process and terminates this agreement.

Step 3. After Bob_2 confirms that the message originated from Bob_1, he also prepares a 17-level initial quantum state $|e_0^0\rangle$, 2 random numbers $c_2 = 5$, $p_2 = 12$, and opens p_2. Then, Bob_2 performs the unitary transformation $U_{p_2,c_2} = U_{12,5}$ on $|e_0^0\rangle$ and obtains a new quantum state $|\Psi_{2,1}\rangle = U_{12,5}|e_0^0\rangle = |e_{12}^5\rangle$. Bob_2 decides another moment $t_{2,1} = 7$ and sends encrypted message $E_{k_{2,1}}(5,7)$ to Bob_1. Lastly, Bob_2 is ready to send $|\Psi_{2,1}\rangle$ to Bob_1 at moment $t_{2,1} = 7$.

Step 4. Bob_1 decrypts the encrypted classical information to obtain a random number pair $(5,7) = D_{k_{1,2}}(E_{k_{2,1}}(5,7))$. After receiving the message particle from Bob_2 at moment $t_{2,1} = 7$, Bob_1 selects the basis $\{|e_l^5\rangle\}(l \in Z_{17})$ to measure $|\Psi_{2,1}\rangle$ to obtain the measurement result $(p_2)'$ and compares $(p_2)'$ with the published random number $p_2 = 12$. If $(p_2)' = p_2 = 12$, Bob_1 believes that all the information comes from Bob_2 and Bob_2 has received an own message. So, Bob$_1$ will send the auxiliary state $|k\rangle_T$ in his own hand to Bob$_2$ through the secure quantum channel at moment $t_{1,2} = 9$.

(V) After Bob$_2$ receives $|k\rangle_T$ at moment $t_{1,2} = 9$, he treats $|k\rangle_T$ as the control bit and $|S_2\rangle = |14\rangle$ as the target bit. He performs controlled black box operation C_k on these two quantum states. After performing the controlled black box operation, Bob$_2$ next conducts the direct product operation on $|S_2\rangle = |14\rangle$ and $|k\rangle_T$. Then the whole quantum state system becomes $|\phi_3\rangle$.

$$\begin{aligned}|\phi_3\rangle &= (I \otimes I \otimes C_k)(\frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{13k}|k\rangle_H|k\rangle_T|14\rangle)\\ &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{13k}|k\rangle_H|k\rangle_T U^k|14\rangle\\ &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{13k}|k\rangle_H|k\rangle_T\omega^{14k}|14\rangle\\ &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{(13+14)k}|k\rangle_H|k\rangle_T|14\rangle.\end{aligned} \tag{35}$$

(VI) Each participant Bob$_i$ and Bob$_{i+1}$ repeat the above mutual authentication and operation process of Bob$_1$ and Bob$_2$. When Bob$_2$ and Bob$_3$ complete mutual authentication, Bob$_2$ will send the auxiliary state $|k\rangle_T$ in his own hand to Bob$_3$ through the secure quantum channel at moment $t_{2,3} = 15$. Bob$_3$ also performs a similar controlled black box operation first. Then, he performs the direct product operation on his quantum state $|S_3\rangle = |3\rangle$ and the whole quantum system, and so on, until the last participant Bob$_4$ completes the direct product operation. At this time, the whole quantum system becomes $|\phi_4\rangle$.

$$\begin{aligned}|\phi_4\rangle &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{(13+14+3+6)k}|k\rangle_H|k\rangle_T|14\rangle|3\rangle|6\rangle\\ &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}|k\rangle_H|k\rangle_T|14\rangle|3\rangle|6\rangle.\end{aligned} \tag{36}$$

(VII) When Bob$_4$ completes the direct product operation, Bob$_4$ completes the identity authentication process with Bob$_1$ in the same way. After completing the authentication operation, Bob$_4$ retransmits the auxiliary state $|k\rangle_T$ back to Bob$_1$ through a secure quantum channel. After Bob$_1$ receives the auxiliary state $|k\rangle_T$ again, he performs a $CNOT$ operation on the two particles in his hand, where $|k\rangle_H$ is control bit and $|k\rangle_T$ is target bit. At this time, the whole quantum system becomes $|\phi_5\rangle$.

$$\begin{aligned}|\phi_5\rangle &= (CNOT(\frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}|k\rangle_H|k\rangle_T))|14\rangle|3\rangle|6\rangle\\ &= \frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}|k\rangle_H|0\rangle_T|14\rangle|3\rangle|6\rangle.\end{aligned} \tag{37}$$

(VIII) Bob$_1$ uses computational basis to measure the quantum state $|k\rangle_T$ which has been handled by $CNOT$ operation. If the measurement result is $|0\rangle$, Bob$_1$ believes that his auxiliary particles have not been destroyed or replaced. Bob$_1$ will continue to perform the following steps. Otherwise Bob$_1$ has reason to believe that the auxiliary state is damaged or replaced during the transmission process, thus ending the entire agreement.

(IX) Bob$_1$ applies IQFT on his first quantum state $|k\rangle_H$ and measures the output to obtain the final secret $S' = 2$.

$$\begin{aligned}
&\mathrm{IQFT} \otimes I(\frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}|k\rangle_H|0\rangle_T) \\
=&(\frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}\mathrm{IQFT}|k\rangle_H)|0\rangle_T \\
=&(\frac{1}{\sqrt{17}}\sum_{k=0}^{16}\omega^{2k}(\frac{1}{\sqrt{17}}\sum_{l=0}^{16}\omega^{-lk})|l\rangle_H)|0\rangle_T \\
=&(\frac{1}{17}\sum_{k=0}^{16}\sum_{l=0}^{16}\omega^{(2-l)k}|l\rangle_H)|0\rangle_T \\
=&(\frac{1}{17}\sum_{k=0}^{16}|2\rangle_H + \frac{1}{17}\sum_{l=0,l\neq 2}^{16}(\sum_{k=0}^{16}\omega^{2-l)k})|l\rangle_H)|0\rangle_T \\
=&(|2\rangle_H + \frac{1}{17}\sum_{l=0,l\neq 2}^{16}0|l\rangle_H)|0\rangle_T \\
=&|2\rangle_H|0\rangle_T.
\end{aligned} \tag{38}$$

(X) Bob$_1$ calculates $H' = h(2)$ according to hash function $h()$ released by Alice and compares with public $H = h(S)$. If $H' = H$, S', the secret obtained by Bob$_1$ is the real secret. If not, Bob$_1$ has reason to believe that there is at least one dishonest participant, thus terminating the agreement.

8. Conclusions

In this article, using QFT, IQFT, mutually unbiased bases, and other relevant knowledge, we propose a quantum secret-sharing scheme that both sides of the communication can mutually verify the identity. Each participant holds his own share which will neither be disclosed nor transferred. Only at the secret-recovery stage, each participant will directly integrate his information into the whole quantum system, which avoids being stolen. Any participant has reason to recover the secret and only the reconstructor obtains the secret and is responsible for it. Since only t participants can recover the secret, the protocol is more flexible and practical. After our analysis, the protocol can resist intercept–resend attacks, entanglement–measurement attacks, collusion attacks, and forgery attacks, so it is safe enough.

Author Contributions: Writing—original draft, D.M.; Writing—review & editing, Z.L., S.L. and Z.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, grant number 11671244.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The relevant data in Section 7 is arbitrarily selected and calculated by us.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. How to share a secret. *Commun. ACM* **1979**, *22*, 612–613. [CrossRef]
2. Hillery, M.; Buzk, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
3. Yang, W.; Huang, L.; Shi, R. Secret sharing based on quantum Fourier transform. *Quantum Inf. Process.* **2013**, *12*, 2465–2474. [CrossRef]
4. Tavakoli, A.; Herbauts, I.; Zukowski, M.; Bourennane, M. Secret sharing with a single *d*-level quantum system. *Phys. Rev. A* **2015**, *92*, 030302. [CrossRef]

5. Tsai, C.W.; Yang, C.W.; Lin, J. Multiparty mediated semi-quantum secret sharing protocol. *Quantum Inf. Process.* **2022**, *21*, 63. [CrossRef]
6. Chou, Y.H.; Zeng, G.J.; Chen, X.Y.; Kuo, S.Y. Multiparty weighted threshold quantum secret sharing based on the Chinese remainder theorem to share quantum information. *Sci. Rep.* **2021**, *11*, 6093. [CrossRef]
7. Song, X.L.; Liu, Y.B.; Deng, H.Y.; Xiao, Y.G. (t, n) Threshold d-Level Quantum Secret Sharing. *Sci. Rep.* **2017**, *7*, 6366. [CrossRef]
8. Sutradhar, K.; Om, H. Efficient quantum secret sharing without a trusted player. *Quantum Inf. Process.* **2020**, *19*, 73. [CrossRef]
9. Mashhadi, S. Improvement of a (t, n) threshold d-level quantum secret sharing scheme. *J. Appl. Secur. Res.* **2022**, *17*, 123–134. [CrossRef]
10. Li, F.L.; Yan, J.Y.; Zhu, S.X. General quantum secret sharing scheme based on two qudit. *Quantum Inf. Process.* **2021**, *20*, 328. [CrossRef]
11. Cao, W.F.; Yang, Y.G. Verifiable quantum secret sharing protocols based on four-qubit entangled states. *Int. J. Theor. Phys.* **2019**, *58*, 1202–1214. [CrossRef]
12. Lu, C.B.; Miao, F.Y.; Hou, J.P.; Huang, W.C.; Y, X. A verifiable framework of entanglement-free quantum secret sharing with information-theoretical security. *Quantum Inf. Process.* **2020**, *19*, 24. [CrossRef]
13. Li, F.L.; Hu, H.; Zhu, S.X.; Yan, J.Y.; Ding, J. A verifiable (k, n) threshold dynamic quantum secret sharing scheme. *Quantum Inf. Process.* **2022**, *21*, 259. [CrossRef]
14. Yan, C.H.; Li, Z.H.; Liu, L.; Lu, D.J. Cheating identifiable (k, n) threshold quantum secret sharing scheme. *Quantum Inf. Process.* **2022**, *21*, 8. [CrossRef]
15. Yang, Y.G.; Wen, Q.Y.; Zhang, X. Multiparty simultaneous quantum identity authentication with secret sharing. *Sci. China Phys. Mech. Astron.* **2008**, *51*, 321–327. [CrossRef]
16. Abulkasim, H.; Hamad, S.; Khalifa, A.; Bahnasy, K.E. Quantum secret sharing with identity authentication based on Bell states. *Int. J. Quantum Inf.* **2017**, *15*, 1750023. [CrossRef]
17. Hu, W.W.; Zhou, R.G.; Li, X.; Fan, P.; Tan, C.Y. A novel dynamic quantum secret sharing in high-dimensional quantum system. *Quantum Inf. Process.* **2021**, *20*, 159. [CrossRef]
18. Liu, J.Y.; Zhou, X.Y.; Wang, Q. Reference-frame-independent measurement-device-independent quantum key distribution using fewer states. *Phys. Rev. A* **2021**, *103*, 022602. [CrossRef]
19. Li, W.; Wang, L.; Zhao, S.M. Extended single-photon entanglement based phase-matching quantum key distribution. *Quantum Inf. Process.* **2022**, *21*, 124. [CrossRef]
20. Liu, B.; Gao, Z.; Xiao, D.; Huang, W.; Liu, X.; Xu, B. Quantum identity authentication in the orthogonal-state-encoding QKD system. *Quantum Inf. Process.* **2019**, *18*, 137. [CrossRef]
21. Ljunggren, D.; Bourennane, M.; Karlsson, A. Authority-based user authentication in quantum key distribution. *Phys. Rev. A* **2002**, *62*, 022305. [CrossRef]
22. Dutta, A.; Pathak, A. A short review on quantum identity authentication protocols: How would bob know that he is talking with alice? *Quantum Inf. Process.* **2022**, *21*, 369. [CrossRef]
23. Bostrom, K.; Felbinger, T. Deterministic secure direct communicationusing entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902. [CrossRef] [PubMed]
24. Bufalo, M.; Bufalo, D.; Orlando, G. A Note on the Computation of the Modular Inverse for Cryptography. *Axioms* **2021**, *10*, 116. [CrossRef]
25. Zou, X.F.; W, Q.D. Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A* **2010**, *82*, 042325. [CrossRef]
26. Wang, T.Y.; Wen, Q.Y. Security of a kind of quantum secret sharing with single photons. *Quant. Inf. Comput.* **2011**, *11*, 434–443. [CrossRef]
27. Wang, T.Y.; Liu, Y.Z.; Wei, C.Y.; Cai, X.Q.; Ma, J.F. Security of a kind of quantum secret sharing with entangled states. *Sci. Rep.* **2017**, *7*, 2485. [CrossRef]
28. Colbeck, R. Impossibility of secure two-party classical computation. *Phys. Rev. A* **2007**, *76*, 062308. [CrossRef]
29. Mayers, D. Unconditional security in quantum cryptography. *J. ACM* **2001**, *48*, 351–406. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.