

Improved quantum (*t*,*n*) threshold group signature

Yaodong Zhang(张耀东), Feng Liu(刘锋), and Haixin Zuo(左海新)

Citation: Chin. Phys. B, 2023, 32 (**9**): 090308. DOI: 10.1088/1674-1056/acac0a
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Improved statistical fluctuation analysis for two decoy-states phase-matching quantum key distribution

Jiang-Ping Zhou(周江平), Yuan-Yuan Zhou(周媛媛), Xue-Jun Zhou(周学军), and Xuan Bao(暴轩)
Chin. Phys. B, 2023, 32 (**8**): 080306. DOI: 10.1088/1674-1056/acbdea

Variational quantum simulation of the quantum critical regime

Zhi-Quan Shi(石志全), Xu-Dan Xie(谢旭丹), and Dan-Bo Zhang(张旦波)
Chin. Phys. B, 2023, 32 (**8**): 080305. DOI: 10.1088/1674-1056/accb43

Variational quantum semi-supervised classifier based on label propagation

Yan-Yan Hou(侯艳艳), Jian Li(李剑), Xiu-Bo Chen(陈秀波), and Chong-Qiang Ye(叶崇强)
Chin. Phys. B, 2023, 32 (**7**): 070309. DOI: 10.1088/1674-1056/acb9fb

Improved quantum key agreement protocol with authentication

Ji-Hong Guo(郭继红), Ming-Qiang Bai(柏明强), Xiao-Yan Lei(雷小燕), Jia-Xin Xie(谢佳欣), and Zhi-Wen Mo(莫智文)
Chin. Phys. B, 2023, 32 (**5**): 050310. DOI: 10.1088/1674-1056/ac9b31

Lorentz quantum computer

Wenhao He(何文昊), Zhenduo Wang(王朕铎), and Biao Wu(吴飙)
Chin. Phys. B, 2023, 32 (**4**): 040304. DOI: 10.1088/1674-1056/acad6a

---

Improved quantum (t,n) threshold group signature

Yaodong Zhang(张耀东)[1,†], Feng Liu(刘锋)[2], and Haixin Zuo(左海新)[1]

[1] *College of Computer Science and Technology, Shandong Technology and Business University, Yantai* 264005, *China*
[2] *College of Mathematic and Information Science, Shandong Technology and Business University, Yantai* 264005, *China*

(Received 11 September 2022; revised manuscript received 13 December 2022; accepted manuscript online 16 December 2022)

Threshold signature is an important branch of the digital signature scheme, which can distribute signature rights and avoid the abuse of signature rights. With the continuous development of quantum computation and quantum information, quantum threshold signatures are gradually becoming more popular. Recently, a quantum (t,n) threshold group signature scheme was analyzed that uses techniques such as quantum-controlled-not operation and quantum teleportation. However, this scheme cannot resist forgery attack and does not conform to the design of a threshold signature in the signing phase. Based on the original scheme, we propose an improved quantum (t,n) threshold signature scheme using quantum (t,n) threshold secret sharing technology. The analysis proves that the improved scheme can resist forgery attack and collusion attack, and it is undeniable. At the same time, this scheme reduces the level of trust in the arbitrator during the signature phase.

Keywords: quantum (t,n) threshold signature, quantum (t,n) threshold secret sharing, forgery attack, collusion attack

PACS: 03.67.Ac, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/acac0a

1. Introduction

As an important branch of the digital signature scheme, threshold signature can ensure the security of transmitted information, provide data integrity and realize identity authentication. After Desmedt and Frankel[1] first proposed the (t,n) threshold signature scheme in 1991, the study of threshold signature has become increasingly popular. For a threshold signature group consisting of n members, a combination of greater than or equal to t members can represent the group to sign messages.[2–4]

With the introduction of the Shor[5] algorithm, the security of traditional digital signatures has been greatly threatened. Cryptosystems based on quantum mechanics can achieve unconditional security, so the study of quantum signatures has become the focus of most researchers. The concept of a quantum signature was first introduced by Gottesman and Chuang[6] in 2001, but the public key in their scheme can only be used once. To make quantum signatures more practical, the first arbitrated quantum signature based on Greenberger–Horne–Zeilinger states was proposed by Zeng *et al.*[7] in 2002. Subsequently, arbitrated quantum signatures gradually became the basic quantum signature scheme.[8–12] Although quantum signature schemes are emerging, many are still in the theoretical research stage. In recent years, many physically realizable quantum signature schemes have been proposed,[13–17] for example Yin *et al.*[13] produced the first work on practical quantum digital signature without secure channels and performed the first experiment without assuming any secure channel,[14] while Lu *et al.*[15] solved two major restrictions of quantum signatures by a post-matching method. These studies paved the way for the practical application of quantum signatures. The present paper concerns a quantum (t,n) threshold signature scheme based on d-dimensional quantum systems; it is still in the theoretical research stage and its physical implementation needs further study.

For a threshold signature, the requirement of a threshold is essential. We added the quantum threshold secret sharing technique to the original signature scheme as part of the design of this new scheme. In 2017, Song *et al.*[18] implemented classical secret sharing based on Shamir secret sharing and the quantum Fourier transform technique. However, their scheme was later shown to be incapable of recovering the secret. In 2018, Mashhadi[19] designed a hybrid secret sharing scheme based on quantum Fourier transform and a monotonic spanning program that implements the features of classical and quantum secret sharing. In 2021, Sutradhar *et al.*[20] improved the scheme of Song *et al.* by increasing the number of quantum Fourier inversions, making the scheme more complex. In this paper we design a threshold scheme based on Shamir secret sharing and the quantum Fourier transform that can be added to quantum signatures. Compared with the previous secret sharing schemes, our scheme does not contain quantum Fourier inversions and significantly reduces the number of quantum measurements.

Recently, a quantum (t,n) threshold group signature scheme that uses techniques such as quantum-controlled-not operations and quantum teleportation was analyzed.[21] After analysis of the scheme by Guo *et al.*,[22] the original scheme was found not to be a (t,n) threshold group signature scheme

[†]Corresponding author. E-mail: zhangyd136@163.com

© 2023 Chinese Physical Society and IOP Publishing Ltd

because any number of members in the scheme could generate a valid signature. The original scheme also has problems with key leakage and trustworthiness of the arbitrator. After our analysis of Qin *et al.*'s scheme,[21] we also found that a forgery attack cannot be resisted in the original scheme.

To address the above issues, we applied the designed quantum (t,n) threshold secret sharing technique to the original signature scheme[21] and improved the original signature scheme. The analysis shows that the improved scheme can resist forgery attack and collusion attack, and it is undeniable. At the same time, this scheme reduces the level of trust in the arbitrator during the signature phase.

2. Preliminaries

In this section we define the preliminaries of our scheme, including Shamir secret sharing, quantum Fourier transform (QFT), the SUM gate and the generalized Pauli operator.

(i) Shamir secret sharing:[23] Share generation: the dealer uses a $t-1$ order polynomial to assign n secret shares to n signing participants

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_{t-1}x^{t-1}. \tag{1}$$

Secret reconstruction: greater than or equal to the threshold number of participants reconstruct the secret

$$f(x)=\sum_{i=1}^{t}f(x_i)\prod_{j=1,j\neq i}^{t}\frac{x-x_j}{x_j-x_i}. \tag{2}$$

(ii) Quantum Fourier transform:[24,25] The QFT is a quantum version of the standard discrete Fourier transform, which is a unitary transformation of a quantum system. For α, $\beta\in\{0,1,\ldots,d-1\}$, the QFT is defined as

$$\mathrm{QFT}\,|\alpha\rangle\rightarrow\frac{1}{\sqrt{d}}\sum_{\beta=0}^{d-1}\mathrm{e}^{2\pi\mathrm{i}\frac{\alpha}{d}\beta}\,|\beta\rangle\,. \tag{3}$$

(iii) The SUM gate:[26,27] In d-dimensional Hilbert space, the quantum SUM gate is defined by

$$\mathrm{SUM}(|x\rangle\,,|y\rangle)=(|x\rangle\,,|x+y\bmod d\rangle), \tag{4}$$

where $|x\rangle$ is the control particle, $|y\rangle$ is the target particle and $x,y\in\{0,1,\ldots,d-1\}$.

(iv) In d-dimensional Hilbert space, the generalized Pauli operator is defined by[28,29]

$$U_{\alpha,\beta}=\sum_{x=0}^{d-1}\omega^{\beta x}\,|x+\alpha\rangle\,\langle x|\,, \tag{5}$$

where $\alpha,\beta\in\{0,1,\ldots,d-1\}$, $\omega=\mathrm{e}^{2\pi\mathrm{i}/d}$ and $+$ denotes the addition module d. In particular, when $\alpha,\beta\in\{0,1\}$, we have

$$X_d=U_{1,0}=\sum_{x=0}^{d-1}|x+1\rangle\,\langle x|\,, \tag{6}$$

$$Z_d=U_{0,1}=\sum_{x=0}^{d-1}\omega^x\,|x\rangle\,\langle x|\,. \tag{7}$$

3. Brief review of Qin's scheme

In this section, we briefly introduce the quantum (t,n) threshold group signature scheme proposed by Qin *et al.* in 2020,[21] as well as pointing out the security problems in the scheme.

3.1. Initializing phase

The quantum message being signed has m quantum states. Alice$_i$ $(i\in\{1,2,\ldots,n\})$ and Charlie share the private key K_{A_i} via the quantum key distribution (QKD) protocol, Bob and Charlie share the private key K_{B}, both in $2m$ bits. Alice$_i$ and Bob share m Bell states, Alice$_i$ holds the particle $|a_{ij}\rangle$, Bob holds the particle $|b_{ij}\rangle$.

3.2. Signing phase

(i) Any t members of the signature group can sign the message, the signed message $|P_1\rangle=|P_2\rangle=|P_3\rangle=\bigotimes_{i=1}^{m}|p_i\rangle=\bigotimes_{i=1}^{m}(\alpha_i|0\rangle+\beta_i|1\rangle)$.

(ii) t members encrypt $|P_1\rangle$ into $|R\rangle$ with the private key K_{A_i} and send $|R\rangle$ and $|P_2\rangle$ to Bob.

(iii) $|P_3\rangle$ will compose m entangled states $\bigotimes_{i=1}^{m}|\phi_i\rangle$ $(|\phi_i\rangle=\alpha_i|\overbrace{0\cdots0}^{t}\rangle+\beta_i|\overbrace{1\cdots1}^{t}\rangle)$ after $m(t-1)$ quantum-controlled-not operations. Alice$_i$ performs m Bell measurements. In the j-th Bell measurement, one particle is the i-th particle of $|\phi_j\rangle$, and the other particle is $|a_{ij}\rangle$. Alice$_i$ uses her private key K_{A_i} to encrypt the measurement result C_i and gets C_i', then she sends it to Bob.

3.3. Verifying phase

(i) After Bob receives $|R\rangle\,,|P_2\rangle\,,C_i'$, he uses private key K_{B} to encrypt them, and then sends them to Charlie.

(ii) Charlie receives the ciphertext and decrypts it to verify whether $|R\rangle$ is the ciphertext of $|P_2\rangle$. If it is, he sets $r=1$, otherwise $r=0$. Charlie encrypts the decrypted C_i' and $|R\rangle$ with the key K_{B} to obtain the signature $S=E(C_i,R)$. Then, Charlie uses his private key K_{B} to encrypt $S,|P_2\rangle\,,r,C_i$, and sends it to Bob.

(iii) Bob first checks whether $r=1$. If $r=1$, Bob performs corresponding unitary operation on particle $|b_{ij}\rangle$ according to c_{ij}, and recovers $|\phi_i\rangle=\alpha_i|\overbrace{0\cdots0}^{t}\rangle+\beta_i|\overbrace{1\cdots1}^{t}\rangle$.

(iv) Bob measures the first $t-1$ qubits in the $\{|+\rangle\,,|-\rangle\}$ basis and records the measurement results. If the result is $|+\rangle$, Bob sets $d_{ij}=0$, if the result is $|-\rangle$, he sets $d_{ij}=1$. Bob computes $D_j=d_{1j}\oplus d_{2j}\oplus\cdots\oplus d_{(t-1)j}$. If $D_j=1$, Bob will carry out σ_z operation on the last qubit and do nothing if $D_j=0$. Finally, Bob recovers the original quantum message $|P_3\rangle$.

(v) Bob compares whether $|P_3\rangle$ is equal to $|P_2\rangle$. If they are equal, Bob accepts the signature; otherwise, he rejects it.

4. Security issues in the original scheme

Guo *et al.*[22] pointed out that the quantum (t,n) threshold group signature scheme proposed by Qin *et al.*[21] has the following three issues:

(i) The original scheme is not the (t,n) threshold group signature scheme. The signature process of the scheme does not conform to the meaning of threshold signature: a valid signature can be generated only when t or more members sign together, otherwise a valid signature cannot be generated.

(ii) Bob can get both the encrypted classical message C_i' and the corresponding text C_i. Then applying the XOR operation on these two messages bit by bit, Bob can learn the key K_{A_i}. Namely Bob can fabricate a valid signature for any message.

(iii) The arbitrator Charlie is completely trusted, which can cause greater difficulties in the practical application.

Through our analysis of Qin *et al.*'s scheme, we found that the scheme has another security issue. This issue will enable Bob to forge the signature and makes Charlie lose the right to arbitrate the signature. The analysis is as follows:

(iv) In the original scheme, Bob receives $|R\rangle$, $|P_2\rangle$ and C_i' from Alice. For $|R\rangle$, the original scheme uses Li *et al.*'s encryption method,[30] $|R\rangle = E_{K_\mathrm{A}}|P\rangle = \bigotimes_{i=1}^{m} E_{K_\mathrm{A}^i}|p_i\rangle$, $|p_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$.

K_A^i	$E_{K_\mathrm{A}^i}$
0	X
1	Z

Here $E_{K_\mathrm{A}^i} \in \{X,Z\}$ are the Pauli operators. From the commutativity of Pauli operators

$$XX = I, \quad YY = I, \quad ZZ = I,$$
$$XY = -YX, \quad XZ = -ZX, \quad ZY = -YZ.$$

Bob can perform the same Pauli operation U_i on $|R\rangle$ and $|P_2\rangle$

$$|P^*\rangle = \bigotimes_{i=1}^{m} U_i|p_i\rangle,$$
$$|R^*\rangle = \bigotimes_{i=1}^{m} U_i E_{K_\mathrm{A}^i}|p_i\rangle = \bigotimes_{i=1}^{m} \pm E_{K_\mathrm{A}^i} U_i|p_i\rangle,$$

where $U_i \in \{I,X,Z,\mathrm{i}Y\}$. Since the global phase factor ± 1 has no observed effect under the quantum swap test circuit of quantum states, $(|P^*\rangle, |R^*\rangle)$ can always pass Charlie's verification. After $(|P^*\rangle, |R^*\rangle)$ has passed Charlie's verification, the signature $S^* = E(C_i, |R^*\rangle)$ will be generated. Thus Bob completes the forgery of the signature. Later, if there is a dispute over the signature, Alice claims that she did not sign the message $|P^*\rangle$ and the arbitrator Charlie will check $|P^*\rangle$ and $|R^*\rangle$. After checking, Charlie will think Alice is lying. So Charlie makes an error of judgment and loses his arbitration.

5. Improved scheme

The members of our scheme include n members of signature group $N = \{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$, the signature receiver Bob and the arbitrator Charlie. The improved scheme consists of three parts: the initialization phase, the signature phase and the verification phase.

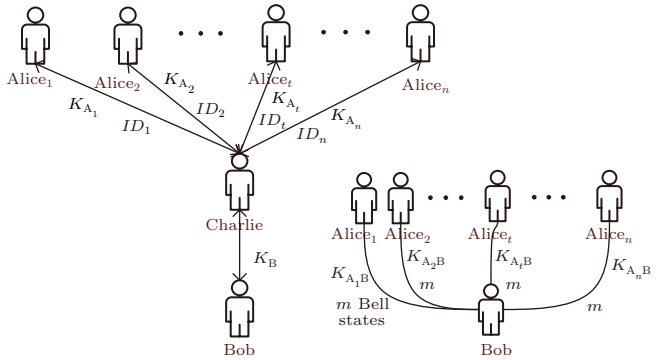


Fig. 1. The initialization phase of the proposed scheme.

5.1. Initialization phase

(i) Each of $\{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$ shares a private key K_{A_i} with Charlie, Bob shares a private key K_B with Charlie and each of $\{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$ shares a private key $K_{\mathrm{A}_i\mathrm{B}}$ with Bob. All keys are $2m$ bits. All the above processes are implemented by quantum key distribution or quantum secure direct communication.[31–33]

(ii) Each of $\{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$ shares m Bell states with Bob. We denote the j-th Bell state of Alice_i as $|\phi_{ij}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, where $i \in \{1,2,\ldots,n\}$, $j \in \{1,2,\ldots,m\}$. Alice_i holds the first particle sequence $|a_{ij}\rangle$ in the Bell state and Bob holds the second particle sequence $|b_{ij}\rangle$.

(iii) According to Bertrand's postulate,[34] given t and n, $\{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$ and Charlie can find a suitable prime d satisfying $n \le d \le 2n$ and set a finite field Z_d. $\{\mathrm{Alice}_1, \mathrm{Alice}_2, \ldots, \mathrm{Alice}_n\}$ and Charlie share a polynomial $f(x)$, $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1}x^{t-1} \bmod d$, where $(a_0, a_1, \ldots, a_{t-1}) \in Z_d$, a_0 being the secret value. Charlie tells the identity information ID_i to Alice_i over a classical secure channel (e.g., QKD-based secure communication).

(iv) There is a correspondence between any single bit i and qubit $|i\rangle$ in the scheme as follows:

$$i = 0 \leftrightarrow |L\rangle = a|0\rangle + b|1\rangle, \quad i = 1 \leftrightarrow |R\rangle = b|0\rangle - a|1\rangle. \quad (8)$$

Its measurement form is known to all participants. In addition, the Bell pair in the scheme has the following correspondence with the two classical bits:

$$|\phi^+\rangle \leftrightarrow 00, \quad |\phi^-\rangle \leftrightarrow 01, \quad |\psi^+\rangle \leftrightarrow 10, \quad |\psi^-\rangle \leftrightarrow 11. \quad (9)$$

5.2. Signature phase

(i) Without loss of generality, let

$$T=\{\text{Alice}_1,\text{Alice}_2,\ldots,\text{Alice}_t\}$$

be the t actual signers. They generates the three same quantum messages $|P_1\rangle=|P_2\rangle=|P_3\rangle=\bigotimes_{i=1}^{m}|p_i\rangle$, where $|p_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$, with $|\alpha_i|^2+|\beta_i|^2=1$.

(ii) Alice$_i$($i\in\{1,2,\ldots,t\}$) encrypts $|P_1\rangle$ into $|R_{\rm A}\rangle$ using the key $K_{{\rm A}_i}$.[35] That is, a one-way hash function f which makes f: $\{0,1\}^{2m}\to\{0,1\}^m$, mapping the $2m$ key $K_{{\rm A}_i}$ into a binary bit string $L=\{l_1,l_2,\ldots,l_m\}$. Each qubit corresponds to a classical bit l_i. For the sake of exposition, the swapping of the i-th and $(m-i+1)$-th qubits in the signature sequence is defined first. We introduce the parameter $\tau^i=l_i\oplus l_{m-i+1}$ and the symmetric rotation $R_2^{\tau^i}$ which satisfies

$$S_2=R_2^{\tau^i}(x_0,x_1)=\begin{cases}(x_0,x_1), & \tau^i=0,\\ (x_1,x_0), & \tau^i=1.\end{cases}\tag{10}$$

Moreover, $R_m^{\tau^i}$ can be generalized into

$$\begin{aligned}S_m&=R_m^{\tau^i}(x_0,x_1,\ldots,x_{m-1})\\&=(x_{\tau^i},x_{\tau^i+1},\ldots,x_{m-1},x_0,x_1,\ldots,x_{\tau^i-1}),\end{aligned}\tag{11}$$

where $\tau^i=(l_1+l_2+\cdots+l_m)$ mod m and S_m is equivalent to a circular shift operation on m qubits. Alice$_1$ encrypts $|P_1\rangle$ first, and the rest of Alice$_r$ encrypts it in turn. The encryption form is

$$E_{K_{{\rm A}_i}}(|P_1\rangle)=S_m^i\bigotimes_{i=1}^{m}\sigma_x^{k_{2i}}\sigma_z^{k_{2i-1}}|p_i\rangle.\tag{12}$$

$\{\text{Alice}_1,\text{Alice}_2,\ldots,\text{Alice}_t\}$ prepare m decoy photons, each chosen randomly from the set $\{|r\rangle\}$ and $\{\text{QFT}|r\rangle\}$, $r\in\{0,1,\ldots,d-1\}$, and insert the m decoy photons randomly into $|R_{\rm A}\rangle$.

(iii) Without loss of generality, any one of the t signers is selected, assumed to be Alice$_1$. Alice$_1$ prepares t qudit particles $|0\rangle_1,|0\rangle_2,\ldots,|0\rangle_t$, and each particle has $\lceil\log_2 d\rceil$ qubits. Alice$_1$ performs the QFT on the first particle $|0\rangle_1$ and then gets $|\varphi_1\rangle$, the state $|\varphi_1\rangle$ is denoted by $|\varphi_1\rangle=\frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}|y\rangle_1$. Then, Alice$_1$ performs SUM operation on $|0\rangle_r$, where $|\varphi_1\rangle$ is the control qudit and $|0\rangle_r$ ($r\in\{2,3,\ldots,t\}$) is the target qudit, to generate the state $|\varphi_2\rangle=\frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}|y\rangle_1|y\rangle_2\cdots|y\rangle_t$. Alice$_1$ sends the particle $|y\rangle_r$ to the participant Alice$_r$.

(iv) Alice$_i$ publishes her ID_i to Alice$_r$ ($r\in\{1,2,\ldots,t\}$). Alice$_i$ ($i\in\{1,2,\ldots,t\}$) computes the secret share $S_i=f(ID_i)\prod_{j=1,j\neq i}^{t}\frac{ID_j}{ID_j-ID_i}$ mod d, then performs QFT on $|y\rangle_i$, $\text{QFT}|y\rangle_i=\frac{1}{\sqrt{d}}\sum_{K_i=0}^{d-1}\omega^{yK_i}|K_i\rangle$. After performing the above operation, Alice$_i$ performs the $U_{S_i,0}$ operation

$$U_{S_i,0}|K_i\rangle=|K_i+S_i\rangle,\tag{13}$$

where $+$ denotes addition modulo d. The state $|\varphi_2\rangle$ evolves as state $|\varphi_3\rangle$:

$$\begin{aligned}|\varphi_3\rangle&=(U_{S_{1,0}}\text{QFT})\otimes(U_{S_{2,0}}\text{QFT})\otimes\cdots\otimes(U_{S_{t,0}}\text{QFT})|\varphi_2\rangle\\&=d^{-\frac{t+1}{2}}\sum_{K_1+K_2+\cdots+K_t=0\bmod d}|K_1+S_1\rangle|K_2+S_2\rangle\\&\quad\otimes\cdots\otimes|K_t+S_t\rangle.\end{aligned}$$

Alice$_i$ uses the computational basis $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle\}$ to measure $|K_i+S_i\rangle$, then Alice$_i$ obtains and saves the measurement result (K_i+S_i). (K_i+S_i) is converted to a binary bit string and converted to $|KS_i\rangle$ according to Eq. (8).

For example, take $t=3$, $n=5$, $d=7$, $K_1=5$ and $S_1=6$. Then $K_1+S_1=4$ mod 7, $4_{(10)}\to0100_{(2)}$.

(v) Alice$_1$ holds the m particles of $|P_3\rangle$. The other $t-1$ members each generate m single particles, and each particle is $|0\rangle$. Then Alice$_1$ performs $m(t-1)$ CNOT$_{ij}$ ($i\in\{1,2,\ldots,m\}$, $j\in\{2,3,\ldots,t\}$). In CNOT$_{ij}$, the control particle is the i-th particle of Alice$_1$, and the target particle is the i-th particle of Alice$_j$. The particles of $\{\text{Alice}_1,\text{Alice}_2,\ldots,\text{Alice}_t\}$ will compose m entangled states $|\Phi\rangle=\bigotimes_{i=1}^{m}|\phi_i\rangle=\alpha_i|\overbrace{0\cdots0}^{t}\rangle+\beta_i|\overbrace{1\cdots1}^{t}\rangle$.

(vi) Alice$_i$ performs Bell measurements. In the j-th ($j\in\{1,2,\ldots,m\}$) Bell measurement, one particle is the i-th particle of $|\phi_j\rangle$, and the other particle is $|a_{ij}\rangle$. Alice$_i$ gets the measurement result $|C_i\rangle=\bigotimes_{j=1}^{m}|c_i^j\rangle$, where $|c_i^j\rangle$ is the random Bell state. Alice$_i$ uses the private key $K_{{\rm A}_i{\rm B}}$ to encrypt $|C_i\rangle$, uses $K_{{\rm A}_i}$ to encrypt $|KS_i\rangle$ and inserts m decoy photons into $E_{K_{{\rm A}_i{\rm B}}}|C_i\rangle$. Finally, $\{\text{Alice}_1,\text{Alice}_2,\ldots,\text{Alice}_t\}$ send the ciphertext of $\{|R_{\rm A}\rangle,|C_i\rangle,|KS_i\rangle,|P_2\rangle\}$ to Bob.

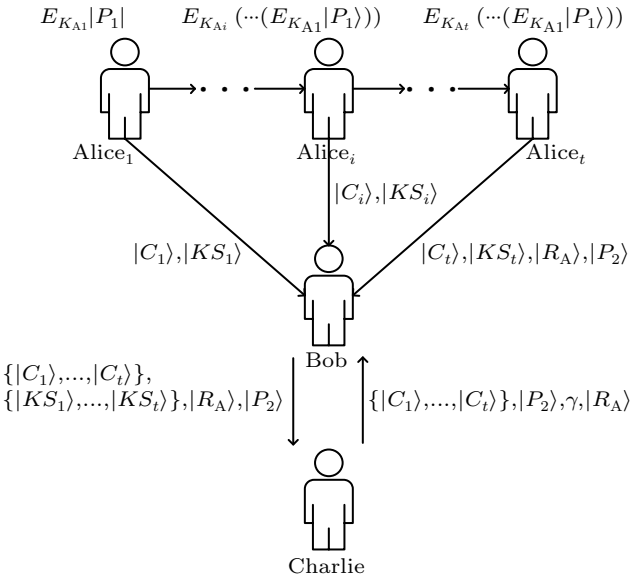


Fig. 2. The flow-process diagram of the proposed scheme.

5.3. Verification phase

(i) Bob directly encrypts the information sent from $\{\text{Alice}_1, \text{Alice}_2, \ldots, \text{Alice}_t\}$ with the private key K_B and sends it to Charlie.

(ii) Charlie uses his private key K_B to decrypt the information from Bob and gets $|R_\text{A}\rangle, |KS_i\rangle, |P_2\rangle, E_{K_{\text{A}_j\text{B}}}|C_i\rangle$. $\{\text{Alice}_1, \text{Alice}_2, \ldots, \text{Alice}_t\}$ tell Charlie the location of the decoy photons and the preparation basis. Charlie uses the preparation basis to measure the decoy photons at the corresponding positions and tells $\{\text{Alice}_1, \text{Alice}_2, \ldots, \text{Alice}_t\}$ the measurement results, and $\{\text{Alice}_1, \text{Alice}_2, \ldots, \text{Alice}_t\}$ determines whether the decoy photons are eavesdropped by comparing the initial states of the decoy photons. If the quantum channel is insecure, then the protocol is terminated; otherwise, the protocol is continued.

(iii) Charlie will perform two steps: (1) Charlie converts $|KS_i\rangle$ to $K_i + S_i$, verifying that $\sum_{i=1}^{t}(K_i + S_i) \bmod d = a_0$; (2) Charlie verifies that $|R_\text{A}\rangle$ is the ciphertext of $|P_2\rangle$. Charlie sets and makes public the verification parameter $\gamma = 1$ if both of the above steps hold, otherwise $\gamma = 0$. Charlie encrypts $\{E_{K_{\text{A}_i\text{B}}}|C_i\rangle, |P_2\rangle, \gamma, |R_\text{A}\rangle\}$ with the private key K_B and sends it to Bob.

(iv) Bob decrypts the ciphertext and gets $|C_i\rangle$, $|P_2\rangle$, γ, $|R_\text{A}\rangle$. If $\gamma = 0$, Bob rejects the signature. If $\gamma = 1$, Bob verifies whether $|C_i\rangle$ is eavesdropped in the same way. Then Bob performs the unitary operation on his particles $|b_{ij}\rangle$ ($i \in \{1,2,\ldots,t\}$, $j \in \{1,2,\ldots,m\}$) as follows: if $|c_i^j\rangle = |\phi^+\rangle$, he performs $\sigma_I = |0\rangle\langle 0| + |1\rangle\langle 1|$ on $|b_{ij}\rangle$; if $|c_i^j\rangle = |\phi^-\rangle$, he performs $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ on $|b_{ij}\rangle$; if $|c_i^j\rangle = |\psi^+\rangle$, he performs $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ on $|b_{ij}\rangle$; if $|c_i^j\rangle = |\psi^-\rangle$, he performs $\mathrm{i}\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ on $|b_{ij}\rangle$.

(v) Bob measures the first $t-1$ qubits of $|b_{ij}\rangle$ in the basis $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. If the measurement result is $|+\rangle$, then $d_{ij} = 0$ ($i \in \{1,2,\ldots,t-1\}$, $j \in \{1,2,\ldots,m\}$); if the result is $|-\rangle$, then $d_{ij} = 1$. Finally, Bob computes $D_j = d_{1j} \oplus d_{2j} \oplus \cdots \oplus d_{(t-1)j}$. If $D_j = 0$, Bob performs σ_I on the last qubit; if $D_j = 1$, Bob performs σ_z on the last qubit. Then Bob can recover the original message $|P_2\rangle'$.

(vi) Bob compares $|P_2\rangle$ with $|P_2\rangle'$. If they are equal, Bob accepts the signature; otherwise, he rejects it.

6. Analysis of improvement scheme

In this section, we will prove the correctness and security of the improved scheme and compare the performance of our improved scheme with the original scheme.

6.1. Correctness

For the correctness of the scheme, we focus on the correctness of the (t,n) threshold and the correctness of the verification phase.

6.1.1. Correctness of the (t,n) threshold

In the signature phase, Alice_1 gets $|\varphi_1\rangle$ by performing the QFT on the first particle $|0\rangle_1$. Then, Alice_1 performs SUM operation on $|0\rangle_r$ and gets $|\varphi_2\rangle$:

$$|\varphi_2\rangle = \frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}|y\rangle_1|y\rangle_2\cdots|y\rangle_t. \tag{14}$$

Alice_i ($i \in \{1,2,\cdots,t\}$) performs QFT and $U_{S_i,0}$ on her particle, and gets $|\varphi_3\rangle$:

$$\begin{aligned}
|\varphi_3\rangle &= (U_{S_1,0}\text{QFT})\otimes(U_{S_2,0}\text{QFT})\otimes\cdots\otimes(U_{S_t,0}\text{QFT})|\varphi_2\rangle \\
&= \frac{1}{\sqrt{d}}\sum_{y=0}^{d-1}(U_{S_1,0}\text{QFT})|y\rangle_1\otimes(U_{S_2,0}\text{QFT})|y\rangle_2 \\
&\quad\otimes\cdots\otimes(U_{S_t,0}\text{QFT})|y\rangle_t \\
&= d^{-\frac{t+1}{2}}\sum_{y=0}^{d-1}\left(\left(\sum_{K_1=0}^{d-1}\omega^{K_1 y}|K_1+S_1\rangle\right)\right. \\
&\quad\left.\otimes\cdots\otimes\left(\sum_{K_t=0}^{d-1}\omega^{K_t y}|K_t+S_t\rangle\right)\right) \\
&= d^{-\frac{t+1}{2}}\sum_{K_1,K_2,\cdots,K_t}\left(\left(\sum_{y=0}^{d-1}\omega^{(K_1+K_2+\cdots+K_t)y}\right)|K_1+S_1\rangle\right. \\
&\quad\left.\otimes\cdots\otimes|K_t+S_t\rangle\right),
\end{aligned} \tag{15}$$

where $\omega = \mathrm{e}^{\frac{2\pi\mathrm{i}}{d}}$. We denote $K_1+K_2+\cdots+K_t$ as K, then we have

$$\sum_{y=0}^{d-1}\omega^{Ky} = \begin{cases} d, & K = 0\ (\bmod d), \\ 0, & K \neq 0\ (\bmod d). \end{cases} \tag{16}$$

(i) Clearly, when $K = 0\ (\bmod\ d)$, $\sum_{y=0}^{d-1}\omega^{0y} = d$.

(ii) When $K \neq 0\ (\bmod\ d)$, $\sum_{y=0}^{d-1}\omega^{Ky} = \sum_{y=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}Ky}{d}}$, we denote $2\pi K/d$ as x, we have

$$\begin{aligned}
\sum_{y=0}^{d-1}\mathrm{e}^{\frac{2\pi\mathrm{i}Ky}{d}} &= \sum_{y=0}^{d-1}\mathrm{e}^{\mathrm{i}xy} \\
&= \sum_{y=0}^{d-1}\left(\frac{\mathrm{e}^{\mathrm{i}xy}+\mathrm{e}^{-\mathrm{i}xy}}{2}+\frac{\mathrm{e}^{\mathrm{i}xy}-\mathrm{e}^{-\mathrm{i}xy}}{2}\right).
\end{aligned} \tag{17}$$

Since

$$\sum_{y=1}^{d}\mathrm{e}^{\mathrm{i}xy} = \frac{1-\mathrm{e}^{\mathrm{i}xd}}{1-\mathrm{e}^{\mathrm{i}x}}\mathrm{e}^{\mathrm{i}x} = \frac{1-\mathrm{e}^{\mathrm{i}xd}}{-2\mathrm{i}\sin(\frac{x}{2})}\mathrm{e}^{\mathrm{i}\frac{x}{2}}, \tag{18}$$

$$\sum_{y=1}^{d}\mathrm{e}^{-\mathrm{i}xy} = \frac{1-\mathrm{e}^{-\mathrm{i}xd}}{1-\mathrm{e}^{-\mathrm{i}x}}\mathrm{e}^{-\mathrm{i}x} = \frac{1-\mathrm{e}^{-\mathrm{i}xd}}{2\mathrm{i}\sin(\frac{x}{2})}\mathrm{e}^{-\mathrm{i}\frac{x}{2}}. \tag{19}$$

So

$$\sum_{y=1}^{d}(\mathrm{e}^{\mathrm{i}xy}+\mathrm{e}^{-\mathrm{i}xy}) = \frac{\sin[(d+\frac{1}{2})x]}{\sin\frac{x}{2}} - 1, \tag{20}$$

$$\sum_{y=1}^{d}(\mathrm{e}^{\mathrm{i}xy}-\mathrm{e}^{-\mathrm{i}xy}) = \frac{\cos\frac{x}{2}-\cos[(d+\frac{1}{2})x]}{\sin\frac{x}{2}}, \tag{21}$$

and we have

$$\begin{aligned}\sum_{y=0}^{d-1}\frac{\mathrm{e}^{\mathrm{i}xy}+\mathrm{e}^{-\mathrm{i}xy}}{2} &= \sum_{y=1}^{d}\frac{\mathrm{e}^{\mathrm{i}xy}+\mathrm{e}^{-\mathrm{i}xy}}{2}+1-\frac{\mathrm{e}^{\mathrm{i}xd}+\mathrm{e}^{-\mathrm{i}xd}}{2}\\ &= -\frac{1}{2}+\frac{\sin(2\pi K+\frac{\pi K}{d})}{2\sin\frac{\pi K}{d}}=0.\end{aligned} \tag{22}$$

Similarly

$$\sum_{y=0}^{d-1}\frac{\mathrm{e}^{\mathrm{i}xy}-\mathrm{e}^{-\mathrm{i}xy}}{2}=0. \tag{23}$$

So far, we can get $\sum_{y=0}^{d-1}\omega^{Ky}=0$ if $K\neq 0 \bmod d$.

Therefore,

$$|\varphi_3\rangle = d^{-\frac{t-1}{2}}\sum_{\substack{0\le K_1,K_2,\ldots,K_t<d\\ K_1+K_2+\cdots+K_t=0 \bmod d}}|K_1+S_1\rangle|K_2+S_2\rangle\cdots|K_t+S_t\rangle.$$

By the Lagrange interpolation formula

$$f(x)=\sum_{i=1}^{t}f(x_i)\prod_{j=1,j\neq i}^{t}\frac{x-x_j}{x_j-x_i},$$

Charlie receives t (K_i+S_i) and calculates $a_0=f(0)=\sum_{i=1}^{t}(K_i+S_i) \bmod d$. If the equation holds, it means that the scheme meets the basic requirement of the threshold signature.

6.1.2. Correctness of the verification phase

After $m(t-1)$ CNOT operations, the original state $|P_3\rangle=\bigotimes_{i=1}^{m}\alpha_i|0\rangle+\beta_i|1\rangle$ will make the entangled state $|\Phi\rangle=\bigotimes_{i=1}^{m}|\phi_i\rangle=\alpha_i|\overbrace{0\cdots0}^{t}\rangle+\beta_i|\overbrace{1\cdots1}^{t}\rangle$.

Table 1. $m(t-1)$ CNOT operations.

Alice$_1$	$\alpha_1\|0\rangle+\beta_1\|1\rangle$	$\cdots$	$\alpha_m\|0\rangle+\beta_m\|1\rangle$
Alice$_2$	$\|0\rangle$	$\cdots$	$\|0\rangle$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
Alice$_t$	$\|0\rangle$	$\cdots$	$\|0\rangle$
CNOT	$\alpha_1\|\overbrace{0\cdots0}^{t}\rangle+\beta_1\|\overbrace{1\cdots1}^{t}\rangle$	$\cdots$	$\alpha_m\|\overbrace{0\cdots0}^{t}\rangle+\beta_m\|\overbrace{1\cdots1}^{t}\rangle$

Alice$_j$ performs the i-th Bell measurement $(\alpha_i|00\cdots0\rangle+\beta_i|11\cdots1\rangle)\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ and gets result.

$$\begin{cases}(\alpha_i|0\cdots\overset{j}{0}\cdots0\rangle+\beta_i|1\cdots\overset{j}{1}\cdots1\rangle)\otimes\dfrac{1}{\sqrt{2}}(|00\rangle+|11\rangle),\\ (\alpha_i|0\cdots\overset{j}{0}\cdots0\rangle-\beta_i|1\cdots\overset{j}{1}\cdots1\rangle)\otimes\dfrac{1}{\sqrt{2}}(|00\rangle-|11\rangle),\\ (\alpha_i|0\cdots\overset{j}{1}\cdots0\rangle+\beta_i|1\cdots\overset{j}{0}\cdots1\rangle)\otimes\dfrac{1}{\sqrt{2}}(|01\rangle+|10\rangle),\\ (\alpha_i|0\cdots\overset{j}{1}\cdots0\rangle-\beta_i|1\cdots\overset{j}{0}\cdots1\rangle)\otimes\dfrac{1}{\sqrt{2}}(|01\rangle-|10\rangle).\end{cases} \tag{24}$$

After all Alice$_j$'s measurements are completed, Bob performs corresponding unitary operations on $|b_{ij}\rangle$ according to the measurement results. Then Bob obtains $(\alpha_1|00\cdots0\rangle+\beta_1|11\cdots1\rangle)\otimes\cdots\otimes(\alpha_m|00\cdots0\rangle+\beta_m|11\cdots1\rangle)$. Bob measures the first $t-1$ qubits in the basis $\{|+\rangle,|-\rangle\}$. For example

$$\alpha_1|00\rangle+\beta_1|11\rangle \tag{25}$$

can be expressed as

$$\alpha_1(|+0\rangle+|-0\rangle)+\beta_1(|+1\rangle-|-1\rangle). \tag{26}$$

Recording $|+\rangle$ as 0 and $|-\rangle$ as 1, denoted by d_{ij}, Bob performs the XOR operation on the first $t-1$ qubits of $\alpha_i|\underbrace{0\cdots0}_{t-1}0\rangle+\beta_1|\underbrace{1\cdots1}_{t-1}1\rangle$. If the result is 1, Bob will carry out σ_z on the last qubit and do nothing if it is 0. In this way, Bob can get $\alpha_i|0\rangle+\beta_i|1\rangle$, and finally get the original message $|P_2\rangle'=\bigotimes_{i=1}^{m}(\alpha_i|0\rangle+\beta_i|1\rangle)$.

6.2. Security

The security characteristics of the quantum (t,n) threshold group signature scheme are mainly unforgeability, non-repudiation and resistance of collusion attack.

6.2.1. Unforgeability

In their analysis Qin *et al.*[21] used the QOTP algorithm for encryption many times in their scheme, so that Bob can get C_i and C_i' at the same time. Bob can get the private key K_{A_i} by the XOR operation, which leads Bob to forge the message and signature.

In this paper, the encryption algorithm used is the key-controlled-'T'QOTP encryption algorithm. In the design of the scheme, we circumvent the problem that Bob can obtain both $|C_i\rangle$ and its ciphertext. We encrypt $|C_i\rangle$ using the private key $K_{\mathrm{A}_i\mathrm{B}}$, and we insert decoy photons into the sent quantum sequence. In this way, we guarantee both that Bob will not recover Alice$_i$'s private key K_{A_i} and that $|C_i\rangle$ will not be falsified by the malicious arbitrator Charlie.

6.2.2. Non-repudiation

A valid signature must be encrypted by the signer's private key. In this paper's scheme, $|R_{\mathrm{A}}\rangle$, $|KS_i\rangle$ and $|C_i\rangle$ are all encrypted by Alice$_i$'s private key $(i\in\{1,2,\ldots,t\})$, so Charlie and Bob can determine whether the signature comes from a member of the signature group and Alice$_i$ cannot deny it. In the signature verification phase, Charlie first checks the legitimacy of the signature and then sends it to Bob to verify its correctness. Therefore, Bob cannot reject a valid and legitimate signature.

6.2.3. Resistance to known signature attack

In the scheme of this paper, Bob receives the $|R_{\rm A}\rangle$ and the message $|P_2\rangle$ from $\{{\rm Alice}_1, {\rm Alice}_2, \ldots, {\rm Alice}_t\}$. For the encryption of $|R_{\rm A}\rangle$ we use the 'T'QOTP encryption algorithm of Zhang *et al.*[35] If Bob performs the unitary operations on $|R_{\rm A}\rangle$ and $|P_2\rangle$:

$$|P_2\rangle^* = U|P_2\rangle, \quad |R_{\rm A}\rangle^* = U|R_{\rm A}\rangle.$$

Zhang *et al.*[35] point out that no one can conclusively determine the form of the cryptographic operator other than the legitimate participants in 'T'QOTP to achieve the correct unitary operation for each qubit, since the controlled transposition operation S_m acts on all m qubits. That is $S_m \neq \bigotimes_{i=1}^{m} u_i$, where u_i is a unitary operation on one qubit. They also point out that the probability of this encryption algorithm being successfully forged is $(1/m)^n$, with n being the number of qubits forged by Bob. In addition to this, we also inserted random decoy photons in the ciphertext $|R_{\rm A}\rangle$. Bob's execution of the above attack method will inevitably change the state of the decoy photons to such an extent that they will be detected in subsequent eavesdropping detection; the signature process is thus aborted.

6.2.4. Resistance to collusion attack

For threshold signature schemes, collusion attack is one of the most representative types of attack. Here we demonstrate the security of our scheme using two types of collusion attack.

(i) Collusion attack from $t-1$ members of signature group.

In this scheme, the secret share of S_i in the threshold phase requires ${\rm Alice}_i$'s private key for encryption. Because $K_{{\rm A}_i}$ is shared between ${\rm Alice}_i$ and Charlie via QKD, which is proven to be unconditionally secure[36], the other group members cannot obtain ${\rm Alice}_i$'s key $K_{{\rm A}_i}$. If an attacker wants to forge ${\rm Alice}_i$'s key, the probability of a successful forgery is $(1/2)^{2m}$. When $2m$ is large enough, the probability of successful forgery is nearly 0.

(ii) Collusion attack from $t-1$ members of the signature group and the malicious arbitrator Charlie.

Suppose a malicious arbitrator Charlie conspires with $t-1$ members of the signature group to attack. The $t-1$ members of the signature group can easily obtain ${\rm Alice}_i$'s private key $K_{{\rm A}_i}$, and can thus easily forge $|R_{\rm A}\rangle'$ and $|KS_i\rangle'$. But in this scheme, $|C_i\rangle$ is encrypted using the private key $K_{{\rm A}_i{\rm B}}$, and even the arbitrator Charlie cannot know ${\rm Alice}_i$'s private key $K_{{\rm A}_i{\rm B}}$. So the malicious $t-1$ members and arbitrator Charlie cannot forge a legitimate signature either.

6.3. Trustworthiness of the arbitrator

In the analysis above, the participation of the arbitrator Charlie in the collusion attack could not lead to forgery of a legitimate signature. We next analyze the trustworthiness of the arbitrator in terms of several other steps.

Since $|C_i\rangle$ is encrypted with the private key $K_{{\rm A}_i{\rm B}}$ and decoy photons are added for eavesdropping detection, Bob is fully capable of believing that $|C_i\rangle$ was sent by ${\rm Alice}_i$ and not falsified by anyone else. The problem of malicious arbitrator Charlie changing $|C_i\rangle$ analyzed by Guo and Cheng[22] can be solved here.

Charlie verifies that $\sum_{i=1}^{t}(K_i + S_i) = a_0 \bmod d$ and $|R_{\rm A}\rangle = E_{K_{\rm A}}|P_2\rangle$, and publicizes that $\gamma = 1$ or 0. If Charlie is malicious, he can always publicize γ as 0. Once $\gamma = 0$, it means that the signature group does not satisfy the threshold signature requirement or the message $|R_{\rm A}\rangle$ or $|P_2\rangle$ has been altered and thus rejected by Charlie, or Charlie is malicious. If it is a matter of threshold requirements, then $\{{\rm Alice}_1, {\rm Alice}_2, \ldots, {\rm Alice}_t\}$ only need to verify that $\sum_{i=1}^{t}(K_i + S_i) = a_0 \bmod d$ is within the signature group to confirm that Charlie is trustworthy. If the problem is $|R_{\rm A}\rangle \neq E_{K_{\rm A}}|P_2\rangle$, the accuracy of $|R_{\rm A}\rangle$ can be guaranteed in the first place due to the insertion of decoy photons into $|R_{\rm A}\rangle$ by the signature group $\{{\rm Alice}_1, {\rm Alice}_2, \ldots, {\rm Alice}_t\}$. The signature group asks the arbitrator to provide $|P_2\rangle$ to verify that $|R_{\rm A}\rangle \neq E_{K_{\rm A}}|P_2\rangle$, and if it is established, there is reason to believe that Charlie is malicious.

Charlie sends a false $|P_2\rangle''$ to Bob, who verifies that $|P_2\rangle' \neq |P_2\rangle''$; at this time the signature group is required to provide the original message $|P_3\rangle$. If $|P_2\rangle' = |P_3\rangle \neq |P_2\rangle''$, the message sent by Charlie is false.

In summary, all malicious behaviors of arbitrator Charlie in our improved scheme can be checked, so the arbitrator Charlie in our scheme cannot be completely trusted.

6.4. Performance comparison

In this section, we analyze the performance of the improved quantum (t,n) threshold signature scheme. It mainly includes whether the scheme has the function of the (t,n) threshold, the class of the (t,n) threshold, whether the scheme is resistant to forgery attacks and the trustworthiness of arbitrator.

Table 2. Performance comparison of schemes.

	(t,n)/class	Unforgeability	Trustworthiness
Qin *et al.*	no	no	trusted
Guo *et al.*	yes/classical	no	semi-trusted
The proposed scheme	yes/quantum	yes	semi-trusted

In addition, we also compare the quantum (t,n) threshold part of our scheme with the existing (t,n) threshold scheme

based on quantum Fourier transform.[18–20] In the scheme proposed by Song *et al.*,[18] the dealer uses polynomials to distribute classical secret shares and the secret reconstructors can perform CNOT operation and QFT^{-1} operation to recover the secret, but they need to obtain information from other participants. The scheme of Mashhadi[19] uses MSP instead of polynomials, and the reconstructor generates entangled states through SUM operation and QFT, and then recovers secrets through QFT and the generalized Pauli operator. The scheme proposed by Sutardhar[20] is an improvement of Song *et al.*'s scheme, and requires each participant to perform the QFT^{-1} operation on his own particle during the secret recovery phase.

In our scheme, we construct the quantum (t,n) threshold function in the original scheme using the Lagrange polynomial and quantum Fourier transform. Our d-level (t,n) threshold is more difficult and practical than the 2-level (t,n) threshold. Our scheme does not need the QFT^{-1} operation in the secret recovery phase, but only needs to send the measured results to the arbitrator, who uses the Lagrange interpolation formula to check whether the results can recover the original secret.

Table 3. Comparison of computational complexity in (t,n) threshold phase.

	Model	QFT	QFT^{-1}	Measure	Qubits
Song *et al.*	(t,n)	1	1	1	$\lceil \log_2 d \rceil t$
Mashhadi	general	1		m	$\lceil \log_2 d \rceil m$
Sutradhar *et al.*	(t,n)	1	$t-1$	t	$\lceil \log_2 d \rceil t$
The proposed scheme	(t,n)	1		t	$\lceil \log_2 d \rceil t$

7. Conclusion

In this paper, we use a quantum secret sharing scheme based on d-level quantum Fourier transform and Lagrange interpolation, adding the threshold function to a quantum (t,n) threshold signature scheme and improving on the scheme. A true quantum (t,n) threshold signature scheme is formed. The improved scheme can resist forgery attack and collusion attack, and has non-repudiation. At the same time, it can reduce the trust of the arbitrator in the signature process. Finally, we not only compare the performance of our scheme with the original scheme, but also compare the (t,n) threshold secret sharing phase with corresponding recent schemes. The results show that the scheme in this paper reduces the consumption of resources. In this paper, we have designed only a theoretical scheme for quantum (t,n) threshold signature, the physical implementation of which is subject to further study.

Acknowledgment

Project supported by the National Natural Science Foundation of China (Grant Nos. 61771294 and 61972235).

References

[1] Desmedt Y and Frankel Y 1991 *Annual International Cryptology Conference*, August 11–15, 1991, Santa Barbara, California, USA, p. 457–469

[2] Zhao L S and Liu J M 2013 *2013 5th International Conference on Intelligent Networking and Collaborative Systems*, September 9–11, 2013, Xian, Shaanxi , China, pp. 649–651

[3] Wang Y and Lu D J 2012 *2012 International Conference on Computer Science and Electronics Engineering*, March 23-25, 2012, Hangzhou, Zhejiang, China, pp. 349–352

[4] Liu D, Wang L J, Wang C and Huo P Y 2017 *Proceedings of the 2017 International Conference on Cryptography*, March 17–19, 2017, Wuhan, China, pp. 78–80

[5] Shor P W 1994 *Proceedings 35th annual symposium on foundations of computer science*, November 20–22, 1994, Santa Fe, NM, USA, pp. 124–134

[6] Gottesman D and Chuang I 2001 arXiv: quant-ph/0105032

[7] Zeng G H and Keitel C H 2002 *Phys. Rev. A* **65** 042312

[8] Lee H, Hong C, Kim H, Lim J and Yang H J 2004 *Phys. Lett. A* **321** 295

[9] Xu G B and Zhang K J 2015 *Quantum Inf. Process.* **14** 2577

[10] Zhang K J and Jia H Y 2015 *Internaltional Journal of Theoretical Physics* **54** 582

[11] Kim T, Lee H S and Lee S 2017 *Quantum Inf. Process.* **16** 268

[12] Zheng T, Zhang S B, Chang Y and Yan L L *International Conference on Artificial Intelligence and Security*, July 17–19, 2020, Hohhot, China, p. 289

[13] Yin H L, Yao F and Chen Z B 2016 *Phys. Rev. A* **93** 032316

[14] Yin H L, Yao F, Liu H, Tang Q J, Wang J, You L X, Zhang W J and Chen S J 2017 *Phys. Rev. A* **95** 032334

[15] Lu Y S, Cao X Y, Weng C X, Gu J, Xie Y M, Zhou M G, Yin H L and Chen Z B 2021 *Opt. Express* **29** 10162

[16] Weng C X, Lu Y S, Gao R Q, Xie Y M, Gu J, Li C L, Li B H, Yin H L and Chen Z B 2021 *Opt. Express* **29** 27661

[17] Yin H L, Yao F, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S and Chen Z B 2022 *Nat. Sci. Rev.* nwac228

[18] Song X L, Liu Y B, Deng H Y and Xiao Y G 2017 *Sci. Rep.* **7** 6366

[19] Mashhadi S 2019 *Quantum Inf. Process.* **18** 114

[20] Sutradhar K and Om H 2021 *Sci. Rep* **11** 17083

[21] Qin H W, Tang W K and Tso R 2020 *Quantum Inf. Process.* **19** 71

[22] Guo R and Cheng X G 2022 *Quantum Inf. Process.* **21** 37

[23] Shamir A 1979 *Communications of the ACM* **22** 612

[24] Diao Z J, Huang C and Wang K 2012 *Acta Applicandae Mathematicae* **118** 147

[25] Shi R H, Mu Y, Zhong H, Cui J and Zhang S 2016 *Sci. Rep.* **6** 19655

[26] Mashhadi S 2019 *Quantum Inf. Process.* **18** 114

[27] Yi X, Cao C, Fan L and Zhang R 2021 *Quantum Inf. Process.* **20** 7

[28] Thas. K 2009 *Europhys. Lett.* **86** 6

[29] Yang Y H, Gao F, Wu X, Qin S J, Zuo H J and Wen Q Y 2015 *Sci. Rep.* **5** 16967

[30] Li Q, Chan W H and Long D Y 2009 *Phys. Rev. A* **79** 054307

[31] Sun Y, Wen Q Y, Gao F and Zhu F C 2009 *Phys. Rev. A* **80** 032321

[32] Zhang Q, Yin J, Chen T Y, Lu S, Zhang J, Li X Q, Yang T, Wang X B and Pan J W 2006 *Phys. Rev. A* **73** 020301

[33] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T, Qin G Q and Long G L 2016 *Light: Science & Applications* **5** e16144

[34] Aigner M and Ziegler G M 2004 *Proofs From the Book* (Berlin: Springer) pp. 7–13

[35] Zhang K J, Zhang W W and Li D 2013 *Quantum Inf. Process.* **12** 2655

[36] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441