Quantum homomorphic aggregate signature based on quantum Fourier transform

Teng Chen
Qinghai Normal University
Dian-Jun Lu
ldj@qhnu.edu.cn

Qinghai Normal University
Zhi-Ming Deng
Qinghai Normal University
Wei-Xin Yao
University of California, Riverside

Research Article

Keywords: Quantum homomorphic aggregate signature, Quantum Fourier transform, Key generation matrix, Basis exchange operator

Posted Date: December 12th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3728263/v1

Additional Declarations: No competing interests reported.

Version of Record: A version of this preprint was published at Quantum Information Processing on March 28th, 2024. See the published version at https://doi.org/10.1007/s11128-024-04341-w.

Quantum homomorphic aggregate signature based on quantum Fourier transform

Teng Chen[1], Dian-Jun Lu[1,2*†], Zhi-Ming Deng[1†], Wei-Xin Yao[3†]

[1*]School of Mathematics and Statistics, Qinghai Normal University, Xining, 810008, China.

[2] School of Mathematics and Statistics, Shaanxi Normal University, Xi'an, 710119, China.

[3] Department of Statistics, University of California, Riverside, Riverside, 92521,California, America.

*Corresponding author(s). E-mail(s): ldj@qhnu.edu.cn;
Contributing authors: 3101900156@qq.com; 1194321025@qq.com; weixin.yao@ucr.edu;
†These authors contributed equally to this work.

Abstract

With the rapid development of computer and internet technology, quantum signature plays an extremely important role in modern secure communication. Quantum homomorphic aggregate signature, as an important guarantee of quantum signature, plays a significant role in reducing storage, communication, and computing costs. This article draws on the idea of quantum multi-party summation and proposes a quantum homomorphic aggregate signature scheme based on quantum Fourier transform. Our scheme uses $\boldsymbol{n}$-particle entangled states as quantum channels, with different particles of each entangled state sent separately. This ensures secure transmission of signatures and messages with fewer entangled particles during transmission, further improving the efficiency of quantum signatures. Meanwhile, our scheme generates private keys for each participating party by randomly constructing key generation matrixes. Different signers perform quantum Fourier transforms and basis exchange operations on entangled particles based on different messages and private keys to generate signatures. In addition, the aggregator does not need to measure and verify the signature particles after receiving signatures from different signers, and the group addition operation process has additive homomorphism. Security analysis shows that our scheme has unforgeability, non-repudiation, and can resist various attacks

such as entanglement measurement attacks, intercept-resend attacks, private key sequence attacks, and internal attacks by aggregator.

Keywords: Quantum homomorphic aggregate signature, Quantum Fourier transform, Key generation matrix, Basis exchange operator

1 Introduction

With the advancement of communication technology and the development of quantum computing theory, traditional encryption algorithms based on computational complexity have faced severe challenges. Quantum cryptography [1, 2] is a cryptographic technique that utilizes quantum mechanic to generate keys and ensure secure information transmission. It ensures secure communication between legitimate users and effectively solves the challenges of classical cryptography, truly achieving unconditional security. In 1984, Bennett and Brassard [3] proposed the famous concept of quantum key distribution, which marked the true beginning of quantum cryptography. Subsequently, due to its ability to resist quantum attacks in information protection and secure communication, quantum cryptography has attracted high attention and achieved rapid development. In recent years, multiple branches of quantum cryptography have been extensively studied, such as quantum secret sharing (QSS) [4, 5], quantum signature (QS) [6–8], quantum key distribution (QKD) [9, 10], quantum secure direct communication (QSDS) [11, 12],and so on.

With the rapid development of internet technology, information security has become a demand for people to keep confidential communication, and information security protection has become a focus of international attention. Digital signature, as an important guarantee of information security, is widely used in fields such as military, communication, e-commerce, and e-government due to its ability to achieve network identity authentication, data integrity protection, and non repudiation services. However, classical digital signature is not unconditionally secure, so QS has been proposed based on the special properties of quantum. QS is a new type of signature system that combines quantum cryptography and digital signature technology, utilizing the physical properties of quantum to achieve unconditional communication security. In 2001, Gottesman and Chuang [13] first proposed the concept of quantum signature based on quantum one-way function. This protocol utilizes the fundamental principles of quantum physics and employs quantum swap test to verify signature. Subsequently, in order to achieve different goals, researchers conducted in-depth research on QS and successively proposed many QS schemes with unconditional security. In 2002, Zeng et al. [14] proposed an arbitrated quantum signature (AQS) scheme using the entanglement properties of Greenberger-Horne-Zeilinger (GHZ) state. This scheme securely transmits messages through quantum channels and provides a detailed explanation of the general principles of QS scheme, clearly stating that the verification of AQS also requires the assistance of arbitrator. In 2009, Li et al. [15] proposed an AQS scheme using Bell states instead of GHZ states based on Zeng's scheme [14]. This scheme can be applied to both known and unknown quantum states. And while retaining the

advantages of the original scheme, it reduces the complexity of the implementation and improves the efficiency of the scheme. In 2010, Zou et al. [16] found that Zeng's scheme [14] and Li's scheme [15] were easily denied by recipients in terms of security. To overcome this drawback, they proposed an AQS scheme using bulletin boards. This scheme not only avoids being denied by the receiver, but also retains the advantages of the original scheme. In addition, Zou et al. [16] also found that existing AQS schemes rely on entanglement, and proposed a non entangled AQS scheme, which reduces the complexity of scheme implementation and improves the efficiency of the scheme. In the above AQS schemes, in order to improve the security of the scheme, trusted third parties need to know the specific content of the message, so most AQS schemes require the arbitrator to be trustworthy. Based on the above discussion, Yang et al. [17] proposed an AQS scheme using an untrusted arbitrator in 2011, drawing on the idea of quantum multi-party computing. This scheme is based on the signature of classical messages and proves the necessity and feasibility of messages signing under the control of an untrusted arbitrator. In 2013, Zou et al. [18] discovered that Yang's scheme [17] was insecure and conducted security analysis and improvement, proposing an improved AQS scheme with untrusted arbitrators. This scheme effectively solves the problem in Yang's scheme [17] where dishonest signers can deny their signatures and verifiers can forge signatures. In 2018, Zhang et al. [19] proposed an improved quantum proxy blind signature scheme, which introduces a trusted third party and uses a six-qubit entangled state to enhance the security of the scheme, making it impossible for the receiver or attacker to forge or modify messages in any way. At the same time, this scheme adopts GHZ state measurement and Bell state measurement, which is easier to implement under existing technology and experimental conditions. In 2019, Jiang et al. [20] proposed a quantum multi-signature scheme based on locally indistinguishable orthogonal product states. This scheme encodes the message into a quantum sequence of orthogonal product states, which can resist known message attacks. And because orthogonal product states are easier to prepare than entangled states, they are easier to implement under current technological conditions. In 2021, He et al. [21] studied the security of Jiang's quantum multi signature scheme [20] and found that Jiang's scheme [20] suffers from signature forgery attacks and signature receiver denial attacks. Based on the above issues, He et al. [21] proposed an improved quantum multi-signature scheme. This scheme addresses the security flaws of Jiang's scheme [20], and since the arbitrator cannot forge any quantum signature of the signer, the arbitrator is semi trustworthy. In 2022, Lu et al. [22] proposed a verifiable AQS scheme based on controlled quantum teleportation using a five-qubit entangled state as a quantum channel. This scheme utilizes a pair of function values of symmetric binary polynomials to perform unitary operations on mutually unbiased basis particles, which prevents any illegal attackers from forging and enables eavesdropping detection and identity authentication among participants. In 2021, Gao et al. [23] proposed a novel quantum (t, n) threshold signature scheme based on d-dimensional quantum systems. This scheme utilizes the cyclic property of mutually unbiased bases to generate effective signatures, and designs a new method to prevent known signature attacks. This method can also be used in other AQS schemes. In 2022, Huang et al. [24] proposed an improved identity based public key quantum signature scheme. In this scheme, the

signer uses her key and the verifier's secret parameter to generate a quantum signature, and the signer and verifier do not need to exchange keys before signing the message, making the scheme highly efficient. In 2023, Deng et al. [25] proposed a quantum (t, m, n) threshold group blind signature scheme with flexible number of participants. In this scheme, any m signers can use the *shamir* threshold secret sharing scheme to reconstruct the key for signature verification, and due to the XOR operation in the blinding process, the scheme is easier to implement in real scenarios.

Quantum Fourier Transform (QFT) is a crucial step in quantum factorization and many quantum algorithms. Using QFT to encrypt messages ensures secure transmission of messages over the channel. In 2019, Lou et al. [26] proposed a quantum blind signature scheme based on block encryption and QFT. This scheme uses a high-dimensional quantum carrier to transmit measurement information encrypted by QFT and permutation algorithms, which can not only resist general forgery attacks but also effectively prevent selective forgery attacks. In 2020, Lou et al. [27] proposed an ordered quantum multi-party signature scheme based on QFT and chaotic systems. In this scheme, the message sender uses QFT encryption and sends the message. Compared with AQS and quantum broadcast multi-party signature, this quantum multi-party signature scheme improves verification efficiency. In 2021, Zhu et al. [28] proposed an efficient quantum blind signature scheme based on QFT. This scheme uses quantum logic gates to manipulate quantum states containing classical information, and uses QFT encryption to transmit them through N-dimensional quantum states. Compared with existing efficiency analysis schemes, this scheme has higher signature efficiency. In 2022, Fan et al. [29] proposed a multi-proxy signature scheme based on controlled quantum teleportation using a five-qubit entangled state. This scheme uses QFT to encrypt quantum states containing messages, which improves quantum efficiency compared to quantum one-time pad. With the continuous deepening of research, many special digital signatures suitable for different usage environments have emerged, such as homomorphic signature, aggregate signature, and digital signature under certificate free systems.

Homomorphic signature [30, 31] is a digital signature with homomorphic properties. In 2000, Rivest [32] first proposed the concept of homomorphic signature. Subsequently, Johnson et al. [33] provided the overall framework and formal definition of homomorphic signature. Suppose M is the message space of a digital signature and Σ is the signature space of a digital signature, their binary operators are $\oplus$ and $\otimes$, respectively. For message signature pairs (m_1,σ_1) and (m_2,σ_2) from M and Σ, where $\sigma_1 = f(m_1)$ and $\sigma_2 = f(m_2)$, if the signature algorithm f is a homomorphic mapping from an algebraic system $(M, \oplus)$ to $(\Sigma, \otimes)$, then $f(m_1 \oplus m_2) = f(m_1) \otimes f(m_2) = \sigma_1 \otimes \sigma_2$. It can be seen that in the same message space M, digital signature can be generated through homomorphic combination algorithms. However, classical homomorphic signature is not suitable for quantum networks, and it is not easy to apply classical networks for identity authentication of different messages. Therefore, studying quantum homomorphic signature is imperative. In 2015, Shang et al. [34] proposed the first quantum homomorphic signature scheme based on entanglement swapping, which combines two initial signatures to generate a new quantum homomorphic signature through entanglement swapping. In

2016, Luo et al. [35] proposed a quantum homomorphic signature scheme based on Bell state measurement. This scheme only uses Bell state measurement, which is easy to implement under existing technical conditions, and is safer and more practical compared to Shang's scheme [34]. In 2023, Chen et al. [36] proposed a verifiable identity based quantum homomorphic signature scheme based on four-particle Cluster states. This scheme uses a four-particle Cluster state as a quantum channel, and verifies the identity of the signer through quantum measurement technology, while ensuring the security of the key and the unforgeability of the signature while satisfying the additive homomorphic property. The quantum homomorphic signatures introduced above only satisfy the properties of additive homomorphism and fail to fully consider cost reduction and resource allocation. Based on the above analysis, we attempt to combine quantum homomorphic signature with quantum aggregate signature to explore quantum homomorphic aggregate signature scheme with homomorphism.

Aggregated signature [37, 38] can compress signatures from different signers and messages into a single digital signature, thereby reducing the communication transmission cost of signatures. In 2003, Boneh et al. [39] first proposed the concept of aggregate signature with the aim of improving the efficiency of verifying a large number of individual signatures. Aggregated signature is different from homomorphic signature. Aggregated signature consists of three types of entities: signers($Alice_1$,$Alice_2$,...,$Alice_n$), aggregator of signatures (Bob), and verifier of signatures ($Charlie$). After receiving signatures from ($Alice_1$,$Alice_2$,...,$Alice_n$), aggregator (Bob) use aggregation algorithms to generate aggregated signature. Subsequently, the aggregator (Bob) sends the aggregated signature to the verifier ($Charlie$) for signature verification. If the aggregated signature is valid, it can be determined that the single signature generated respectively by the signers ($Alice_1$,$Alice_2$,...,$Alice_n$) is valid. However, due to the continuous improvement of people's computing power, the security based on classical digital signature schemes is facing unprecedented challenges. Therefore, many researchers have shifted their research on aggregate signature to the study of quantum aggregate signature. In 2022, You et al. [40] proposed a quantum aggregate signature scheme based on controlled quantum teleportation using a four-qubit Cluster state, which cannot be denied by the signer or forged by any illegal attacker. Meanwhile, intercept-resend attacks is ineffective in this scheme. The digital signatures introduced above have both the functions of ordinary signatures and their unique characteristics. If they are combined and flexibly used, they can achieve twice the result with half the effort in cloud computing environments.

This paper proposes a quantum homomorphic aggregate signature scheme that satisfies additive homomorphic properties, starting from quantum homomorphic signature and quantum aggregate signature. This scheme first generates a signature by using QFT and basis exchange operator on entangled particles from different signers based on different messages. Then, the aggregator aggregates the signature particles received from different signers to form one signature. Due to the addition homomorphism during aggregation operations, the quantum signature generated by aggregation is called a quantum homomorphic aggregate signature. Finally, the aggregator encrypts the quantum signature with a private key and sends it to the verifier for final signature verification. Compared with other similar signature schemes, our scheme's main contributions are as follows:

(1) After receiving signature particles from different signers, the aggregator uses group addition operations to aggregate multiple signatures into one signature. This process does not require measurement and verification of signature particles, and the group addition operation has additive homomorphism.

(2) By using key generation matrixes to generate private keys for each participant, and using quantum algorithms such as QFT and basis exchange operations, the scheme has unforgeability and non-repudiation. At the same time, it can resist various attacks such as entanglement measurement attacks, intercept-resend attacks, private key sequence attacks, and internal attacks by aggregator.

(3) The security of the scheme is improved by randomly generating key generation matrixes, and the secure transmission of signatures and messages is ensured with fewer entangled particles, which makes the signature scheme highly efficient.

The remaining structure of this article is as follows. Section 2 introduces concepts such as key generation matrix, quantum Fourier transform, SUM gate, and group addition operation. Section 3 introduces the detailed process of the proposed quantum homomorphic aggregate signature. In Section 4, we will provide a specific example in comparison to this scheme. Section 5 provides an analysis of the correctness and homomorphism of the scheme. Section 6 provides a security analysis of the scheme. Section 7 conducts an efficiency analysis. Section 8 provides a brief conclusion.

2 Preliminary

2.1 Key generation matrix

The key generation matrix is used to generate private keys for multiple participants, and then encrypt information using the private keys to ensure the secure transmission of information for each participant. The key generation matrix is an $n \times n$ square matrix [41], which is represented as

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}. \tag{1}$$

Where $a_{it}(a_{it} \in \{1, 2, 3, ...\})$ represents the element in the ith row tth column of the key generation matrix, and the sum modulus $d(d = 2^n)$ of each row is 0, which means $\sum_{t=1}^{n} a_{it}(mod\, d) = 0$.

2.2 Quantum Fourier transform

QFT is a key step in quantum factor decomposition and many quantum algorithms, and is an effective quantum algorithm for performing Fourier transform of quantum mechanical amplitudes [42]. This article uses QFT to encrypt information in order to ensure secure transmission of information in the channel. In a d-dimensional quantum

system, for $x \in \{0, 1, ..., d-1\}$, QFT is defined as follows:

$$QFT : |x\rangle \to \frac{1}{\sqrt{d}} \sum_{y=0}^{d-1} e^{2\pi i \frac{x}{d} y} |y\rangle. \tag{2}$$

Meanwhile, inverse QFT is defined as:

$$QFT^{-1} : |y\rangle \to \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} e^{-2\pi i \frac{y}{d} x} |x\rangle. \tag{3}$$

In addition, due to the

$$\sum_{y=0}^{d-1} e^{2\pi i \frac{x}{d} y} = \begin{cases} 0, & if x \neq 0 \, mod \, d \\ d, & if x = 0 \, mod \, d \end{cases}, \tag{4}$$

so there is $QFT^{-1}(QFT|x\rangle) = |x\rangle$.

2.3 SUM gate

The definition of a SUM gate is as follows:

$$SUM(|u\rangle, |v\rangle) = (|u\rangle, |u + v(mod \, d)\rangle), \tag{5}$$

where $|u\rangle$ and $|v\rangle$ are the control bit and target bit respectively, and $u, v \in \{0, 1, ..., d-1\} (d = 2^n)$.
Let's assume that the binary expressions for u and v are $u = u_0 \cdot 2^0 + u_1 \cdot 2^1 + u_2 \cdot 2^2 + \cdots + u_{n-1} \cdot 2^{n-1}$ and $v = v_0 \cdot 2^0 + v_1 \cdot 2^1 + v_2 \cdot 2^2 + \cdots + v_{n-1} \cdot 2^{n-1}$ respectively, where $u_j, v_j \in \{0, 1\}, (j = 0, 1, 2, ..., n-1)$. Therefore, the operations of SUM gate can be transformed into operations between the binary of u and v. As shown in Figure 1, a quantum circuit diagram for SUM gate binary operations is presented.

2.4 Basis exchange operator

In d-dimensional quantum systems, the basis exchange operator U_k is defined as:

$$U_k = \sum_{u=0}^{d-1} |u + k\rangle\langle u|, \tag{6}$$

where $k \in \{0, 1, ..., d-1\}$. Obviously, for a d-dimensional ground state $|e\rangle (e \in \{0, 1, ..., d-1\})$, the result of being acted upon by operator U_k is

$$U_k|e\rangle = |e + k(mod \, d)\rangle. \tag{7}$$

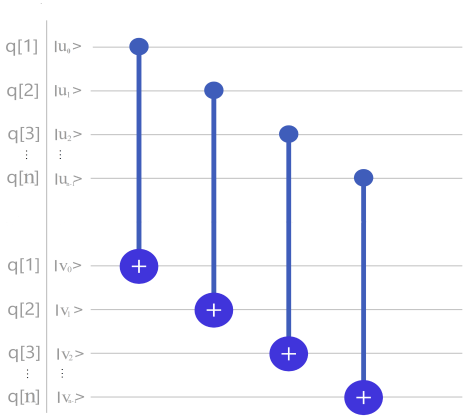

Fig. 1 Quantum circuit diagram of SUM gate binary operations

2.5 Group addition operation

In this article, we need to use the group addition operator Θ to aggregate multiple initial signatures to generate a quantum homomorphic aggregate signature with homomorphic properties. Its definition is as follows:

Definition 1 (Group addition operation)**.** *Firstly, the addition operation of module d on the set $\{0,1,2,...,d-1\}$ forms a group that satisfies the properties of associative law, identity element, and inverse element. Then, we define a mapping from set $\{0,1,2,...,d-1\}$ to set $\{|0\rangle,|1\rangle,...,|d-1\rangle\}$, with a mapping function δ satisfying $\delta(0)=|0\rangle,\delta(1)=|1\rangle,...,\delta(d-1)=|d-1\rangle$. Based on this mapping function δ, there is $\delta(x)\Theta\delta(y)=\delta((x+y)mod\, d)$ for $\forall x,y\in\{0,1,2,...,d-1\}$, where the symbol Θ is the group addition operator on the set $\{|0\rangle,|1\rangle,...,|d-1\rangle\}$, and the operation of the symbol Θ on the set $\{|0\rangle,|1\rangle,...,|d-1\rangle\}$ forms an addition group. Suppose $d=4$, the operations between the elements in the group are shown in Table1.*

Table 1 The operation situation between each element

Θ	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$
$\|1\rangle$	$\|1\rangle$	$\|2\rangle$	$\|3\rangle$	$\|0\rangle$
$\|2\rangle$	$\|2\rangle$	$\|3\rangle$	$\|0\rangle$	$\|1\rangle$
$\|3\rangle$	$\|3\rangle$	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$

3 The proposed scheme

This scheme needs to involve $n+2$ participants in total. They are respectively: $Alice_i(i=1,2,...,n)$ are the initial signers of messages, *Bob* is the aggregator of the initial signatures, *Charlie* is the verifier of homomorphic aggregate signature. The

scheme consists of four stages, namely: initialization phase, signature phase, aggregation phase, and verification phase. The specific details of the scheme are described as follows:

3.1 Initialization phase

Suppose there are n initial signers $Alice_i(i = 1, 2, ..., n)$ who each need to sign messages $X_i \in \{0,1\}^n$. $Alice_i(i = 1, 2, ..., n)$ and $Charlie$ share a key K_{A_iC} with a length of n bits respectively. To ensure unconditional security, the distribution of these keys can be completed through QKD [43]. In this stage, the initial signers, aggregator, and verifier generate their own private keys through the key generation matrixes. Then Bob generates entangled particles through quantum operations such as QFT, and distributes the entangled particles to the initial signers.

Step I1. the initial signers $Alice_i(i = 1, 2, ..., n)$, aggregator Bob, and verifier $Charlie$ jointly construct n $n+2$-order key generation matrixes, which can be referred to as $\{B^0, B^1, ..., B^{n-1}\}$. Taking the key generation matrix $B^j(j = 0, 1, 2, ..., n-1)$ as an example, we will construct and explain the matrix. Firstly, each participant constructs a row of the key generation matrix B^j, which means that $Alice_i$ constructs the ith row element of the key generation matrix B^j, Bob generates the $(n+1)$th row element of the key generation matrix B^j, and $Charlie$ generates the $(n+2)$th row element of the key generation matrix B^j. Then, $Alice_i$ randomly generates $n+2$ positive integers $\{a^j_{i1}, a^j_{i2}, ..., a^j_{in}, b^j_i, c^j_i\}$ as the ith$(1 \le i \le n)$ row element of the key generation matrix B^j, where the ith row element satisfies $\sum_{t=1}^{n} a^j_{it} + b^j_i + c^j_i = 0(mod\, d)$, a^j_{it} represents the ith row tth column element in matrix B^j, b^j_i represents the ith row $(n+1)$th column element in matrix B^j, and c^j_i represents the ith row $(n+2)$th column element in matrix B^j. Bob randomly generates $n+2$ positive integers $\{a^j_{(n+1)1}, a^j_{(n+1)2}, ..., a^j_{(n+1)n}, b^j_{n+1}, c^j_{n+1}\}$ as the $(n+1)$th row element of the key generation matrix B^j, where the $(n+1)$th row element satisfies $\sum_{t=1}^{n} a^j_{(n+1)t} + b^j_{n+1} + c^j_{n+1} = 0(mod\, d)$, $a^j_{(n+1)t}$ represents the $(n+1)$th row tth column element in matrix B^j, b^j_{n+1} represents the $(n+1)$th row $(n+1)$th column element in matrix B^j, and c^j_{n+1} represents the $(n+1)$th row $(n+2)$th column element in matrix B^j. Next, $Charlie$ randomly generates $n+2$ positive integers $\{a^j_{(n+2)1}, a^j_{(n+2)2}, ..., a^j_{(n+2)n}, b^j_{n+2}, c^j_{n+2}\}$ as the $(n+2)$th row element of the key generation matrix B^j, where the $(n+2)$th row element satisfies $\sum_{t=1}^{n} a^j_{(n+2)t} + b^j_{n+2} + c^j_{n+2} = 0(mod\, d)$, $a^j_{(n+2)t}$ represents the $(n+2)$th row tth column element in matrix B^j, b^j_{n+2} represents the $(n+2)$th row $(n+1)$th column element in matrix B^j, and c^j_{n+2} represents the $(n+2)$th row $(n+2)$th column element in matrix B^j. Subsequently, $Alice_i$ publicly discloses elements other than a^j_{ii} from the ith$(1 \le i \le n)$ row element $\{a^j_{i1}, a^j_{i2}, ..., a^j_{in}, b^j_i, c^j_i\}$ of the matrix B^j she generates to other participants, while retaining the element a^j_{ii} herself. Bob publicly exposes elements other than b^j_{n+1} from the $(n+1)$th row element

$\{a^j_{(n+1)1}, a^j_{(n+1)2}, ..., a^j_{(n+1)n}, b^j_{n+1}, c^j_{n+1}\}$ of the matrix B^j he generates to other participants, while retaining element b^j_{n+1} himself. *Charlie* publicly exposes elements other than c^j_{n+2} from the $(n+2)$th row element $\{a^j_{(n+2)1}, a^j_{(n+2)2}, ..., a^j_{(n+2)n}, b^j_{n+2}, c^j_{n+2}\}$ of the matrix B^j he generates to other participants, while retaining element c^j_{n+2} himself. At this point, after receiving the element $\{a^j_{1i}, a^j_{2i}, ..., a^j_{(i-1)i}, a^j_{(i+1)i}, ..., a^j_{(n+2)i}\}$ publicly disclosed by other participants, $Alice_i$ sets a^j_i as the sum of all elements in the ith column of the key generation matrix B^j, i.e. $a^j_i = \sum_{z=1}^{n+2} a^j_{zi}$, so that $Alice'_i s$ private key in the key generation matrix B^j is a^j_i. Combining matrix sequences $\{B^0, B^1, ..., B^{n-1}\}$, $Alice_i$ has a private key sequence $k_{A_i} = (a^0_i, a^1_i, ..., a^{n-1}_i)$. After receiving the element $\{b^j_1, b^j_2, ..., b^j_n, b^j_{(n+2)}\}$ publicly disclosed by other participants, *Bob* sets b^j as the sum of all elements in the $(n+1)$th column of the key generation matrix B^j, i.e. $b^j = \sum_{z=1}^{n+2} b^j_z$, so that $Bob's$ private key in the key generation matrix B^j is b^j . Combining matrix sequences $\{B^0, B^1, ..., B^{n-1}\}$, *Bob* has a private key sequence $k_B = (b^0, b^1, ..., b^{n-1})$. After receiving the element $\{c^j_1, c^j_2, ..., c^j_{n+1}\}$ publicly disclosed by other participants, *Charlie* sets c^j as the sum of all elements in the $(n+2)$th column of the key generation matrix B^j, i.e. $c^j = \sum_{z=1}^{n+2} c^j_z$, so that $Charlie's$ private key in the key generation matrix B^j is c^j . Combining matrix sequences $\{B^0, B^1, ..., B^{n-1}\}$, *Charlie* has a private key sequence $k_C = (c^0, c^1, ..., c^{n-1})$. It is obvious that $\sum_{i=1}^{n} a^j_i + b^j + c^j = 0 (mod\, d)$. Finally, $Alice_i (i = 1, 2, ..., n)$ respectively encrypts the message $X_i (i = 1, 2, ..., n)$ with the key $K_{A_i C}$ to obtain $E_{k_{A_i C}}(X_i)$, which is then sent to *Charlie* via a classical channel. The schematic diagram of the key generation matrix B^j is shown in Figure 2. The process of generating the key generation matrix B^j is shown in Figure 3.

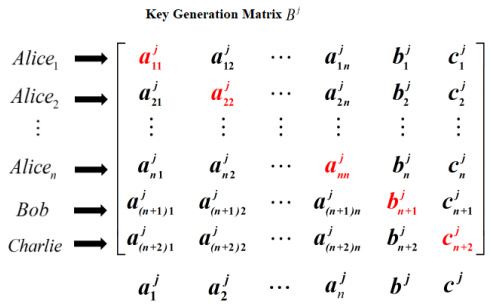

Fig. 2 The representation of key generation matrix B^j

Step I2. At this stage, aggregator *Bob* generates n entangled n-particle states, denoted as $\{|w\rangle^0, |w\rangle^1, ..., |w\rangle^{n-1}\}$, by using QFT and SUM gate. Next, take the preparation of $|w\rangle^j (j = 0, 1, 2, ..., n-1)$ as an example for explanation. Firstly, *Bob* prepares n single particle states $\{|0\rangle_1, |0\rangle_2, ..., |0\rangle_n\}$ and applies QFT to the first particle $|0\rangle_1$,

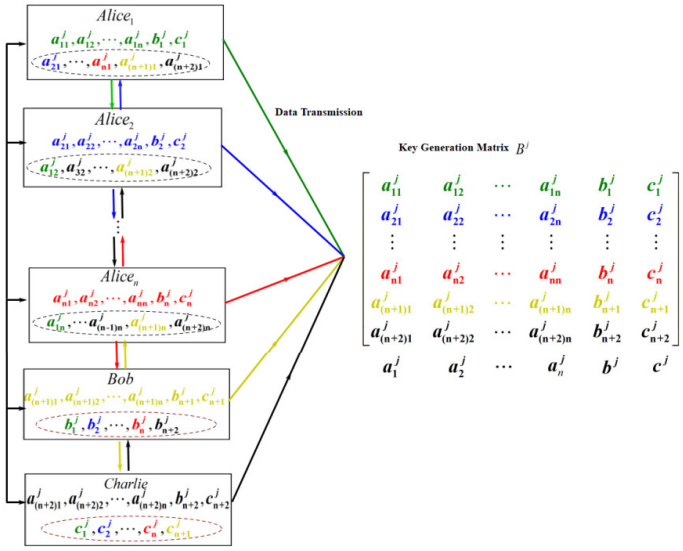

Fig. 3 The generation process of key generation matrix B^j

resulting in $|\phi\rangle = QFT|0\rangle_1 = \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}|p\rangle_1$. Then, *Bob* uses $n-1$ SUM gate operations to generate an n-particle entangled state $|w\rangle^j$, where $|\phi\rangle$ is the control bit and $|0\rangle_m (m = 2, 3, ..., n)$ is the target bit. Thus, there is $|w\rangle^j = \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}|p\rangle_1^j|p\rangle_2^j\cdots|p\rangle_n^j$, where $|p\rangle_i^j$ represents the ith particle in the entangled state of the jth particle.

Step I3. *Bob* generates n entangled n-particle states in the Step I2, with the order represented as

$$\left(\frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}|p\rangle_1^0|p\rangle_2^0\cdots|p\rangle_n^0, \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}|p\rangle_1^1|p\rangle_2^1\cdots|p\rangle_n^1, \cdots, \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}|p\rangle_1^{n-1}|p\rangle_2^{n-1}\cdots|p\rangle_n^{n-1}\right). \tag{8}$$

Then *Bob* extracts the ith particle from each n-particle entangled state to construct a sequence containing n particles, thus generating n n-particle sequences and sending the ith n-particle sequence directly to $Alice_i$ through quantum secure communication [44]. Therefore, the particle sequence obtained by each initial signer $Alice_i (i = 1, 2, ..., n)$ is $(|p\rangle_i^0, |p\rangle_i^1, ..., |p\rangle_i^{n-1})$, where $|p\rangle_i^j$ represents the ith particle in the jth entangled state. The schematic diagram of particles distribution is shown in Figure 4.

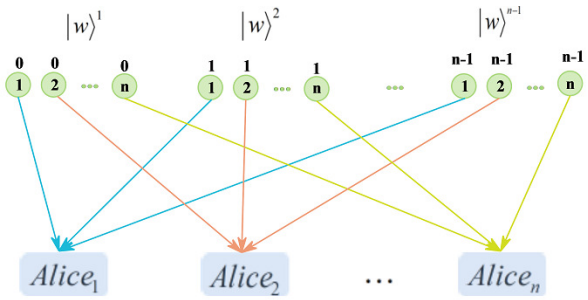

Fig. 4 Particles distribution diagram

3.2 Signature phase

After receiving a particle sequence $(|p\rangle_i^0, |p\rangle_i^1, ..., |p\rangle_i^{n-1})$ from *Bob*, $Alice_i (i = 1, 2, ..., n)$ perform QFT and basis exchange operations on the received particles based on their own private keys $k_{A_i} = (a_i^0, a_i^1, ..., a_i^{n-1})$ and $X_i \in \{0, 1\}^n$ to generate signatures. Then $Alice_i (i = 1, 2, ..., n)$ send the computed particle sequences to *Bob*. This stage is completed in two steps, as shown below.

Step S1. The initial signers $Alice_i (i = 1, 2, ..., n)$ respectively perform $U_{r_i^j + a_i^j} QFT$ operations on the particles they own, and the $r_i^j + a_i^j$ in $U_{r_i^j + a_i^j}$ corresponding to different messages X_i are different. The corresponding rule is: if the jth$(j = 0, 1, ..., n-1)$ bit of the binary bits of message X_i is 1, then the parameter $r_i^j = 1$ in $U_{r_i^j + a_i^j}$ acting on the jth particle; If the jth$(j = 0, 1, ..., n-1)$ bit of the binary bits of message X_i is 0, then the parameter $r_i^j = 0$ in $U_{r_i^j + a_i^j}$ acting on the jth particle.

Next, the entangled state $|w\rangle^j$ prepared by *Bob* will be used as an example to illustrate, where n particles contained in the entangled state $|w\rangle^j$ are respectively sent to n initial signers $Alice_i (i = 1, 2, ..., n)$. Each initial signer $Alice_i$ performs corresponding operations based on the corresponding rules mentioned above. Suppose that the entangled state $|w\rangle^j$ is subjected to $U_{r_i^j + a_i^j} QFT$ operations, the result of the operations is denoted as $|R\rangle^j$. The calculation process is as follows:

$$
\begin{aligned}
|R\rangle^j &= (U_{r_1^j+a_1^j}QFT)\otimes(U_{r_2^j+a_2^j}QFT)\otimes\cdots\otimes(U_{r_n^j+a_n^j}QFT)|w\rangle^j \\
&= \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}(U_{r_1^j+a_1^j}QFT)|p\rangle_1^j\otimes(U_{r_2^j+a_2^j}QFT)|p\rangle_2^j\otimes\cdots\otimes(U_{r_n^j+a_n^j}QFT)|p\rangle_n^j \\
&= \frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}\left(\frac{1}{\sqrt{d}}\sum_{l_1^j=0}^{d-1}e^{2\pi i\frac{p}{d}l_1^j}|l_1^j+r_1^j+a_1^j\rangle\right)\otimes\left(\frac{1}{\sqrt{d}}\sum_{l_2^j=0}^{d-1}e^{2\pi i\frac{p}{d}l_2^j}|l_2^j+r_2^j+a_2^j\rangle\right) \\
&\quad\otimes\cdots\otimes\left(\frac{1}{\sqrt{d}}\sum_{l_n^j=0}^{d-1}e^{2\pi i\frac{p}{d}l_n^j}|l_n^j+r_n^j+a_n^j\rangle\right) \\
&= d^{-\frac{n+1}{2}}\sum_{p=0}^{d-1}\left(\sum_{l_1^j,l_2^j,\cdots,l_n^j=0}^{d-1}e^{2\pi i\frac{l_1^j+l_2^j+\cdots+l_n^j}{d}p}|l_1^j+r_1^j+a_1^j\rangle\otimes\cdots\otimes|l_n^j+r_n^j+a_n^j\rangle\right) \\
&= d^{-\frac{n+1}{2}}\sum_{l_1^j,l_2^j,\cdots,l_n^j=0}^{d-1}\left(\sum_{p=0}^{d-1}e^{2\pi i\frac{l_1^j+l_2^j+\cdots+l_n^j}{d}p}|l_1^j+r_1^j+a_1^j\rangle\otimes\cdots\otimes|l_n^j+r_n^j+a_n^j\rangle\right).
\end{aligned}
\tag{9}
$$

Combining the property of QFT

$$
\sum_{p=0}^{d-1}e^{2\pi i\frac{l_1^j+l_2^j+\cdots+l_n^j}{d}p}=\begin{cases}0, & l_1^j+l_2^j+\cdots+l_n^j\neq 0\,mod\,d\\ d, & l_1^j+l_2^j+\cdots+l_n^j=0\,mod\,d\end{cases},
\tag{10}
$$

So there is

$$
|R\rangle^j = d^{-\frac{n-1}{2}}\sum_{l_1^j+l_2^j+\cdots+l_n^j=0\,mod\,d}|l_1^j+r_1^j+a_1^j\rangle\otimes|l_2^j+r_2^j+a_2^j\rangle\otimes\cdots\otimes|l_n^j+r_n^j+a_n^j\rangle.
\tag{11}
$$

Based on the above calculation results, the signatures of $Alice_i(i=1,2,...,n)$ are shown in Table 2.

Table 2 Information signature pairs of initial signers

Initial signers	Information signature pairs of initial signers
$Alice_1$	$\{X_1, S_1=(\|l_1^0+r_1^0+a_1^0\rangle, \|l_1^1+r_1^1+a_1^1\rangle, ..., \|l_1^{n-1}+r_1^{n-1}+a_1^{n-1}\rangle)\}$
$Alice_2$	$\{X_2, S_2=(\|l_2^0+r_2^0+a_2^0\rangle, \|l_2^1+r_2^1+a_2^1\rangle, ..., \|l_2^{n-1}+r_2^{n-1}+a_2^{n-1}\rangle)\}$
$\vdots$	$\vdots$
$Alice_n$	$\{X_n, S_n=(\|l_n^0+r_n^0+a_n^0\rangle, \|l_n^1+r_n^1+a_n^1\rangle, ..., \|l_n^{n-1}+r_n^{n-1}+a_n^{n-1}\rangle)\}$

Step S2. After $Alice_i (i = 1, 2, ..., n)$ complete the signature, they need to return the signature particles to Bob. During the transmission process, eavesdropping detection will be used between $Alice_i$ and Bob to ensure the secure transmission of signatures. Taking $Alice_i$ as an example, the specific eavesdropping detection process is as follows.

$Alice_i$ randomly selects a set of decoy particles from the set $V_1 = \{|0\rangle, |1\rangle, ..., |d-1\rangle\}$ or $V_2 = \{QFT|0\rangle, QFT|1\rangle, ..., QFT|d-1\rangle\}$, and then inserts the decoy particles into the signature sequence S_i to form an ordered quantum sequence S_i', and records the position of each decoy particle. Afterwards, $Alice_i$ sends the quantum sequence S_i' to Bob, while informing him of the randomly selected decoy particles's positions and corresponding measurement basis.

After receiving S_i', Bob measures the corresponding particles using the same measurement basis as $Alice_i$. Then Bob sends the measurement results to $Alice_i$, who compares the measurement results between them. If the error rate is lower than the predetermined threshold for channel noise, proceed to the next step; Otherwise, $Alice_i$ tells Bob to abandon the sequence and start a new one. Finally, Bob removes the decoy particles from S_i' and obtains the quantum signature sequence S_i. The distribution and signature process of entangled particles is shown in Figure 5.

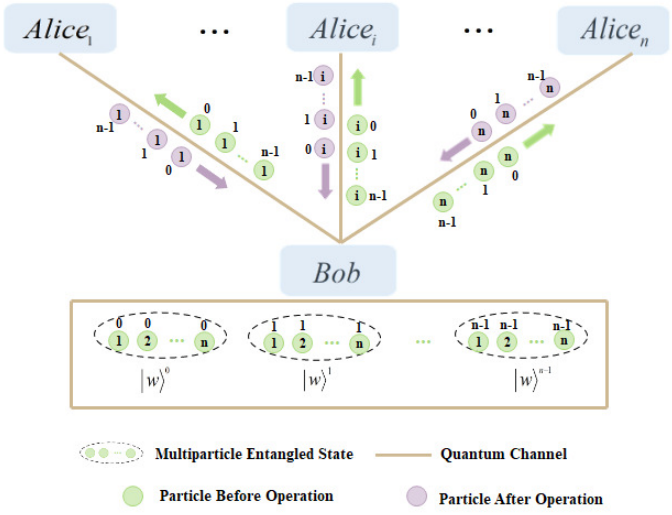

Fig. 5 Entangled particle distribution and signature process

3.3 Aggregation phase

In this stage, aggregator Bob first aggregates the quantum signatures among the initial signers $Alice_i (i = 1, 2, ..., n)$ using the group addition operator Θ to generate a new quantum homomorphic aggregate signature, which is Bob's quantum signature. Then, Bob encrypts the quantum homomorphic aggregate signature by combining his own private key with basis exchange operator. After encryption is completed, the

encrypted quantum sequence is sent to *Charlie* through a quantum channel. This stage is completed in two steps, and the specific process is as follows.

Step A1. In the Step S2 stage, it is possible to know the signature $S_i = (|l_i^0 + r_i^0 + a_i^0\rangle, |l_i^1 + r_i^1 + a_i^1\rangle, ..., |l_i^{n-1} + r_i^{n-1} + a_i^{n-1}\rangle)$ recovered by *Bob* from the inserted decoy particle's S_i'. In the preliminary section, a group addition operator Θ is defined that satisfies: $\delta(x)\Theta\delta(y) = \delta((x+y) mod\, d)$. *Bob* performs $(n-1)\Theta$ group addition operations on the $jth(j = 0, 1, 2, ..., n-1)$ particle from each of the n signature particles sent by $Alice_i(i = 1, 2, ..., n)$, thereby aggregating n sets of quantum sequences into one set of quantum sequence. Therefore, *Bob* can obtain $S = \{|(r_1^0 + r_2^0 + \cdots + r_n^0 + a_1^0 + \cdots + a_n^0) mod\, d\rangle, |(r_1^1 + r_2^1 + \cdots + r_n^1 + a_1^1 + \cdots + a_n^1) mod\, d\rangle, \cdots, |(r_1^{n-1} + r_2^{n-1} + \cdots + r_n^{n-1} + a_1^{n-1} + \cdots + a_n^{n-1}) mod\, d\rangle\}$, which is a quantum signature generated by *Bob* through Θ group addition operations, that is, a quantum homomorphic aggregate signature. The specific aggregation process is shown in Figure 6.

$$
\begin{array}{ccccccc}
S_1 = \{ & |l_1^0 + r_1^0 + a_1^0\rangle & , & |l_1^1 + r_1^1 + a_1^1\rangle & , & |l_1^2 + r_1^2 + a_1^2\rangle , \cdots , & |l_1^{n-1} + r_1^{n-1} + a_1^{n-1}\rangle \ \} \\
& \Theta & & \Theta & & \Theta & \Theta \\
S_2 = \{ & |l_2^0 + r_2^0 + a_2^0\rangle & , & |l_2^1 + r_2^1 + a_2^1\rangle & , & |l_2^2 + r_2^2 + a_2^2\rangle , \cdots , & |l_2^{n-1} + r_2^{n-1} + a_2^{n-1}\rangle \ \} \\
& \Theta & & \Theta & & \Theta & \Theta \\
& \vdots & & \vdots & & \vdots & \vdots \\
& \Theta & & \Theta & & \Theta & \Theta \\
S_n = \{ & |l_n^0 + r_n^0 + a_n^0\rangle & , & |l_n^1 + r_n^1 + a_n^1\rangle & , & |l_n^2 + r_n^2 + a_n^2\rangle , \cdots , & |l_n^{n-1} + r_n^{n-1} + a_n^{n-1}\rangle \ \} \\
& \| & & \| & & \| & \| \\
S = \Big\{ & \Big|\sum_{i=1}^{n}(r_i^0 + a_i^0) \bmod d\Big\rangle, & & \Big|\sum_{i=1}^{n}(r_i^1 + a_i^1) \bmod d\Big\rangle, & & \Big|\sum_{i=1}^{n}(r_i^2 + a_i^2) \bmod d\Big\rangle, \cdots , & \Big|\sum_{i=1}^{n}(r_i^{n-1} + a_i^{n-1}) \bmod d\Big\rangle \Big\}
\end{array}
$$

Fig. 6 The generation process of quantum homomorphic aggregate signature

Step A2. After *Bob* generates a quantum homomorphic aggregate signature through the Θ group addition operations, in order to ensure the secure transmission of the quantum homomorphic aggregate signature to *Charlie*, *Bob* uses the U_{b^j} operations to add his private key $k_B = (b^0, b^1, ..., b^{n-1})$ to the quantum homomorphic aggregate signature S, resulting in $U_{b^j}|r_1^j + r_2^j + \cdots + r_n^j + a_1^j + \cdots + a_n^j\rangle = |r_1^j + r_2^j + \cdots + r_n^j + a_1^j + \cdots + a_n^j + b^j\rangle$. Suppose the encrypted quantum sequence is S', there is $S' = \{|(r_1^0 + r_2^0 + \cdots + r_n^0 + a_1^0 + \cdots + a_n^0 + b^0) mod\, d\rangle, |(r_1^1 + r_2^1 + \cdots + r_n^1 + a_1^1 + \cdots + a_n^1 + b^1) mod\, d\rangle, ..., |(r_1^{n-1} + r_2^{n-1} + \cdots + r_n^{n-1} + a_1^{n-1} + \cdots + a_n^{n-1} + b^{n-1}) mod\, d\rangle\}$. Then, *Bob* sends the encrypted quantum sequence S' to *Charlie* through a quantum channel.

3.4 Verification phase

At this stage, *Charlie* will verify the validity of the initial signatures by verifying the validity of the quantum homomorphic aggregate signature. This stage is completed in two steps, and the specific process is as follows.

Step V1. After receiving the S' sent by *Bob*, *Charlie* also uses U_{c^j} operations to add his private key $k_C = (c^0, c^1, ..., c^{n-1})$ to the quantum sequence S', marking the

transformed quantum sequence as S''. Thus, there is $U_{c^j}|(r_1^j + r_2^j + \cdots + r_n^j + a_1^j + \cdots + a_n^j + b^j) mod\, d\rangle = |(r_1^j + r_2^j + \cdots + r_n^j + a_1^j + \cdots + a_n^j + b^j + c^j) mod\, d\rangle$. By combining the property of the key generation matrixes, i.e. $\sum_{i=1}^{n} a_i^j + b^j + c^j = 0 (mod\, d)$, the quantum sequence owned by *Charlie* is transformed into $S'' = \{|(r_1^0 + r_2^0 + \cdots + r_n^0) mod\, d\rangle, |(r_1^1 + r_2^1 + \cdots + r_n^1) mod\, d\rangle, \cdots, |(r_1^{n-1} + r_2^{n-1} + \cdots + r_n^{n-1}) mod\, d\rangle\}$.

Step V2. *Charlie* used a set of computational bases $\{|0\rangle, |1\rangle, ..., |n\rangle\}$ to measure the quantum sequence S'', and the measured results are $g^0 = r_1^0 + r_2^0 + \cdots + r_n^0, g^1 = r_1^1 + r_2^1 + \cdots + r_n^1, ..., g^{n-1} = r_1^{n-1} + r_2^{n-1} + \cdots + r_n^{n-1}$. Then *Charlie* calculates the sum of the messages $X_i (i = 1, 2, ..., n)$ converted to decimal based on the measurement results as $Sum' = g^0 \cdot 2^0 + g^1 \cdot 2^1 + g^2 \cdot 2^2 + \cdots + g^{n-1} \cdot 2^{n-1}$.

When *Charlie* receives the $E_{k_{A_i C}}(X_i)$ sent by $Alice_i (i = 1, 2, ..., n)$, he decrypts it using the key $K_{A_i C}$ to obtain $X_i (i = 1, 2, ..., n)$. Then *Charlie* converts X_i to decimal $x_i (i = 1, 2, ..., n)$ and calculates $Sum = x_1 + x_2 + \cdots + x_n$. Finally, *Charlie* compares and verifies Sum with Sum'. If $Sum = Sum'$ is met, the signature is valid; Otherwise, *Charlie* declares the signature invalid and refuses to accept it. For the above stages, the information exchange between the participants is shown in Figure 7. Here, we also present the quantum circuit diagram of the proposed scheme, as shown in Figure 8.

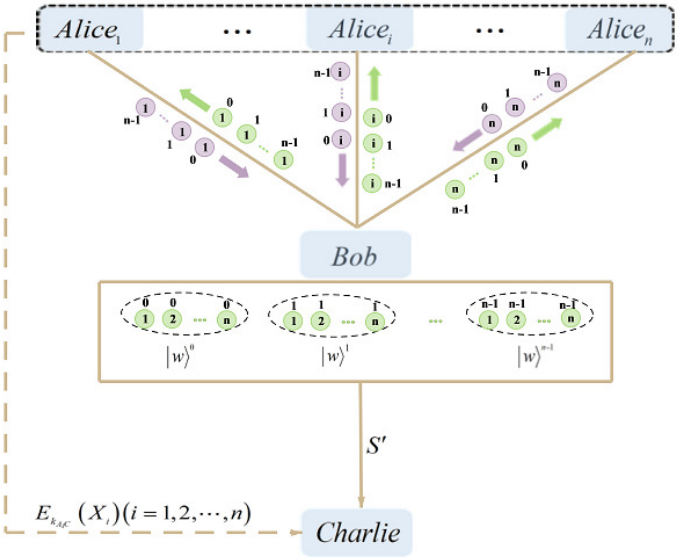

Fig. 7 Information exchange diagram

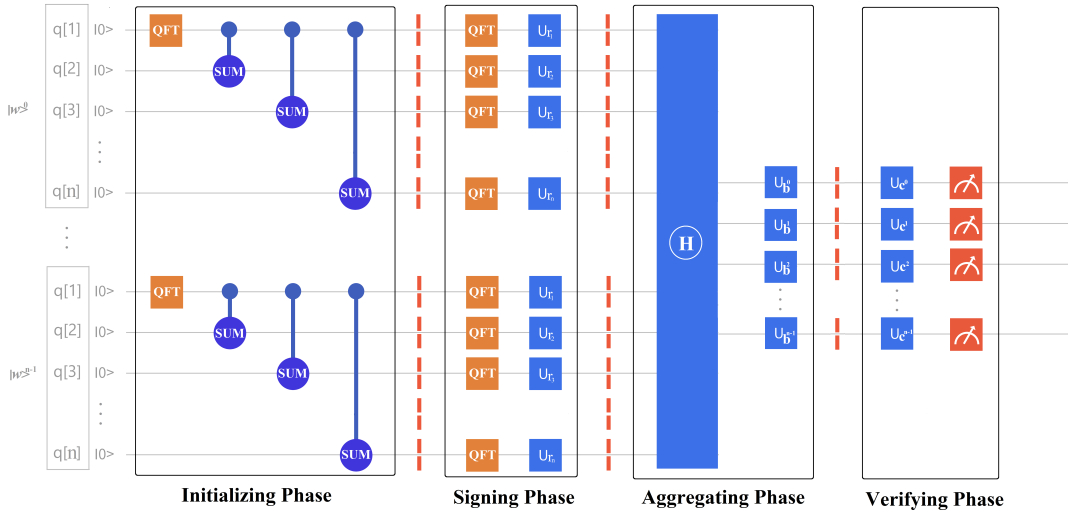

Fig. 8 Quantum circuit diagram of the proposed scheme

4 Example of scheme

In this section, we provide a example to describe the proposed scheme and verify its correctness. If $n+2$ participants can honestly execute the operations of the scheme, then their initial signatures generated by the messages and the quantum signature generated by aggregation using homomorphic properties are both valid. In the process of giving an example, we overlooked the corresponding security checks.

4.1 Initialization phase

Suppose there are six initial signers $Alice_1$, $Alice_2$, $Alice_3$, $Alice_4$,$Alice_5$ and $Alice_6$ who need to sign messages $X_1 = 101110$, $X_2 = 100100$, $X_3 = 000111$, $X_4 = 001110$, $X_5 = 011100$ and $X_6 = 111000$, there is $d = 2^6 = 64$.

Step I1. Firstly, $Alice_1$, $Alice_2$, $Alice_3$, $Alice_4$,$Alice_5$, $Alice_6$, Bob, $Charlie$ jointly construct six key generation matrixes, denoted as $\{B^0, B^1, ..., B^5\}$. For each key generation matrix $B^j (j = 0, 1, 2, ..., 5)$, each participant reconstructs one row of the key generation matrix. Next, we will describe the process of constructing the key generation matrix B^0. $Alice_1$, $Alice_2$, $Alice_3$, $Alice_4$,$Alice_5$, $Alice_6$, Bob, $Charlie$ randomly generate eight positive integers as elements of the key generation matrix B^0, and the positive integers generated by each participating party are shown in Table 3.

Table 3 Each participant generates the row elements of the key generation matrix B^0 separately

Participants	The row elements of B^0	Participants	The row elements of B^0
$Alice_1$	$7, 27, 20, 1, 3, 5, 43, 22$	$Alice_2$	$23, 13, 3, 25, 9, 6, 2, 47$
$Alice_3$	$5, 4, 3, 30, 3, 15, 17, 51$	$Alice_4$	$6, 17, 44, 6, 1, 9, 10, 35$
$Alice_5$	$24, 30, 14, 8, 1, 5, 36, 10$	$Alice_6$	$30, 17, 7, 4, 3, 5, 16, 46$
Bob	$61, 20, 6, 2, 2, 7, 23, 7$	$Charlie$	$57, 16, 18, 11, 2, 5, 4, 15$

Table 4 Private keys of each participant on matrix B^0

Participants	Private keys of participant
$Alice_1$	$a_1^0 = 7 + 23 + 5 + 6 + 24 + 30 + 61 + 57 = 213$
$Alice_2$	$a_2^0 = 27 + 13 + 4 + 17 + 30 + 17 + 20 + 16 = 144$
$Alice_3$	$a_3^0 = 20 + 3 + 3 + 44 + 14 + 7 + 6 + 18 = 115$
$Alice_4$	$a_4^0 = 1 + 25 + 30 + 6 + 8 + 4 + 2 + 11 = 87$
$Alice_5$	$a_5^0 = 3 + 9 + 3 + 1 + 1 + 3 + 2 + 2 = 24$
$Alice_6$	$a_6^0 = 5 + 6 + 15 + 9 + 5 + 5 + 7 + 5 = 57$
Bob	$b^0 = 43 + 2 + 17 + 10 + 36 + 16 + 23 + 4 = 151$
$Charlie$	$c^0 = 22 + 47 + 51 + 35 + 10 + 46 + 7 + 15 = 233$

Therefore, the B^0 matrix is represented as

$$\begin{bmatrix} 7 & 27 & 20 & 1 & 3 & 5 & 43 & 22 \\ 23 & 13 & 3 & 25 & 9 & 6 & 2 & 47 \\ 5 & 4 & 3 & 30 & 3 & 15 & 17 & 51 \\ 6 & 17 & 44 & 6 & 1 & 9 & 10 & 35 \\ 24 & 30 & 14 & 8 & 1 & 5 & 36 & 10 \\ 30 & 17 & 7 & 4 & 3 & 5 & 16 & 46 \\ 61 & 20 & 6 & 2 & 2 & 7 & 23 & 7 \\ 57 & 16 & 18 & 11 & 2 & 5 & 4 & 15 \end{bmatrix} \tag{12}$$

Obviously, the private keys of each participant in matrix B^0 are shown in Table 4.

The private keys of the above participants meet $\sum_{t=1}^{6} a_i^0 + b^0 + c^0 = 1024 = 0(mod\,64)$. Similar to matrix B^0, the representation of other key generation matrixes $\{B^1, B^2, ..., B^5\}$ can be found in the appendix A. Therefore, based on the key generation matrixes $\{B^0, B^1, B^2, ..., B^5\}$, the private keys sequence owned by each participant is shown in Table 5.

Step I2. Bob generates six entangled six-particle states, represented as $\{|w\rangle^0, |w\rangle^1, ..., |w\rangle^5\}$, by using QFT and SUM gate. Thus, there is $|w\rangle^j = \frac{1}{8}\sum_{p=0}^{63} |p\rangle_1^j |p\rangle_2^j \cdots |p\rangle_6^j (j = 0, 1, 2, ..., 5)$, where $|p\rangle_i^j$ represents the ith particle in the jth entangled state.

Table 5 Private keys sequence owned by each participant

Participants	Private keys sequences of participants
$Alice_1$	$\{a_1^0, a_1^1, a_1^2, a_1^3, a_1^4, a_1^5 = 213, 307, 239, 210, 371, 350\}$
$Alice_2$	$\{a_2^0, a_2^1, a_2^2, a_2^3, a_2^4, a_2^5 = 144, 199, 206, 205, 200, 289\}$
$Alice_3$	$\{a_3^0, a_3^1, a_3^2, a_3^3, a_3^4, a_3^5 = 115, 147, 240, 268, 182, 306\}$
$Alice_4$	$\{a_4^0, a_4^1, a_4^2, a_4^3, a_4^4, a_4^5 = 87, 188, 278, 121, 299, 235\}$
$Alice_5$	$\{a_5^0, a_5^1, a_5^2, a_5^3, a_5^4, a_5^5 = 24, 66, 50, 117, 314, 161\}$
$Alice_6$	$\{a_6^0, a_6^1, a_6^2, a_6^3, a_6^4, a_6^5 = 57, 138, 166, 67, 160, 192\}$
Bob	$\{b^0, b^1, b^2, b^3, b^4, b^5 = 151, 162, 174, 275, 241, 252\}$
$Charlie$	$\{c^0, c^1, c^2, c^3, c^4, c^5 = 233, 201, 183, 273, 281, 263\}$

Step I3. Bob generates six entangled six-particle states in the Step I2, with the order represented as

$$\left(\frac{1}{8}\sum_{p=0}^{63}|p\rangle_1^0|p\rangle_2^0\cdots|p\rangle_6^0, \frac{1}{8}\sum_{p=0}^{63}|p\rangle_1^1|p\rangle_2^1\cdots|p\rangle_6^1, \cdots, \frac{1}{8}\sum_{p=0}^{63}|p\rangle_1^5|p\rangle_2^5\cdots|p\rangle_6^5\right). \tag{13}$$

Then Bob extracts the $ith(i = 1, 2, ..., 6)$ particle from each six-particle entangled state to construct a sequence containing six particles, thus generating six six-particle sequences and sending the ith six-particle sequence directly to $Alice_i$ through quantum channel. Therefore, the particle sequence obtained by each initial signer $Alice_i(i = 1, 2, ..., 6)$ is $(|p\rangle_i^0, |p\rangle_i^1, ..., |p\rangle_i^5)$.

4.2 Signature phase

Step S1. The initial signers $Alice_i(i = 1, 2, ..., 6)$ respectively perform $U_{r_i^j + a_i^j} QFT$ operations on the particles they own, and the $r_i^j + a_i^j$ in $U_{r_i^j + a_i^j}$ corresponding to different messages X_i are different. The corresponding rule is: if the $jth(j = 0, 1, ..., 5)$ bit of the binary bits of message X_i is 1, then the parameter $r_i^j = 1$ in $U_{r_i^j + a_i^j}$ acting on the jth particle; If the $jth(j = 0, 1, ..., 5)$ bit of the binary bits of message X_i is 0, then the parameter $r_i^j = 0$ in $U_{r_i^j + a_i^j}$ acting on the jth particle. The detailed description is shown in Table 6.

Table 6 The case where the initial signers perform basis exchange operators on different particles they possess

Initial signers	i	X_i	$\|p\rangle_i^0$	$\|p\rangle_i^1$	$\|p\rangle_i^2$	$\|p\rangle_i^3$	$\|p\rangle_i^4$	$\|p\rangle_i^5$
$Alice_1$	$i = 1$	$X_1 = 101110$	$U_{a_1^0}$	$U_{1+a_1^1}$	$U_{1+a_1^2}$	$U_{1+a_1^3}$	$U_{a_1^4}$	$U_{1+a_1^5}$
$Alice_2$	$i = 2$	$X_2 = 100100$	$U_{a_2^0}$	$U_{a_2^1}$	$U_{1+a_2^2}$	$U_{a_2^3}$	$U_{a_2^4}$	$U_{1+a_2^5}$
$Alice_3$	$i = 3$	$X_3 = 000111$	$U_{1+a_3^0}$	$U_{1+a_3^1}$	$U_{1+a_3^2}$	$U_{a_3^3}$	$U_{a_3^4}$	$U_{a_3^5}$
$Alice_4$	$i = 4$	$X_4 = 001110$	$U_{a_4^0}$	$U_{1+a_4^1}$	$U_{1+a_4^2}$	$U_{1+a_4^3}$	$U_{a_4^4}$	$U_{a_4^5}$
$Alice_5$	$i = 5$	$X_5 = 011100$	$U_{a_5^0}$	$U_{a_5^1}$	$U_{1+a_5^2}$	$U_{1+a_5^3}$	$U_{1+a_5^4}$	$U_{a_5^5}$
$Alice_6$	$i = 6$	$X_6 = 111000$	$U_{a_6^0}$	$U_{a_6^1}$	$U_{a_6^2}$	$U_{1+a_6^3}$	$U_{1+a_6^4}$	$U_{1+a_6^5}$

Next, the entangled state $|w\rangle^0 = \frac{1}{8}\sum_{p=0}^{63}|p\rangle_1^0|p\rangle_2^0\cdots|p\rangle_6^0$ prepared will be used as an example to illustrate, where six particles contained in the entangled state $|w\rangle^0$ are respectively sent to six initial signers. $Alice_1$ performs $U_{a_1^0}QFT$ operation on the first particle of entangled state $|w\rangle^0$. $Alice_2$ performs $U_{a_2^0}QFT$ operation on the second particle of entangled state $|w\rangle^0$. $Alice_3$ performs $U_{1+a_3^0}QFT$ operation on the third particle of entangled state $|w\rangle^0$. $Alice_4$ performs $U_{a_4^0}QFT$ operation on the fourth particle of entangled state $|w\rangle^0$. $Alice_5$ performs $U_{a_5^0}QFT$ operation on the fifth particle of entangled state $|w\rangle^0$. $Alice_6$ performs $U_{a_6^0}QFT$ operation on the sixth particle of entangled state $|w\rangle^0$. Suppose that the entangled state $|w\rangle^0$ is subjected to $U_{r_i^0+a_i^0}QFT$ operations, the result of the operations is denoted as $|R\rangle^0$. The calculation process is as follows:

$$
\begin{aligned}
&|R\rangle^0 = (U_{a_1^0}QFT)\otimes(U_{a_2^0}QFT)\otimes(U_{1+a_3^0}QFT)\otimes(U_{a_4^0}QFT)\otimes(U_{a_5^0}QFT)\otimes(U_{a_6^0}QFT)|w\rangle^0\\
&=\frac{1}{8}\sum_{p=0}^{63}(U_{a_1^0}QFT)|p\rangle_1^0\otimes(U_{a_2^0}QFT)|p\rangle_2^0\otimes(U_{1+a_3^0}QFT)|p\rangle_3^0\otimes(U_{a_4^0}QFT)|p\rangle_4^0\\
&\quad\otimes(U_{a_5^0}QFT)|p\rangle_5^0\otimes(U_{a_6^0}QFT)|p\rangle_6^0\\
&=\frac{1}{8}\sum_{p=0}^{63}\left(\frac{1}{8}\sum_{l_1^0=0}^{63}e^{2\pi i\frac{p}{64}l_1^0}|l_1^0+a_1^0\rangle\right)\otimes\left(\frac{1}{8}\sum_{l_2^0=0}^{63}e^{2\pi i\frac{p}{64}l_2^0}|l_2^0+a_2^0\rangle\right)\otimes\left(\frac{1}{8}\sum_{l_3^0=0}^{63}e^{2\pi i\frac{p}{64}l_3^0}|l_3^0+1+a_3^0\rangle\right)\\
&\quad\otimes\left(\frac{1}{8}\sum_{l_4^0=0}^{63}e^{2\pi i\frac{p}{64}l_4^0}|l_4^0+a_4^0\rangle\right)\otimes\left(\frac{1}{8}\sum_{l_5^0=0}^{63}e^{2\pi i\frac{p}{64}l_5^0}|l_5^0+a_5^0\rangle\right)\otimes\left(\frac{1}{8}\sum_{l_6^0=0}^{63}e^{2\pi i\frac{p}{64}l_6^0}|l_6^0+a_6^0\rangle\right)\\
&=\left(\frac{1}{8}\right)^7\sum_{l_1^0,l_2^0,\cdots,l_6^0=0}^{63}(\sum_{p=0}^{63}e^{2\pi i\frac{l_1^0+l_2^0+\cdots+l_6^0}{64}p}|l_1^0+a_1^0\rangle\otimes|l_2^0+a_2^0\rangle\otimes|l_3^0+1+a_3^0\rangle\\
&\quad\otimes|l_4^0+a_4^0\rangle\otimes|l_5^0+a_5^0\rangle\otimes|l_6^0+a_6^0\rangle).
\end{aligned}
\tag{14}
$$

Because of

$$
\sum_{p=0}^{63}e^{2\pi i\frac{l_1^0+l_2^0+\cdots+l_6^0}{64}p}=\begin{cases}0, & l_1^0+l_2^0+\cdots+l_6^0\neq 0\,mod\,64\\ 64, & l_1^0+l_2^0+\cdots+l_6^0=0\,mod\,64\end{cases},
\tag{15}
$$

so there is

$$
\begin{aligned}
|R\rangle^0=\left(\frac{1}{8}\right)^5\sum_{l_1^0+l_2^0+\cdots+l_6^0=0 mod\,64}&|l_1^0+a_1^0\rangle\otimes|l_2^0+a_2^0\rangle\otimes|l_3^0+1+a_3^0\rangle\otimes|l_4^0+a_4^0\rangle\\
&\otimes|l_5^0+a_5^0\rangle\otimes|l_6^0+a_6^0\rangle.
\end{aligned}
\tag{16}
$$

Similarly, the operations of other entangled particles $\{|w\rangle^1, |w\rangle^2, ..., |w\rangle^5\}$ are as follows:

$$|R\rangle^1 = \left(\frac{1}{8}\right)^5 \sum_{l_1^1+l_2^1+\cdots+l_6^1=0 mod\, 64} |l_1^1+1+a_1^1\rangle \otimes |l_2^1+a_2^1\rangle \otimes |l_3^1+1+a_3^1\rangle \otimes |l_4^1+1+a_4^1\rangle \otimes |l_5^1+a_5^1\rangle \otimes |l_6^1+a_6^1\rangle. \tag{17}$$

$$|R\rangle^2 = \left(\frac{1}{8}\right)^5 \sum_{l_1^2+l_2^2+\cdots+l_6^2=0 mod\, 64} |l_1^2+1+a_1^2\rangle \otimes |l_2^2+1+a_2^2\rangle \otimes |l_3^2+1+a_3^2\rangle \otimes |l_4^2+1+a_4^2\rangle \otimes |l_5^2+1+a_5^2\rangle \otimes |l_6^2+a_6^2\rangle. \tag{18}$$

$$|R\rangle^3 = \left(\frac{1}{8}\right)^5 \sum_{l_1^3+l_2^3+\cdots+l_6^3=0 mod\, 64} |l_1^3+1+a_1^3\rangle \otimes |l_2^3+a_2^3\rangle \otimes |l_3^3+a_3^3\rangle \otimes |l_4^3+1+a_4^3\rangle \otimes |l_5^3+1+a_5^3\rangle \otimes |l_6^3+1+a_6^3\rangle. \tag{19}$$

$$|R\rangle^4 = \left(\frac{1}{8}\right)^5 \sum_{l_1^4+l_2^4+\cdots+l_6^4=0 mod\, 64} |l_1^4+a_1^4\rangle \otimes |l_2^4+a_2^4\rangle \otimes |l_3^4+a_3^4\rangle \otimes |l_4^4+a_4^4\rangle \otimes |l_5^4+1+a_5^4\rangle \otimes |l_6^4+1+a_6^4\rangle. \tag{20}$$

$$|R\rangle^5 = \left(\frac{1}{8}\right)^5 \sum_{l_1^5+l_2^5+\cdots+l_6^5=0 mod\, 64} |l_1^5+1+a_1^5\rangle \otimes |l_2^5+1+a_2^5\rangle \otimes |l_3^5+a_3^5\rangle \otimes |l_4^5+a_4^5\rangle \otimes |l_5^5+a_5^5\rangle \otimes |l_6^5+1+a_6^5\rangle. \tag{21}$$

Based on the above calculation results, the signatures of $Alice_i (i = 1, 2, ..., 6)$ are shown in Table 7.

Table 7 Information signature pairs of initial signers

Initial signers	Information signature pairs of initial signers
$Alice_1$	$\{X_1, S_1 = (\|l_1^0+a_1^0\rangle, \|l_1^1+1+a_1^1\rangle, \|l_1^2+1+a_1^2\rangle, \|l_1^3+1+a_1^3\rangle, \|l_1^4+a_1^4\rangle, \|l_1^5+1+a_1^5\rangle)\}$
$Alice_2$	$\{X_2, S_2 = (\|l_2^0+a_2^0\rangle, \|l_2^1+a_2^1\rangle, \|l_2^2+1+a_2^2\rangle, \|l_2^3+a_2^3\rangle, \|l_2^4+a_2^4\rangle, \|l_2^5+1+a_2^5\rangle)\}$
$Alice_3$	$\{X_3, S_3 = (\|l_3^0+1+a_3^0\rangle, \|l_3^1+1+a_3^1\rangle, \|l_3^2+1+a_3^2\rangle, \|l_3^3+a_3^3\rangle, \|l_3^4+a_3^4\rangle, \|l_3^5+a_3^5\rangle)\}$
$Alice_4$	$\{X_4, S_4 = (\|l_4^0+a_4^0\rangle, \|l_4^1+1+a_4^1\rangle, \|l_4^2+1+a_4^2\rangle, \|l_4^3+1+a_4^3\rangle, \|l_4^4+a_4^4\rangle, \|l_4^5+a_4^5\rangle)\}$
$Alice_5$	$\{X_5, S_5 = (\|l_5^0+a_5^0\rangle, \|l_5^1+a_5^1\rangle, \|l_5^2+1+a_5^2\rangle, \|l_5^3+1+a_5^3\rangle, \|l_5^4+1+a_5^4\rangle, \|l_5^5+a_5^5\rangle)\}$
$Alice_6$	$\{X_6, S_6 = (\|l_6^0+a_6^0\rangle, \|l_6^1+a_6^1\rangle, \|l_6^2+a_6^2\rangle, \|l_6^3+1+a_6^3\rangle, \|l_6^4+1+a_6^4\rangle, \|l_6^5+1+a_6^5\rangle)\}$

After the initial signers $Alice_i(i = 1, 2, ..., 6)$ complete the signatures, they return the signature particles they own to *Bob*. During the transmission process, eavesdropping detection is used between $Alice_i$ and *Bob* to ensure the secure transmission of signatures.

4.3 Aggregation phase

Step A1. *Bob* performs five group addition operations on the $jth(j = 0, 1, ..., 5)$ particle from each of the six signature particles sent by $Alice_i(i = 1, 2, ..., 6)$, resulting in the aggregation of six sets of quantum sequences into one set of quantum sequence. Therefore, *Bob* can obtain $S = \{|(l_1^0+l_2^0+\cdots+l_6^0+a_1^0+a_2^0+\cdots+a_6^0+1)mod\,64\rangle, |(l_1^1+l_2^1+\cdots+l_6^1+a_1^1+a_2^1+\cdots+a_6^1+3)mod\,64\rangle, |(l_1^2+l_2^2+\cdots+l_6^2+a_1^2+a_2^2+\cdots+a_6^2+5)mod\,64\rangle, |(l_1^3+l_2^3+\cdots+l_6^3+a_1^3+a_2^3+\cdots+a_6^3+4)mod\,64\rangle, |(l_1^4+l_2^4+\cdots+l_6^4+a_1^4+a_2^4+\cdots+a_6^4+2)mod\,64\rangle, |(l_1^5+l_2^5+\cdots+l_6^5+a_1^5+a_2^5+\cdots+a_6^5+3)mod\,64\rangle\} = \{|(a_1^0+a_2^0+\cdots+a_6^0+1)mod\,64\rangle, |(a_1^1+a_2^1+\cdots+a_6^1+3)mod\,64\rangle, |(a_1^2+a_2^2+\cdots+a_6^2+5)mod\,64\rangle, |(a_1^3+a_2^3+\cdots+a_6^3+4)mod\,64\rangle, |(a_1^4+a_2^4+\cdots+a_6^4+2)mod\,64\rangle, |(a_1^5+a_2^5+\cdots+a_6^5+3)mod\,64\rangle\}$, which is a quantum signature generated by *Bob* through group addition operations, that is, a quantum homomorphic aggregate signature.

Step A2. In order to ensure the secure transmission of the quantum homomorphic aggregate signature to *Charlie*, *Bob* uses the U_{b^j} operations to add his private key $k_B = (b^0, b^1, ..., b^5)$ to the quantum homomorphic aggregate signature S. Suppose the encrypted quantum sequence is S', there is $S' = \{|(a_1^0 + a_2^0 + \cdots + a_6^0 + 1 + b^0)mod\,64\rangle, |(a_1^1+a_2^1+\cdots+a_6^1+3+b^1)mod\,64\rangle, |(a_1^2+a_2^2+\cdots+a_6^2+5+b^2)mod\,64\rangle, |(a_1^3+a_2^3+\cdots+a_6^3+4+b^3)mod\,64\rangle, |(a_1^4+a_2^4+\cdots+a_6^4+2+b^4)mod\,64\rangle, |(a_1^5+a_2^5+\cdots+a_6^5+3+b^5)mod\,64\rangle\}$. Then, *Bob* sends the encrypted quantum sequence S' to *Charlie* through a quantum channel.

4.4 Verification phase

Step V1. After receiving the S' sent by *Bob*, *Charlie* also uses $U_{c^j}(j = 0, 1, 2, ..., 5)$ operations to add his private key $k_C = (c^0, c^1, ..., c^5)$ to the quantum sequence S', marking the transformed quantum sequence as S''. Thus, there is $S'' = \{|(a_1^0 + a_2^0 + \cdots + a_6^0 + 1 + b^0 + c^0)mod\,64\rangle, |(a_1^1+a_2^1+\cdots+a_6^1+3+b^1+c^1)mod\,64\rangle, |(a_1^2+a_2^2+\cdots+a_6^2+5+b^2+c^2)mod\,64\rangle, |(a_1^3+a_2^3+\cdots+a_6^3+4+b^3+c^3)mod\,64\rangle, |(a_1^4+a_2^4+\cdots+a_6^4+2+b^4+c^4)mod\,64\rangle, |(a_1^5+a_2^5+\cdots+a_6^5+3+b^5+c^5)mod\,64\rangle\}$. By combining the property of the key generation matrixes, i.e. $\sum_{i=1}^{6} a_i^j + b^j + c^j = 0(mod\,64)$, the quantum sequence owned by *Charlie* is transformed into $S'' = \{|1\rangle, |3\rangle, |5\rangle, |4\rangle, |2\rangle, |3\rangle\}$.

Step V2. *Charlie* used a set of computational bases $\{|0\rangle, |1\rangle, ..., |6\rangle\}$ to measure the quantum sequence S'', and the measured results are $g^0 = 1, g^1 = 3, g^2 = 5, g^3 = 4, g^4 = 2, g^5 = 3$. Then *Charlie* calculates the sum of the messages $X_i(i = 1, 2, ..., 6)$ converted to decimal based on the measurement results as $Sum' = 1 \cdot 2^0 + 3 \cdot 2^1 + 5 \cdot 2^2 + 4 \cdot 2^3 + 2 \cdot 2^4 + 3 \cdot 2^5 = 187$.

When *Charlie* receives the $E_{k_{A_iC}}(X_i)$ sent by $Alice_i(i = 1, 2, ..., 6)$, he decrypts it using the key K_{A_iC} to obtain $X_i(i = 1, 2, ..., 6)$. Then *Charlie* converts X_i to decimal $x_i(i = 1, 2, ..., 6)$, i.e. $x_1 = 46, x_2 = 36, x_3 = 7, x_4 = 14, x_5 = 28, x_6 = 56$, so there is

$Sum = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 187$. Finally, *Charlie* compares and verifies Sum with Sum'.

5 Analysis of the scheme

5.1 Correctness analysis

In this section, we provide a correctness analysis of the scheme, which mainly focuses on the signature, aggregation, and final messages verification. This section takes the messages as the starting point and verifies the validity of the signature by verifying the correctness of the messages.

Theorem 1. *Suppose that the initial signer* $Alice_i$ *owns the message* $X_i \in \{0,1\}^n$ *and converts it to decimal* x_i*. Then* $Alice_i$ *performs* $U_{r_i^j}$ *operations on* n *particles* $\{|0\rangle_i^0, |0\rangle_i^1, ..., |0\rangle_i^{n-1}\}$ *based on* X_i*, corresponding to the rule: if the* $jth (j = 0, 1, ..., n-1)$ *bit of the binary bits of message* X_i *is 1, then the parameter* r_i^j *in* $U_{r_i^j}$ *acting on the* jth *particle is 1; Otherwise, the parameter* $r_i^j = 0$*. If and only if* $2^0 r_i^0 + 2^1 r_i^1 + \cdots + 2^{n-1} r_i^{n-1} = x_i$*, then the proposed quantum homomorphic aggregate signature scheme is correct.*

Proof of Theorem 1. In this scheme, $Alice_i (i = 1, 2, ..., n)$ use $U_{r_i^j + a_i^j} QFT$ operations to add the messages X_i to the signature, and then send it to the aggregator *Bob* through a quantum channel. Finally, Bob sends it to the verifier *Charlie* for final messages verification. To prove the correctness of the proposed signature scheme, it is only necessary to verify that the operation results encrypted by $U_{r_i^j}$ match the original messages $X_i \in \{0,1\}^n$. Firstly, we perform $U_{r_i^j}$ operations on $\{|0\rangle_i^0, |0\rangle_i^1, ..., |0\rangle_i^{n-1}\}$ based on X_i, resulting in the expression $\{(U_{r_i^0}|0\rangle_i^0), (U_{r_i^1}|0\rangle_i^1), ..., (U_{r_i^{n-1}}|0\rangle_i^{n-1})\}$, and the results of the operations are represented as $\{|r_i^0\rangle_i^0, |r_i^1\rangle_i^1, ..., |r_i^{n-1}\rangle_i^{n-1}\}$. Then we measure the operation results to obtain $\{r_i^0, r_i^1, ..., r_i^{n-1}\}$. Starting from the corresponding rule, r_i^j is the element representation of the jth bit of message X_i. Therefore, there is $2^0 r_i^0 + 2^1 r_i^1 + \cdots + 2^{n-1} r_i^{n-1} = x_i$. □

5.2 Homomorphism analysis

In this section, we mainly analyze the homomorphism of the proposed scheme. In preliminary section, we define a mapping from set $\{0, 1, ..., d-1\}$ to set $\{|0\rangle, |1\rangle, ..., |d-1\rangle\}$, and the mapping function δ satisfies $\delta(0) = |0\rangle, \delta(1) = |1\rangle, ..., \delta(d-1) = |d-1\rangle$. Based on this mapping function δ, there is $\delta(x)\Theta\delta(y) = \delta((x+y) mod\, d)$ for $\forall x, y \in \{0, 1, 2, ..., d-1\}$, so the mapping δ satisfies the property of additive homomorphism. In fact, since the mapping δ is a bijective, it is also an isomorphic mapping. Let's assume that $Alice_1$'s signature is $Sig(X_1) = U_{r_1^j + a_1^j} QFT|p\rangle_1^j = |l_1^j + r_1^j + a_1^j\rangle = \delta(l_1^j + r_1^j + a_1^j)$. $Alice_2$'s signature is $Sig(X_2) = U_{r_2^j + a_2^j} QFT|p\rangle_2^j = |l_2^j + r_2^j + a_2^j\rangle = \delta(l_2^j + r_2^j + a_2^j)$. Similarly, $Alice_n$'s signature is $Sig(X_n) = U_{r_n^j + a_n^j} QFT|p\rangle_n^j = |l_n^j + r_n^j + a_n^j\rangle = \delta(l_n^j + r_n^j + a_n^j)$. Thus, the signature of the message $X_1 + X_2 + \cdots + X_n$ can be generated as

follows:

$$
\begin{aligned}
&Sig(X_1)\Theta Sig(X_2)\Theta\cdots\Theta Sig(X_n)\\
&\quad=\delta(l_1^j+r_1^j+a_1^j)\Theta\delta(l_2^j+r_2^j+a_2^j)\Theta\cdots\Theta\delta(l_n^j+r_n^j+a_n^j)\\
&\quad=\delta\{(l_1^j+r_1^j+a_1^j+l_2^j+r_2^j+a_2^j+\cdots+l_n^j+r_n^j+a_n^j)mod\,d\}\\
&\quad=\delta\{(l_1^j+l_2^j+\cdots+l_n^j+r_1^j+r_2^j+\cdots+r_n^j+a_1^j+a_2^j+\cdots+a_n^j)mod\,d\}\\
&\quad=Sig(X_1+X_2+\cdots+X_n)
\end{aligned}
\tag{22}
$$

Compared with the additive homomorphic model $f(\rho(a_1),\rho(a_2),...,\rho(a_n))=\rho(a_1+a_2+\cdots+a_n)$, our signature scheme satisfies the additive homomorphic property.

6 Safety analysis

In this section, we provide a security analysis of the scheme, mainly from six aspects: non-repudiation, unforgeability, entanglement measurement attacks, private key sequence attacks, intercept-resend attacks, and aggregator *Bob*'s attacks.

6.1 Unforgeability

In the process of quantum signature, internal attackers generally have a greater ability to forge signatures than external attackers. Therefore, this section mainly analyzes the possibility of signature forgery among the participants of the scheme.

6.1.1 The initial signer $Alice_i$ cannot forge the signatures of other initial signers

This scheme has n initial signers $Alice_i(i=1,2,...,n)$ who need to sign messages $X_i(i=1,2,...,n)$ respectively. Each initial signer needs to perform $U_{r_i^j+a_i^j}QFT$ operations on n particles based on a message of length n. Let's assume that $Alice_i$ wants to forge a signature on $Alice_{i+1}(i+1\leq n)$, at which point $Alice_i$ must know $r_{i+1}^j+a_{i+1}^j$. Due to the fact that $a_{i+1}^j=\sum_{z=1}^{n+2}a_{z(i+1)}^j$ and $a_{z(i+1)}^j$ are randomly generated elements, it is clearly not feasible for $Alice_i$ to forge the signature of $Alice_{i+1}$.

6.1.2 Aggregator *Bob* cannot forge signature

If *Bob* wants to forge the signature of the initial signer $Alice_i$, since $a_i^j=\sum_{z=1}^{n+2}a_{zi}^j$ and a_{zi}^j is a randomly generated element in the key generation matrix, it is not feasible for *Bob* to forge $Alice_i$'s signature through $U_{r_i^j+a_i^j}QFT$. Further analysis shows that if *Bob* uses computational basis $V_1=\{|0\rangle,|1\rangle,\cdots,|d-1\rangle\}$ to measure the quantum signature S_i sent by $Alice_i$, he still cannot obtain any information about $Alice_i$, so it is not feasible for *Bob* to forge $Alice_i$'s signature.

6.1.3 Verifier *Charlie* cannot forge signature

If *Charlie* wants to forge the signature of the initial signer $Alice_i$, he must know $r_i^j+a_i^j$. Due to *Charlie* receiving an $E_{k_{A_iC}}(X_i)$ sent by $Alice_i$, only the value of r_i^j can be inferred, but the value of $a_i^j=\sum_{z=1}^{n+2}a_{zi}^j$ cannot be inferred. Therefore, *Charlie* cannot forge the signature of the initial signer $Alice_i$. If *Charlie* wants to forge the signature

of aggregator Bob, because Bob's signature S also contains the random private key a_i^j of $Alice_i$, and Bob adds his own random private key b^j to the quantum signature through the basis exchange operations during the quantum signature sending process to $Charlie$. Based on the above analysis, $Charlie$ cannot infer a_i^j and b^j, so $Charlie$ cannot forge the signature of aggregator Bob.

6.2 Non-repudiation

This section focuses on two aspects of analysis and explanation, namely, the initial signer $Alice_i$ denies sending the signature to Bob, and the aggregator Bob denies sending the signature to $Charlie$.

6.2.1 The initial signer $Alice_i$ denies sending the signature S_i to Bob

Anyone can only obtain S_i with the correct key a_i^j and message X_i. According to the unconditional security of QKD, only $Alice_i$ has the key a_i^j and message X_i, thus Bob cannot forge the signature. So, in this scheme, $Alice_i$ cannot deny that she sent the signature S_i to Bob.

6.2.1 The aggregator Bob denies sending the signature to $Charlie$

In the previous section, we analyzed that the scheme has unforgeability, so no one can forge the signature S_i of $Alice_i$. When Bob receives a signature from $Alice_i$, only Bob has $Alice_i$'s signature S_i and his private key b^j, so only Bob can generate a quantum homomorphic aggregate signature S. Therefore, in this scheme, Bob cannot deny that he sent the signature S to $Charlie$.

6.3 Entanglement measurement attack

Assuming that the adversary Eve attempts an entanglement measurement attack between n initial signers $Alice_i$. When aggregator Bob sends entangled particles to $Alice_i$, Eve intercepts these particles during the particles transport from Bob to $Alice_i$. Then Eve prepares several auxiliary particles and performes SUM operations on the intercepted particles and auxiliary particles. After $Alice_i$ completes the signature, Eve measures the auxiliary particles to obtain useful information about $Alice_i$.

Let's assume that Bob sends the ith particle of the jth entangled state to the initial signer $Alice_i$, and the adversary Eve will intercept this particle during the transmission process. Then the adversary Eve prepares a d-dimensional auxiliary particle $|q\rangle (q \in 0, 1, ..., d-1)$, and uses the intercepted particle as the control particle and $|q\rangle$ as the target particle to perform SUM operation. The operation result is represented as $|E\rangle = U_{SUM}|w\rangle^j = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} |p\rangle_1^j |p\rangle_2^j \cdots |p\rangle_i^j |p+q\rangle_{Eve} \cdots |p\rangle_n^j$.

Then Eve sends the intercepted particle to $Alice_i$. After completing channel security detection in $Alice_i$, if Eve measures auxiliary particle, he will obtain $p+q$. Although Eve can deduce p, it does not contain any information about the initial signer $Alice_i$, so Eve cannot obtain any personal information about $Alice_i$. If $Alice_i$

will sign, $|E\rangle$ will take the following form:

$$\begin{aligned}|E\rangle' &= (U_{r_1^j+a_1^j}QFT)\otimes(U_{r_2^j+a_2^j}QFT)\otimes\cdots\otimes(U_{r_n^j+a_n^j}QFT)|E\rangle \\ &= d^{\frac{1-n}{2}}\sum_{l_1^j+l_2^j+\cdots+l_n^j=0\,mod\,d}|l_1^j+r_1^j+a_1^j\rangle\otimes\cdots\otimes|l_i^j+r_i^j+a_i^j\rangle|p+q\rangle_{Eve} \\ &\quad\otimes\cdots\otimes|l_n^j+r_n^j+a_n^j\rangle.\end{aligned} \tag{23}$$

It is obvious that even if *Eve* measures auxiliary particle, he still cannot obtain any information about $Alice_i$. Therefore, our scheme can resist entanglement measurement attacks.

6.4 Private key sequence attack

In this section, we provide a security analysis of the public key generation matrix elements, except for those retained by each participant themselves.

Firstly, during the initialization phase, the scheme generates the private keys of each participating party by constructing key generation matrixes, thereby utilizing the private key sequences for secure transmission of signatures. Secondly, the key generation matrixes are randomly generated by each participating party under the condition that the sum of each row element modulus d is 0. Even if all elements except for those retained by each participating party are publicly available, it can ensure the secure transmission and verification of messages and signatures. Let's assume that the sum of elements in each row of the key generation matrixes is kd. Obviously, it can be seen that the value of k here is any integer value, so there are infinite possibilities for the elements retained by each participating party. Therefore, the disclosure of the remaining elements of the key generation matrixes is secure. Further analysis reveals that even if the adversary infers the elements retained by each participant, he will know the private keys of each participant. However, since our quantum signature $S_i = (|l_i^0 + r_i^0 + a_i^0\rangle, |l_i^1 + r_i^1 + a_i^1\rangle, \cdots, |l_i^{n-1} + r_i^{n-1} + a_i^{n-1}\rangle)$ contains not only the private key sequence $(a_i^0, a_i^1, ..., a_i^{n-1})$, but also the $(l_i^0, l_i^1, ..., l_i^{n-1})$ and $(r_i^0, r_i^1, ..., r_i^{n-1})$ sequences, it is impossible for an adversary to steal the private information of the signers through the private key sequence.

6.5 Intercept-resend attack

If the adversary *Eve* wants to carry out intercept-resend attack, the main target of the attack is concentrated in the transmission process of particles. In this scheme, the transmission of particles mainly involves three processes: firstly, *Bob* allocates entangled particles to $Alice_i$; secondly, after performing the $U_{r_i^j+a_i^j}QFT$ operations, $Alice_i$ sends the signed particles to *Bob*; thirdly, *Bob* aggregates the signatures of $Alice_i$ through group addition operations and sends the aggregated signature particles to the verifier *Charlie*.

In the first process, *Bob* allocates entangled particles to $Alice_i$ through quantum secure direct communication in the scheme, which has been proven to be unconditionally secure [44]. Further analysis shows that if *Eve* intercepts entangled particles,

based on the analysis in section 6.3, we can conclude that the first process of particle transport is safe. In the second process, we use eavesdropping detection to randomly select decoy particles from two sets of conjugate bases V_1 and V_2 to detect the presence of external enemies. This technique has been proven to be unconditionally safe [45]. Further analysis shows that if Eve intercepts the signature particles, according to section 6.3, it can be concluded that the transmission of the second process signature particles is secure. In the third process, Bob encrypts the aggregated signature particles using the private key b^j, and then sends them to the verifier $Charlie$ through a quantum channel. Even if Eve intercepts the signature particles, due to the presence of $Alice_i$'s random private key $a_i^j$and Bob's random private key b^j in the signature particles, Eve still cannot obtain any privacy information about $Alice_i$ and Bob. Therefore, our scheme can resist intercept-resend attack.

6.6 internal attacks by aggregator

Compared to external enemy attacks, Bob has a stronger possibility of attack. Because he is responsible for the preparation and distribution of entangled particles, as well as the generation of quantum homomorphic aggregate signature, thus he is a core participant in the entire scheme. If Bob wants to steal $Alice_i$ privacy information, he can launch the following attacks. Here, we take the n-particle entangled state $|w\rangle^0$ prepared by Bob as an example for analysis, where $|w\rangle^0 = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} |p\rangle_1^0 |p\rangle_2^0 \cdots |p\rangle_n^0$.

6.6.1 Attack 1

Let's assume that Bob also make a copy of $|w\rangle^0$ while preparing $|w\rangle^0$, denoted as $|w'\rangle^0$. Firstly, Bob uses computational base $V_1 = \{|0\rangle, |1\rangle, ..., |d-1\rangle\}$ to measure all n particles in copy $|w'\rangle^0$ and obtains the measurement result $(p, p, ..., p)$. Then, Bob performs inverse QFT on n particles of $|w\rangle^0$, and the result is represented as $QFT^{-1}|w\rangle^0 = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} (QFT^{-1}|p\rangle_1^0) \otimes (QFT^{-1}|p\rangle_2^0) \otimes \cdots \otimes (QFT^{-1}|p\rangle_n^0)$. Bob distributes the ith particle after QFT^{-1} operation to the initial signer $Alice_i$. After receiving the ith particle, $Alice_i$ performs $U_{r_i^0+a_i^0}QFT$ operation on it, and the operation result is represented as $U_{r_i^0+a_i^0}QFT(QFT^{-1}|p\rangle_i^0) = U_{r_i^0+a_i^0}|p\rangle_i^0 = |p + r_i^0 + a_i^0\rangle_i^0$.

After completing the $U_{r_i^0+a_i^0}QFT$ operations, $Alice_i$ sends the particles to the aggregator Bob, and the particle sequence is represented as$(|p + r_1^0 + a_1^0\rangle_1^0, |p + r_2^0 + a_2^0\rangle_2^0, ..., |p + r_n^0 + a_n^0\rangle_n^0)$. Then, Bob measures these particles and obtains the following result $(p + r_1^0 + a_1^0, p + r_2^0 + a_2^0, ..., p + r_n^0 + a_n^0)$. Obviously, Bob knows the value of p, but he doesn't know the value of $r_i^0 + a_i^0$. Therefore, no relevant information can be obtained.

6.6.2 Attack 2

Bob first performs QFT on the last $n-1$ particles of $|w\rangle^0 = \frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} |p\rangle_1^0 |p\rangle_2^0 \cdots |p\rangle_n^0$, keeping the first particle unchanged. The result of the operation is represented as $\frac{1}{\sqrt{d}} \sum_{p=0}^{d-1} |p\rangle_1^0 (QFT|p\rangle_2^0) \otimes \cdots \otimes (QFT|p\rangle_n^0)$. Then, Bob sends the first particle of $|w\rangle^0$ to

$Alice_i$, while he saves the remaining particles himself. When $Alice_i$ receives a particle and performs $U_{r_i^0+a_i^0}QFT$ operation on it, the entangled state will take the following form

$$\begin{aligned}\frac{1}{\sqrt{d}}\sum_{p=0}^{d-1}(U_{r_i^0+a_i^0}QFT|p\rangle_1^0)\otimes(QFT|p\rangle_2^0)\otimes\cdots\otimes(QFT|p\rangle_n^0)\\ =d^{\frac{1-n}{2}}\sum_{l_1^0+l_2^0+\cdots+l_n^0=0\ mod\ d}|l_1^0+r_i^0+a_i^0\rangle\otimes|l_2^0\rangle\otimes|l_3^0\rangle\otimes\cdots\otimes|l_n^0\rangle.\end{aligned} \tag{24}$$

Bob measures n particles in the above equation, and the measurement results are $\{l_1^0+r_i^0+a_i^0, l_2^0, l_3^0, ..., l_n^0\}$. Next, Bob calculates the sum of the measurement results, which is $l_1^0+r_i^0+a_i^0+l_2^0+l_3^0+\cdots+l_n^0 = r_i^0+a_i^0(mod\ d)$. Due to Bob not knowing the value of $r_i^0+a_i^0$, he is unable to obtain the secret information of $Alice_i$. In summary, Bob's attack is ineffective for our scheme.

7 Efficiency analysis

In this section, we analyze the quantum efficiency of the scheme, without considering the required number of bits for eavesdropping detection. According to reference [46], here is a formal definition of quantum efficiency

$$\eta = \frac{b_s}{q_t + b_t}, \tag{25}$$

where b_s represents the number of bits of information X, q_t represents the number of quantum bits transmitted in the quantum channel, and b_t represents the number of classical bits transmitted in the classical channel. In our scheme, the length of information X_i is n bits, the total quantum information transmitted between $Alice_i$ and Bob is 2n bits, and the total quantum information transmitted between $Charlie$ and Bob is n bits, so $q_t = 2n^2+n$. The classical information transmitted between $Alice_i$ and Bob is a total of 0 bits, the classical information transmitted between $Charlie$ and Bob is a total of 0 bits, and the classical information transmitted between $Alice_i$ and $Charlie$ is a total of n bits, so $b_t = n^2$. Therefore, the efficiency of our scheme is

$$\eta = \frac{b_s}{q_t + b_t} = \frac{n^2}{3n^2+n} = \frac{n}{3n+1}. \tag{26}$$

For the example presented in this article, its efficiency is $\eta = \frac{6}{3\times6+1} = \frac{6}{19} = 31.5\%$. The comparison of schemes is shown in Table 8.

Compared with references [34–36, 40], our scheme has significant characteristics in quantum resources, length of signature message, eavesdropping detection, quantum circuit, and efficiency. The comparison of the above schemes is analyzed under the condition of $n = 2$. Firstly, references [34–36] are all quantum homomorphic signature schemes with homomorphic properties. Our scheme uses n-particle entangled states as quantum channels, generates private keys for each participant using key generation

Table 8 The comparison of schemes

Scheme	Quantum resource	Length of signature message	Eavesdropping detection	Quantum circuit	Efficiency
The scheme of reference [34]	EPR state	4 bits	No	No	12%
The scheme of reference [35]	Single-quantum state	$2n$ bits	No	No	14%
The scheme of reference [36]	Cluster state	$2n$ bits	No	Yes	9%
The scheme of reference [40]	EPR state	tn bits	Yes	No	14%
The scheme of this article	n-particle entangled state	n^2 bits	Yes	Yes	28.5%

matrixes, and uses QFT and basis exchange operator for signature. During the process of sending signed particles, eavesdropping detection is used. These characteristics are not present in references [34–36]. Reference [40] is a quantum aggregate signature scheme based on EPR states. Compared with reference [40], our scheme has significant advantages in quantum resources, signature message length, quantum circuit, and efficiency.

8 Conclusion

This article draws on the idea of quantum multi-party summation and proposes a quantum homomorphic aggregate signature scheme based on quantum Fourier transform. Our scheme uses QFT and SUM gate to generate n-particle entangled states, and the number of entangled particles can be adjusted according to the number of signers. This ensures the secure transmission of signatures and messages with fewer entangled particles during transmission, further improving the efficiency of quantum signatures. Based on the properties of the key generation matrix, our scheme randomly determines the row elements of the key generation matrix, and its column elements are the private keys of each participating party. Moreover, the scheme generates signatures from different signers based on different messages and private keys, which conforms to the overall framework and formal definition of aggregate signatures. In addition, the transmission of signature particles uses eavesdropping detection, and the message and private key transmission process is a quantum sequence combined with random numbers, so the aggregator does not need to measure and verify the quantum signature after receiving signatures from different signers. Our scheme utilizes quantum algorithms such as QFT and basis exchange operator, combined with randomly constructed key generation matrixes, making our scheme unforgeability and non-repudiation while satisfying additive homomorphic property. At the same time, our scheme can resist various attacks such as entanglement measurement attacks, private key sequence attacks, intercept-resend attacks, and internal attacks by aggregator.

Appendix A The representation of key generation matrixes

The B^1 matrix is represented as

$$\begin{bmatrix} 40 & 5 & 6 & 1 & 1 & 5 & 4 & 2 \\ 46 & 29 & 42 & 6 & 1 & 5 & 21 & 42 \\ 51 & 12 & 30 & 40 & 13 & 18 & 21 & 7 \\ 44 & 37 & 27 & 32 & 13 & 9 & 17 & 13 \\ 49 & 36 & 9 & 14 & 2 & 12 & 12 & 58 \\ 24 & 15 & 10 & 39 & 19 & 50 & 6 & 29 \\ 14 & 22 & 4 & 39 & 13 & 34 & 57 & 9 \\ 39 & 43 & 19 & 17 & 4 & 5 & 24 & 41 \end{bmatrix} \tag{A1}$$

The B^2 matrix is represented as

$$\begin{bmatrix} 11 & 2 & 60 & 27 & 4 & 33 & 7 & 48 \\ 4 & 17 & 43 & 33 & 12 & 17 & 52 & 14 \\ 37 & 36 & 24 & 42 & 5 & 32 & 13 & 3 \\ 28 & 53 & 20 & 13 & 2 & 5 & 32 & 39 \\ 35 & 4 & 59 & 34 & 12 & 35 & 7 & 6 \\ 31 & 60 & 3 & 4 & 2 & 5 & 25 & 62 \\ 47 & 24 & 3 & 61 & 9 & 28 & 11 & 9 \\ 46 & 10 & 28 & 64 & 4 & 11 & 27 & 2 \end{bmatrix} \tag{A2}$$

The B^3 matrix is represented as

$$\begin{bmatrix} 31 & 48 & 9 & 4 & 2 & 5 & 58 & 35 \\ 48 & 2 & 61 & 8 & 24 & 6 & 10 & 33 \\ 44 & 1 & 31 & 5 & 4 & 62 & 62 & 36 \\ 9 & 64 & 63 & 18 & 5 & 13 & 13 & 12 \\ 19 & 30 & 11 & 38 & 16 & 49 & 49 & 17 \\ 18 & 27 & 35 & 36 & 8 & 1 & 1 & 57 \\ 40 & 25 & 2 & 11 & 1 & 57 & 57 & 50 \\ 1 & 8 & 56 & 1 & 57 & 25 & 25 & 33 \end{bmatrix} \tag{A3}$$

The B^4 matrix is represented as

$$\begin{bmatrix} 42 & 30 & 21 & 33 & 62 & 6 & 1 & 61 \\ 16 & 19 & 28 & 56 & 62 & 7 & 19 & 49 \\ 64 & 11 & 22 & 18 & 39 & 26 & 54 & 22 \\ 43 & 18 & 24 & 45 & 31 & 18 & 40 & 37 \\ 64 & 17 & 6 & 43 & 57 & 40 & 1 & 28 \\ 56 & 32 & 22 & 37 & 26 & 9 & 64 & 10 \\ 38 & 17 & 49 & 26 & 26 & 6 & 50 & 44 \\ 48 & 56 & 10 & 41 & 11 & 48 & 12 & 30 \end{bmatrix} \tag{A4}$$

The B^5 matrix is represented as

$$\begin{bmatrix} 51 & 44 & 9 & 10 & 63 & 50 & 25 & 4 \\ 54 & 46 & 27 & 27 & 11 & 6 & 33 & 52 \\ 28 & 54 & 42 & 33 & 5 & 8 & 54 & 32 \\ 32 & 3 & 53 & 48 & 16 & 10 & 43 & 51 \\ 46 & 26 & 47 & 59 & 10 & 9 & 12 & 47 \\ 22 & 51 & 63 & 12 & 3 & 18 & 36 & 51 \\ 62 & 2 & 39 & 29 & 43 & 52 & 23 & 6 \\ 55 & 63 & 26 & 17 & 10 & 39 & 26 & 20 \end{bmatrix} \tag{A5}$$

Acknowledgments We would like to thank the anonymous reviewers for their valuable comments. This work was supported by Special Project for International Cooperation in Science and Technology of Qinghai Province. (No. 202402050039)

Declarations

- Conflict of interest The authors declare that they have no conflict of interest.

References

[1] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. Preprint at http://arxiv.org/abs/1510.05836 (2015)

[2] Pirandola, S., Andersen, U.L., Banchi, L., *et al.*: Advances in quantum cryptography. Adv. Opt. Photonics **12**(4), 1012–1236 (2020)

[3] Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10-19 December.pp.175–179 (1984)

[4] Bai, C.M., Zhang, S.J., Liu, L.: Quantum secret sharing based on quantum information masking. Quantum Inf. Process. **21**(11), 377 (2022)

[5] Li, F.L., Hu, H., Zhu, S.X., *et al.*: A verifiable (k,n)-threshold dynamic quantum secret sharing scheme. Quantum Inf. Process. **21**(7), 259 (2022)

[6] Xin, X.J., Ding, L., Li, C.Y., *et al.*: Quantum public-key designated verifier signature. Quantum Inf. Process. **21**(1), 33 (2022)

[7] Huang, X.J., Li, Z.Z., Li, Z.C., *et al.*: Quantum signature scheme based on secret sharing. Int. J. Theor. Phys. **61**(6), 180 (2022)

[8] Mor, T., Shapira, R., Shemesh, G.: Digital signatures with quantum candies. Entropy **24**(2), 207 (2022)

[9] Wang, X.B., Yu, Z.W., Hu, X.L.: Twin-field quantum key distribution with large misalignment erro. Phys. Rev. A **98**(6), 062323 (2018)

[10] Bera, S., Gupta, S., Majumdar, A.S.: Device-independent quantum key distribution using random quantum states. Quantum Inf. Process. **22**(2), 109 (2023)

[11] Sheng, Y.B., Zhou, L., Long, G.L.: One-step quantum secure direct communication. Sci. Bull. **67**(4), 367–374 (2022)

[12] Hong, Y.P., Zhou, L., Zhong, W., *et al.*: Measurement-device-independent three-party quantum secure direct communication. Quantum Inf. Process. **22**(2), 111 (2023)

[13] Gottesman, D., Chuang, I.: Quantum digital signatures. Preprint at https://arxiv.org/abs/quant-ph/0105032v2 (2001)

[14] Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2001)

[15] Li, Q., Chan, W.H., Long, D.Y.: Arbitrated quantum signature scheme using bell states. Phys. Rev. A **79**(5), 054307 (2009)

[16] Zou, X., Qiu, D.: Arbitrated quantum signature scheme using bell states. Phys. Rev. A **82**(4), 042325 (2010)

[17] Yang, Y.G., Zhou, Z., Teng, Y.W., *et al.*: Arbitrated quantum signature with an untrusted arbitrator. Eur. Phys. J. D **61**(3), 773–778 (2011)

[18] Zou, X.F., Qiu, D.W., Mateus, P.: Security analyses and improvement of arbitrated quantum signature with an untrusted arbitrator. Int. J. Theor. Phys. **52**(9), 3295–3305 (2013)

[19] Zhang, J.L., Zhang, J.Z., Xie, S.C.: Improvement of a quantum proxy blind signature scheme. Int. J. Theor. Phys. **57**(6), 1612–1621 (2018)

[20] Jiang, D.H., Hu, Q.Z., Liang, X.Q., *et al.*: A novel quantum multi-signature protocol based on locally indistinguishable orthogonal product states. Quantum Inf. Process. **18**(9), 268 (2019)

[21] He, Q., Xin, X., Yang, Q.: Security analysis and improvement of a quantum multi-signature protocol. Quantum Inf. Process. **20**(1), 26 (2021)

[22] Lu, D.J., Li, Z.H., Yu, J., *et al.*: A verifiable arbitrated quantum signature scheme based on controlled quantum teleportation. Entropy **24**(1), 111 (2022)

[23] Gao, M.Z., Yang, W., Liu, Y.: A novel quantum (t, n) threshold group signature based on d-dimensional quantum system. Quantum Inf. Process. **20**(9), 288 (2021)

[24] Huang, Y.F., Xu, G.X., Song, X.L.: An improved efficient identity-based quantum signature scheme. Quantum Inf. Process. **22**(1), 36 (2022)

[25] Deng, Z.M., Lu, D.J., Chen, T., *et al.*: Quantum (t, m, n) threshold group blind signature scheme with flexible number of participants. Int. J. Theor. Phys. **62**, 201 (2023) https://doi.org/10.1007/s10773-023-05449-y

[26] Lou, X.P., Tang, W.S., Long, H., *et al.*: A quantum blind signature scheme based

on block encryption and quantum fourier transfer. Int. J. Theor. Phys. **58**(10), 3192–3202 (2019)

[27] Lou, X.P., Wang, Y., Long, H., *et al.*: Sequential quantum multiparty signature based on quantum fourier transform and chaotic system. Ieee Access **8**, 13218–13227 (2020) https://doi.org/10.1109/ACCESS.2020.2966255

[28] Zhu, H.F., Zhang, Y.L., Li, Z.X.: Efficient quantum blind signature scheme based on quantum fourier transform. Int. J. Theor. Phys. **60**(6), 2311–2321 (2021)

[29] Fan, T.T., Lu, D.J., You, M.G., *et al.*: Multi-proxy signature scheme using five-qubit entangled state based on controlled quantum teleportation. Int. J. Theor. Phys. **61**(12), 273 (2022)

[30] Lin, Q., Li, J., Huang, Z.A., *et al.*: A short linearly homomorphic proxy signature scheme. Ieee Access **6**, 12966–12972 (2018) https://doi.org/10.1109/ACCESS.2018.2809684

[31] Chang, J.Y., Ji, Y.Y., Shao, B.L., *et al.*: Certificateless homomorphic signature scheme for network coding. Ieee Acm T. Network. **28**(6), 2615–2628 (2021)

[32] Rivest, L.R.: Two signature schemes. http://people.csail.mit.edu/rivest/pubs.html (2000)

[33] Johnson, R., Molnar, D., Song, D., et al.: Homomorphic signature schemes. In: Topics in Cryptology—CTRSA 2002. Springer Berlin Heidelberg, 2002: 244–262 (2002)

[34] Shang, T., Zhao, X.J., Wang, C., *et al.*: Quantum homomorphic signature. Quantum Inf. Process. **14**(1), 393–410 (2015)

[35] Luo, Q.B., Yang, G.W., She, K., *et al.*: Quantum homomorphic signature based on bell-state measurement. Quantum Inf. Process. **15**(12), 5051–5061 (2016)

[36] Chen, T., Lu, D.J., Deng, Z.M., *et al.*: A quantum homomorphic signature scheme with verifiable identity based on four-particle cluster states. Laser Phys. Lett. **20**(10), 105205 (2023)

[37] Mei, Q., Xiong, H., Chen, J.H., *et al.*: Efficient certificateless aggregate signature with conditional privacy preservation in iov. Ieee Syst. J. **15**(1), 245–256 (2021)

[38] Hwang, Y.W., Lee, I.Y.: A lightweight certificate-based aggregate signature scheme providing key insulation. Cmc-Comput. Mater. Con. **69**(2), 1747–1764 (2021)

[39] Boneh, D., Gentry, C., Lynn, B., et al.: Aggregate and verifiably encrypted signatures from bilinear maps. International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt 2003), Warsaw, Poland, 4–8 May 1978

(2003)

[40] You, M.G., Lu, D.J., Fan, T.T., *et al.*: A quantum aggregate signature scheme based on quantum teleportation using four-qubit cluster state. Int. J. Theor. Phys. **61**(6), 155 (2022)

[41] Cai, D.Q., Chen, X., Han, Y.H., *et al.*: Implementation of an e-payment security evaluation system based on quantum blind computing. Int. J. Theor. Phys. **59**(9), 2757 (2020)

[42] Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Math. Struct. in Comp. Sci. **17**(6), 1115–1115 (2002)

[43] Shor, P.W., Preskill, J.: Simple proof of security of the bb84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)

[44] Jeong, Y.C., Ji, S.W., Hong, C., *et al.*: Deterministic secure quantum communication on the bb84 system. Entropy **22**(11), 1268 (2020)

[45] Yang, H.Y., Ye, T.Y.: Secure multi-party quantum summation based on quantum fourier transform. Quantum Inf. Process. **17**(6), 129 (2018)

[46] Cabello, A.: Quantum key distribution in the holevo limit. Phys. Rev. Lett. **85**(26), 5635–5638 (2000)