

Quantum homomorphic broadcast multi-signature based on homomorphic aggregation

Xin Xu(徐鑫) and Ai-Han Yin(殷爱菡)

Citation: Chin. Phys. B, 2023, 32 (**7**): 070302. DOI: 10.1088/1674-1056/acac0e
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Faithful and efficient hyperentanglement purification for spatial-polarization-time-bin photon system

Fang-Fang Du(杜芳芳), Gang Fan(樊钢), Yi-Ming Wu(吴一鸣), and Bao-Cang Ren(任宝藏)
Chin. Phys. B, 2023, 32 (**6**): 060304. DOI: 10.1088/1674-1056/aca395

Nearly invariant boundary entanglement in optomechanical systems

Shi-Wei Cui(崔世威), Zhi-Jiao Deng(邓志姣), Chun-Wang Wu(吴春旺), and Qing-Xia Meng(孟庆霞)
Chin. Phys. B, 2021, 30 (**11**): 110311. DOI: 10.1088/1674-1056/ac16ca

Chaotic dynamics of complex trajectory and its quantum signature

Wen-Lei Zhao(赵文垒), Pengkai Gong(巩膨恺), Jiaozi Wang(王骄子), and Qian Wang(王骞)
Chin. Phys. B, 2020, 29 (**12**): 120302. DOI: 10.1088/1674-1056/abc0dc

Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states

Yan-Yan Feng(冯艳艳), Rong-Hua Shi(施荣华), Ying Guo(郭迎)
Chin. Phys. B, 2018, 27 (**2**): 020302. DOI: 10.1088/1674-1056/27/2/020302

Enhanced arbitrated quantum signature scheme using Bell states

Wang Chao (王朝), Liu Jian-Wei (刘建伟), Shang Tao (尚涛)
Chin. Phys. B, 2014, 23 (**6**): 060309. DOI: 10.1088/1674-1056/23/6/060309

Quantum homomorphic broadcast multi-signature based on homomorphic aggregation

Xin Xu(徐鑫) and Ai-Han Yin(殷爱菡)†

Department of Information Engineering, East China JiaoTong University, Nanchang 330013, *China*

(Received 23 September 2022; revised manuscript received 3 December 2022; accepted manuscript online 16 December 2022)

Quantum multi-signature has attracted extensive attention since it was put forward. Beside its own improvement, related research is often combined with other quantum signature. However, this type of quantum signature has one thing in common, that is, the generation and verification of signature depend heavily on the shared classical secret key. In order to increase the reliability of signature, the homomorphic aggregation technique is applied to quantum multi-signature, and then we propose a quantum homomorphic multi-signature protocol. Unlike previous quantum multi-signature protocols, this protocol utilizes homomorphic properties to complete signature generation and verification. In the signature generation phase, entanglement swapping is introduced, so that the individual signatures of multiple users are aggregated into a new multi-signature. The original quantum state is signed by the shared secret key to realize the verification of the signature in the verification phase. The signature process satisfies the homomorphic property, which can improve the reliability of the signature.

Keywords: quantum signature, homomorphic aggregation, homomorphic multi-signature, Bell state

PACS: 03.67.–a, 03.67.Ac, 03.67.Bg, 03.67.Hk **DOI:** 10.1088/1674-1056/acac0e

1. Introduction

As an extension of handwritten signatures in the digital field, digital signatures are now used in daily life. Since modern computers cannot solve such problems in polynomial time, the security of signatures relies on mathematically complex puzzles in classical cryptography. However, since the Shor quantum parallel algorithm[1] solved RSA encryption problem in a limited time in 1994, the security of digital signatures has begun to shake. In order to improve the security of digital signatures, many researchers have begun to use quantum properties to study how to ensure signature security, which opens the door of quantum signature.

In 1984, Bennett and Brassard[2] proposed the first quantum key distribution protocol. Quantum key distribution is the premise of other quantum protocols, one of which is quantum signature. Its purpose is to enable communication parties to generate a secure key for processing messages. Although the research of quantum key distribution set up early, there are still many scholars to enrich the content of this field now. For example, Wang *et al.*[3] proposed twin-field quantum key distribution over 830-km fibre and made a breakthrough in the establishment of ground-based quantum security networks on a scale of 1000 km, and Fan-Yuan *et al.*[4,5] proposed that all contributes to the development of quantum cryptography.

Quantum signature is an important research direction in quantum cryptography. One of its important characteristics is that its security completely changes the traditional digital signature's dependence on difficult mathematical assumptions, that is, the security of quantum signature depends on the basic principles of quantum mechanics, such as uncertainty principle and non-cloning theorem. So, in theory, a secure quantum signature could deal with a quantum computer attack. Because of these security characteristics of quantum signature, the related research has received much attention.[6–8] In recent years, the research on quantum signature has made new progress, such as efficient quantum digital signatures without symmetrization step proposed by Lu *et al.*,[9] which improves the signature rate of the protocol; secure and practical multiparty quantum digital signatures proposed by Weng *et al.*,[10] which improves the data utilization rate; and experimental quantum secure network with digital signatures and encryption proposed by Yin *et al.*,[11] which combines quantum signature with network and expands the research scope of quantum signature.

Quantum multi-signature is a branch of quantum signature, which is widely used in e-commerce, property division, fund management and other scenarios.[12–14] It is characterized by multiple signers signing the same message, and according to the different signature orders that can be divided into ordered signature and broadcast signature: these two modes have their own advantages and disadvantages. Both models have advantages and disadvantages. In 2007, Wen *et al.*[15] firstly proposed a realizable quantum ordered multiple digital signature scheme based on classical multiple signatures, which relies on quantum key distribution and one-time pad algorithm to ensure the security of the protocol. Then, they[16] proposed a quantum digital multi-signature using controlled quantum teleportation for multi-signature and does not

†Corresponding author. E-mail: yinaihan@126.com

© 2023 Chinese Physical Society and IOP Publishing Ltd

rely on an arbitrator to verify the signature. In the same year, Wen *et al.*[17] proposed two quantum broadcast multi-signature protocols, one for classical digital message, which uses quantum unidirectional function to realize signature and verification, and the other for quantum message, which uses quantum teleportation technology. In 2016, Du *et al.*[18] proposed an efficient quantum ordered multi-signature protocol, which also uses quantum key distribution and one-time pad algorithm, but only needs to perform unitary operations on single particles to complete the signature instead of multi-particle entangled state. In 2019, Jiang *et al.*[19] proposed a novel quantum multi-signature protocol based on locally indistinguishable orthogonal product states, which ensures information security with fewer decoy particles during transmission. In 2021, He *et al.*[20] analyzed the security of some quantum multi-signature protocols that have been used so far and proposed related improvements. This shows that the research on quantum multi-signature is slow but still ingoing.[21,22]

Quantum multi-signature protocols are also often combined with other signature protocols. In 2019, Qin *et al.*[23] proposed an efficient quantum multi-proxy signature protocol, in which the rights of the original signer are assigned to multiple proxy signers, that is, a single signature becomes multiple proxy signatures. In the same year, Zhang *et al.*[24] proposed a novel quantum broadcasting multiple blind signature scheme based on partial entanglement of multiple particles. With the deepening of the research, the research on the application in the signature protocol is also conducted. In 2017, Shao *et al.*[25] proposed an electronic payment protocol based in quantum multi-agent blind signature. In 2018, Niu *et al.*[26] improved the Shao *et al.*'s protocol and proposed a practical quantum multi-agent blind signature electronic payment protocol.

Quantum homomorphic signature has been proposed in recent year, which is the extension of homomorphic signature in quantum field. In 2015, Shang *et al.*[27] proposed a quantum homomorphic signature protocol for the first time, which uses entanglement swapping to complete signature aggregation. This protocol solves the problem of multi-stream identity authentication in quantum signature, effectively ensures the security of key, and verifies the identities of different data sources in quantum network. In 2016, Luo *et al.*[28] also proposed a quantum homomorphic signature protocol. Unlike Shang's protocol, this protocol is based on signature aggregation of Bell state measurement. In 2017, Li *et al.*[29] thought of a new idea from the spectral characteristics, and proposed a quantum homomorphic signature scheme by using the continuous variable part of the quantum spectrum. This scheme uses continuous-variable quantum information and transmits more information at lower cost. In 2019, Shang *et al.*[30] introduced a serial verification model and a parallel verification model, and proposed a new quantum homomorphic signature protocol with repeatable verification. The serial model handles the signature verification problem, and the parallel verification model handles the signature repetition problem. This protocol is beneficial to signature verification in general scenarios.

These quantum homomorphic signatures are based on the signature model proposed by Shang *et al.*[27] In this model, the message holder and the signer are played by the same person, which can authenticate the identities of different data sources. However, this setting also limits the application scenarios of quantum homomorphic signatures. To broaden its application scope, we introduce quantum multi signatures, and also improve the shortcomings of traditional quantum multi signatures through quantum homomorphic signatures. Quantum multi signature is a common signature. It needs to convert classical messages into quantum sequences. Therefore, it needs to prepare multiple quantum states, leading to a long initialization phase. In addition, in the verification phase, it only relies on the classical bit key. If the key is stolen, it is easy to forge the signature and pass the verification.

In this paper, we apply homomorphic aggregation to quantum multi-signature, and propose a quantum homomorphic multi-signature protocol, which uses homomorphic property to complete the generation and verification of signature. This method not only broadens the application scope of quantum homomorphic signature, but also improves quantum multi signature, so that it only needs to prepare a quantum state, reducing the preparation time, and requires quantum sequences and classical keys when verifying signatures, making attackers unable to pass the verification when they only have the key. We mainly introduce the following aspects. First, we introduce the basic knowledge related to quantum signatures, then we introduce the proposed scheme in detail, and finally analyze the proposed scheme.

2. Related works

2.1. Quantum homomorphic signature

Quantum homomorphic signature is a quantum signature with homomorphic properties, or an extension of a homomorphic signature in a quantum field, and the generation and verification of signatures are realized by using the homomorphic properties. From the calculation method, we can divide homomorphism into additive homomorphism and multiplicative homomorphism. Suppose that there are two inputs Y_1 and Y_2, if there is a function f that satisfies $\rho(Y_1+Y_2) = f(\rho(Y_1),\rho(Y_2))$, then the function ρ will be additively homomorphic. Similarly, the function ρ is multiplicative homomorphic when the function f conforms to $\rho(Y_1 \times Y_2) = f(\rho(Y_1),\rho(Y_2))$.

Homomorphic signature schemes are mainly divided into

five types: linear homomorphism, polynomial function homomorphism, full homomorphism, homomorphic aggregation, and multi-key homomorphism.[31,32] Among them, homomorphic aggregation is different from other schemes, it can solve multi-user application scenarios. In this type of scenario, the generated signatures are aggregated from the signatures corresponding to different messages, which are signed by different users, and each user has its own secret key.

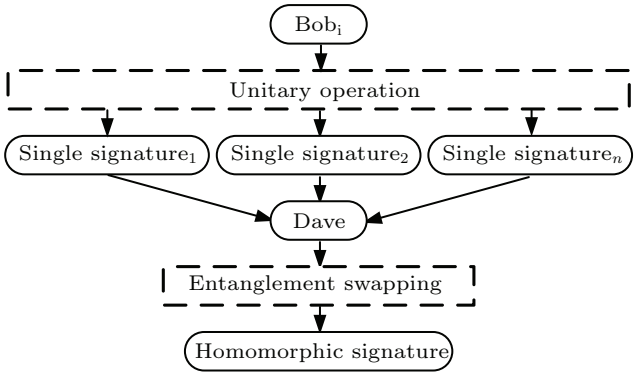


Fig. 1. Homomorphic aggregation.

Entanglement swapping is a property of quantum state,[33–35] it can be used to achieve homomorphic aggregation in the field of quantum signatures. Assume that there are two Bell states, $|\phi^+\rangle_{12}$ and $|\phi^+\rangle_{34}$. The Bell state measurement is performed on particle 1 and particle 3, so that the two particles that are not originally entangled are entangled together, becoming Bell state $|\varphi\rangle_{13}$, and the other two particles collapse into $|\varphi\rangle_{24}$. The specific quantum states of these two pairs of new Bell states are as follows:

$$\begin{aligned}|\phi^+\rangle_{12}\otimes|\phi^+\rangle_{34} = \frac{1}{2}\big(&|\phi^+\rangle_{13}|\phi^+\rangle_{24}+|\phi^-\rangle_{13}|\phi^-\rangle_{24}\\ &+|\psi^+\rangle_{13}|\psi^+\rangle_{24}+|\psi^-\rangle_{13}|\psi^-\rangle_{24}\big).\end{aligned} \quad (1)$$

Here is just one of entanglement swapping of Bell state.

2.2. Quantum multi-signature

Quantum multi-signature can be divided into two types according to the signature order of the signers, namely quantum broadcast multi-signature and quantum ordered multi-signature.

In quantum broadcast multi-signature,[36] the issuer sends the message to be signed to each signer out of order; each signer sends the message and corresponding signature to the collector after completing the signature; the collector verifies each individual signature and then aggregates them into a multi-signature and sends it to the verifier; finally, the verifier verifies the validity of the multi-signature. The advantage of this is that the signers will not contact each other's information, and the signature does not need to wait. After the signature is completed, it can be directly sent to the collector. However, the disadvantage is that the multi signature work is completed by one node, which needs to have high credibility and strong processing capability.

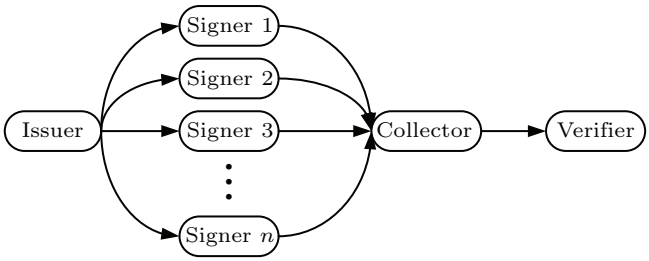


Fig. 2. Quantum broadcast multi-signature.

In an ordered multi-signature scheme,[37,38] the issuer specifies the order of the signers' signature, and then sends the message to the first signer. Except the first signer, each signer verifies the validity of the previous signature after receiving it, if the signature is valid, the signer continues to sign, and then sends the signature to the next signer; otherwise, it would reject the signature and terminates the entire process. Until all signers complete the signing operation, the signed message is sent to the verifier. Finally, the verifier verifies the validity of the multi-signature. The advantage of this approach is that when problems occur in the signature, they can be found in a timely manner and will not accumulate errors to the final verifier. However, the disadvantage is that previous signature will be received by the subsequent signers, which may cause attacks between signers. In addition, the subsequent signers need to wait for the previous signer to complete the signature before signing, resulting in a long overall time.

It can be seen that quantum homomorphic signature and quantum broadcast multi signature have a high degree of consistency in the signature model.

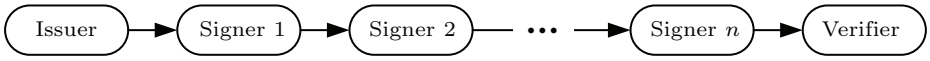


Fig. 3. Quantum ordered multi-signature.

3. Proposed protocol

In this section, we propose a quantum homomorphic multi-signature scheme based on homomorphic aggregation in detail. The scheme consists of four stages, namely initialization, signing, aggregation and verification. There are four kinds of participants, namely Alice who holds the message to be signed, Bob who is responsible for signing, Dace who

aggregates signatures, and Charlie who verifies the signature. The flow chart of this scheme is shown in Fig. 4.

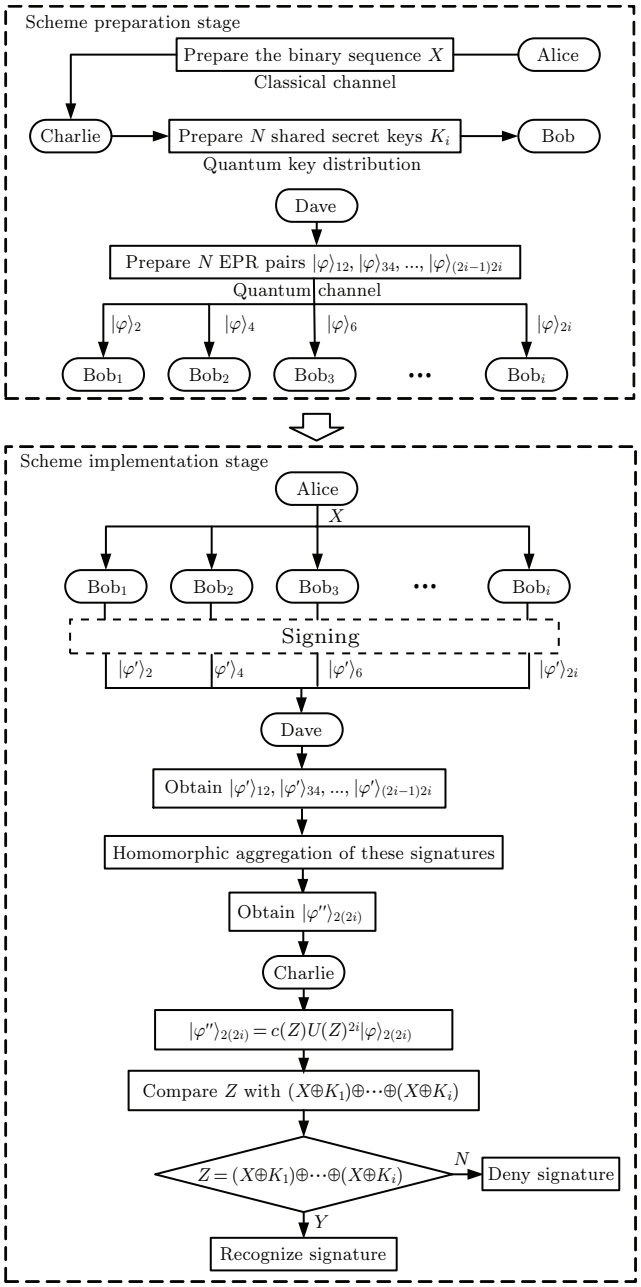


Fig. 4. Scheme flow chart.

(i) Initialization

Step 1 Alice converts the message to be signed into a binary sequence. Here, we limit the length of the binary sequence to 2, which is a special value in order to better introduce the details of the scheme and avoid the redundancy of content. It does not affect the universality of the scheme. The resulting binary sequence is named X and send to Charlie in advance.

Step 2 According to the length of the binary sequence X owned by Alice, Charlie prepares three classical bits of the same length (denoted as K_i), and shares them with Bob_i by quantum key distribution protocol, these are secret keys shared between Bob_i and Charlie, here $K_i \in \{00, 01, 10, 11\}$.

Step 3 Dave prepares three EPR entangled pairs:

$$\left|\phi^+\right\rangle_{12} = \frac{1}{\sqrt{2}}\left(|0_1 0_2\rangle + |1_1 1_2\rangle\right), \tag{2}$$

$$\left|\phi^+\right\rangle_{34} = \frac{1}{\sqrt{2}}\left(|0_3 0_4\rangle + |1_3 1_4\rangle\right), \tag{3}$$

$$\left|\phi^+\right\rangle_{56} = \frac{1}{\sqrt{2}}\left(|0_5 0_6\rangle + |1_5 1_6\rangle\right). \tag{4}$$

(ii) Signing

Step 1 Dave takes one particle from each of the three entangled EPR pairs, here we choose particle 2, particle 4 and particle 6, which can be denoted as $|\varphi\rangle_2$, $|\varphi\rangle_4$, $|\varphi\rangle_6$, respectively. Then Dave sends these particles to Bob_1, Bob_2, and Bob_3 respectively. At the same time, Alice also sends the binary sequence X to Bob_i.

Step 2 After Bob_i receives the binary sequence X and particles from Alice, he performs an exclusive OR operation on the binary sequence X and the secret key K_i he holds, and the result $X \oplus K_i$ is used to sign the received particle $2i$.

Here, the unitary operator used in the particle signature corresponds to the exclusive OR result $X \oplus K_i$, and the corresponding relationship is as follows:

$$X \oplus K_i = 00 \to I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{5}$$

$$X \oplus K_i = 01 \to \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{6}$$

$$X \oplus K_i = 10 \to \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{7}$$

$$X \oplus K_i = 11 \to -\mathrm{i}\sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{8}$$

Step 3 Bob_i sends the transformed particle $2i$, namely $|\varphi'\rangle_{2i}$, and the exclusive OR result $X \oplus K_i$ to Dave. Here, the superscript $(')$ indicates that the particle or quantum state completes the signature operation.

(iii) Aggregation

After Bob_i completes the signature of particle $2i$ with the exclusive OR result $X \oplus K_i$, the original three EPR entangled pairs would change, the states of these would be $|\varphi'\rangle_{12} = U(X \oplus K_1)^{(2)} \cdot |\phi^+\rangle_{12}$, $|\varphi'\rangle_{34} = U(X \oplus K_2)^{(4)} \cdot |\phi^+\rangle_{34}$, $|\varphi'\rangle_{56} = U(X \oplus K_3)^{(6)} \cdot |\phi^+\rangle_{56}$. These transformed EPR entangled pairs are Bob_i's signatures.

Then, Dave combines these individual signatures $|\varphi'\rangle_{(2i-1)(2i)}$ received from Bob_i to generate an aggregated signature. The generation process of the aggregated signature is as follows.

Step 1 Dave would aggregate the signature of Bob_2 and Bob_3. The way to aggregate is to perform an entanglement swapping on quantum states $|\varphi'\rangle_{34}$ and $|\varphi'\rangle_{56}$. First, Dave performs a Bell state measurement on particle 3 and particle 5 in these two quantum states, then, we obtain an entangled

pair $|\varphi''\rangle_{35}$. This measurement enables two unentangled particles to become entangled. According to the entanglement exchange principle, the remaining non-entangled particles 4 and 6 would collapse into a pair of entangled states $|\varphi''\rangle_{46}$. Here, $|\varphi''\rangle_{46}$ would be the combined signature of Bob_2 and Bob_3, and the superscript ($''$) indicates that the particle or quantum state completes the two operations of signature and entanglement swapping.

Step 2 Dave performs an entanglement swapping on $|\varphi'\rangle_{12}$ and $|\varphi''\rangle_{46}$ to connect the combined signature of Bob_2 and Bob_3 and the signature of Bob_1. According to the procedure in Step 1, we can easily obtain the state of particle 1 and particle 4 after measurement which is $|\varphi''\rangle_{14}$. Similarly, the state of the particles 2 and 6 would collapse into $|\varphi''\rangle_{26}$. The $|\varphi''\rangle_{26}$ would be the signature of Dave.

Step 3 Dave performs exclusive OR operation on each signer's signature information $X\oplus K_i$, and obtains $(X\oplus K_1)\oplus(X\oplus K_2)\oplus(X\oplus K_3)$.

Step 4 Dave sends the signature information $(X\oplus K_1)\oplus(X\oplus K_2)\oplus(X\oplus K_3)$ and $|\varphi''\rangle_{26}$ to Charlie.

(iv) Verification

Charlie receives quantum states $|\varphi''\rangle_{26}$ and $(X\oplus K_1)\oplus(X\oplus K_2)\oplus(X\oplus K_3)$ from Dave, and can use this information to verify the signature. The verification process is as follows.

Step 1 After Charlie receives quantum state $|\varphi''\rangle_{26}$ from Dave, he performs a Bell state measurement on the particles in $|\varphi''\rangle_{26}$ to obtain the state of the quantum state $|\varphi''\rangle_{26}$, and then compares the measurement result $|\varphi''\rangle_{26}$ with the initial quantum state $|\varphi\rangle_{26}$ in order to find an operator that satisfies the formula $|\varphi''\rangle_{26}=c(Z)U(Z)^6\cdot|\varphi\rangle_{26}$. In the formula, the subscript "6" means operating on particle 6, and $|c(Z)|=1$.

Step 2 Charlie compares $(X\oplus K_1)\oplus(X\oplus K_2)\oplus(X\oplus K_3)$ with Z. If $(X\oplus K_1)\oplus(X\oplus K_2)\oplus(X\oplus K_3)=Z$, Charlie would confirm that $|\varphi''\rangle_{26}$ is the signature of Dave. Otherwise, Charlie would deny the signature.

4. Scheme analysis

In this section, we analyze the proposed protocol from three aspects, namely homomorphic properties, security analysis and comparison.

4.1. Homomorphic property

We refer to two proven lemmas in Ref. [27] to demonstrate the homomorphic properties of our proposed scheme. The representation of these lemmas is as follows.

Lemma 1 $U(Y_1)\cdot U(Y_2)\cdot|\varphi\rangle=c(Y_1,Y_2)\cdot U(Y_1\oplus Y_2)\cdot|\varphi\rangle$, where $Y_1,Y_2\in\{00,01,10,11\}\,|c(Y_1,Y_2)|=1$.

Note that $U(Y_1)$ and $U(Y_2)$ represent the unitary operators corresponding to secret keys Y_1 and Y_2, and $|c(Y_1,Y_2)|=1$ is a factor that only affects the phase, so it can be ignored after the Bell state measurement.

Lemma 2 $U_1^{(1)}\cdot U_2^{(2)}\cdot|\varphi\rangle_{12}=c_j\cdot(U_1\cdot U_2)^{(2)}\cdot|\varphi\rangle_{12}\,|c_j|=1$, where $U_1U_2\in\{I,\sigma_x,\sigma_y,-\mathrm{i}\sigma_z\}$, $|\varphi\rangle_{12}\in\{|\phi^+\rangle,|\phi^-\rangle,|\psi^+\rangle,|\psi^-\rangle\}$.

Note that $U_1^{(1)}$ and $U_2^{(2)}$ are unitary operators that operate on particles 1, 2 in $|\varphi\rangle_{12}$, and $|c_j|=1$ is also a phase factor.

As can be seen from the aggregation phase of the signature, the signature of Bob_i is $|\varphi'\rangle_{2i}=U(X\oplus K_i)^{(2i)}\cdot|\varphi\rangle_{2i}$. Then, Dave receives these signatures and first aggregates the signatures of Bob_2 and Bob_3, *i.e.*, $|\varphi'\rangle_{34}\oplus|\varphi'\rangle_{56}\to|\varphi''\rangle_{3456}$.

$$\begin{aligned}|\varphi''\rangle_{3456}&=|\varphi'\rangle_{34}\otimes|\varphi'\rangle_{56}\\&=U(X\oplus K_2)^4|\phi^+\rangle_{34}\otimes U(X\oplus K_3)^6|\phi^+\rangle_{56}\\&=\frac{1}{2}U(X\oplus K_2)^4U(X\oplus K_3)^6\big(|0000\rangle_{3456}\\&\quad+|0011\rangle_{3456}+|1100\rangle_{3456}+|1111\rangle_{3456}\big)\\&=\frac{1}{2}U(X\oplus K_2)^4U(X\oplus K_3)^6\big(|\phi^+\rangle_{35}|\phi^+\rangle_{46}\\&\quad+|\phi^-\rangle_{35}|\phi^-\rangle_{46}+|\psi^+\rangle_{35}|\psi^+\rangle_{46}\\&\quad+|\psi^-\rangle_{35}|\psi^-\rangle_{46}\big).\end{aligned}\tag{9}$$

Bringing Lemma 2 into the above formula, the resulting equation is obtained as follows:

$$\begin{aligned}&|\varphi''\rangle_{3456}\\&=\frac{1}{2}\big[\big(|\phi^+\rangle_{35}\big)\big(c_jU(X\oplus K_2)^6U(X\oplus K_3)^6|\phi^+\rangle_{46}\big)\\&\quad+\big(|\phi^-\rangle_{35}\big)\big(c_jU(X\oplus K_2)^6U(X\oplus K_3)^6|\phi^-\rangle_{46}\big)\\&\quad+\big(|\psi^+\rangle_{35}\big)\big(c_jU(X\oplus K_2)^6U(X\oplus K_3)^6|\psi^+\rangle_{46}\big)\\&\quad+\big(|\psi^+\rangle_{35}\big)\big(c_jU(X\oplus K_2)^6U\big(X\oplus K_3\big)^6|\psi^+\rangle_{46}\big)\big].\end{aligned}\tag{10}$$

Then bring Lemma 1 into the above formula. the resulting equation is below:

$$\begin{aligned}&|\varphi''\rangle_{3456}\\&=\frac{1}{2}\big[\big(|\phi^+\rangle_{35}\big)\big(c_jc(U_2,U_3)U(X\oplus K_2\oplus X\oplus K_3)^6|\phi^+\rangle_{46}\big)\\&\quad+\big(|\phi^-\rangle_{35}\big)\big(c_jc(U_2,U_3)U(X\oplus K_2\oplus X\oplus K_3)^6|\phi^-\rangle_{46}\big)\\&\quad+\big(|\psi^+\rangle_{35}\big)\big(c_jc(U_2,U_3)U(X\oplus K_2\oplus X\oplus K_3)^6|\psi^+\rangle_{46}\big)\\&\quad+\big(|\psi^-\rangle_{35}\big)\big(c_jc(U_2,U_3)U(X\oplus K_2\oplus X\oplus K_3)^6|\psi^-\rangle_{46}\big)\big].\end{aligned}\tag{11}$$

Comparing the above formula with

$$\begin{aligned}|\phi^+\rangle_{35}\oplus|\phi^+\rangle_{46}=\frac{1}{2}\big(&|\phi^+\rangle_{35}|\phi^+\rangle_{46}+|\phi^-\rangle_{35}|\phi^-\rangle_{46}\\&+|\psi^+\rangle_{35}|\psi^+\rangle_{46}+|\psi^-\rangle_{35}|\psi^-\rangle_{46}\big),\end{aligned}$$

we can see that $|\varphi''\rangle_{3456}$ is obtained by the unitary operation on particle 6 in $|\phi^+\rangle_{35}\oplus|\phi^+\rangle_{46}$. Therefore, we obtain that $|\varphi''\rangle_{46}=c(Z)U(Z)^6|\varphi\rangle_{46}$, where $Z=X\oplus K_2\oplus X\oplus K_3$, $c(Z)=c_jc(U_2U_3)$. $|c_jc(U_2,U_3)|=1$ is a phase factor. $|\varphi''\rangle_{46}$ is the aggregate signature of Bob_2 and Bob_3.

Similarly, Dave performs the same operation on $|\phi^+\rangle_{12}$ and $|\varphi''\rangle_{46}$, and we obtain easily that $|\varphi''\rangle_{26}=$

$c(Z)U(Z)^6|\varphi\rangle_{26}$, where $c(Z)=c_jc(U_1,U_2,U_3)$, $Z=X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3$, $|c_jc(U_1,U_2,U_3)|=1$ is a phase factor and $|\varphi''\rangle_{26}$ is the aggregate signature of Bob_1, Bob_2, and Bob_3.

Here, we define that the function of f as the operation of entanglement swapping and the function Sign as the operation of signature.

Thus, the signatures of the signers can be written as follows:

$$\begin{aligned}\text{Sign}(X\oplus K_1) &= |\varphi'\rangle_2 = U(X\oplus K_1)|\varphi\rangle_2 \to |\varphi'\rangle_{12}\\ &= U(X\oplus K_1)^2|\varphi\rangle_{12}, \qquad (12)\\ \text{Sign}(X\oplus K_2) &= |\varphi'\rangle_4 = U(X\oplus K_2)|\varphi\rangle_4 \to |\varphi'\rangle_{34}\\ &= U(X\oplus K_2)^4|\varphi\rangle_{34}, \qquad (13)\\ \text{Sign}(X\oplus K_3) &= |\varphi'\rangle_6 = U(X\oplus K_3)|\varphi\rangle_6 \to |\varphi'\rangle_{56}\\ &= U(X\oplus K_3)^6|\varphi\rangle_{56}. \qquad (14)\end{aligned}$$

Then, collector aggregates these signatures through entanglement swapping, and the result can be written as follows:

$$\begin{aligned}&f[\text{Sign}(X\oplus K_1),\text{Sign}(X\oplus K_2),\text{Sign}(X\oplus K_3)]\\ &= f[\text{Sign}(X\oplus K_1),f[\text{Sign}(X\oplus K_2),\text{Sign}(X\oplus K_3)]]\\ &= |\varphi'\rangle_{12}\otimes|\varphi''\rangle_{46}\\ &= U(X\oplus K_1)^2|\varphi\rangle_{12}\otimes U(X\oplus K_2\oplus X\oplus K_3)^6|\varphi\rangle_{46}\\ &= |\varphi\rangle_{14}\otimes U(X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3)^6|\varphi\rangle_{46}. \qquad (15)\end{aligned}$$

In the above formula,

$$\begin{aligned}&f[\text{Sign}(X\oplus K_1),\text{Sign}(X\oplus K_2),\text{Sign}(X\oplus K_3)]\to|\varphi''\rangle_6\\ &= U(X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3)^6|\varphi\rangle_6.\end{aligned}$$

If the aggregated signature is generated by the information $X_i\oplus Y_i$, then

$$\begin{aligned}&\text{Sign}(X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3)\to|\varphi''\rangle_6\\ &= U(X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3)^6|\varphi\rangle_6.\end{aligned}$$

Thus,

$$\begin{aligned}&f[\text{Sign}(X\oplus K_1),\text{Sign}(X\oplus K_2),\text{Sign}(X\oplus K_3)]\\ &= \text{Sign}(X\oplus K_1\oplus X\oplus K_2\oplus X\oplus K_3).\end{aligned}$$

Compared with the additive homomorphic model $\rho(Y_1+Y_2)=f(\rho(Y_1)\rho(Y_2))$, our signature scheme satisfies the additive homomorphism property.

4.2. Security analysis

We analyze the security of the proposed quantum signature protocol from the following three aspects: verifiability, non-repudiation, and unforgeability. To simplify the model, the participants in the protocol are assumed to be honest.

(I) Verifiability: The verifier can verify the validity of the signature of the corresponding signer through the shared secret key.

In our scheme, there are two signature processes: one is the individual signature generated by the signer and the other is the aggregated signature generated by the collector, and the verifier can verify the validity of both signatures. After the verifier receives the signature sent by the collector, an equation $|\varphi''\rangle_{AB}=c(Z)U(Z)^B|\varphi\rangle_{AB}$ with the initial quantum state is formed, and then Z in the equation is compared with the secret key X_i to verify the validity of the signer's signature. Then, the verifier can ask the collector to send it the quantum state after the entanglement swapping, and can calculate whether the aggregate signature generated by the collector is valid through initial quantum state.

Non-repudiation and unforgeability are important security requirements in a signature scheme. For convenience, we use the examples in this work to illustrate the above two properties.

(II) Non-repudiation: The secret key held by the signer is not only a tool for signing, but also the signer's identity label, so it cannot deny its own signature.

No signer can deny their signatures. The verifier compares the received aggregated signature $|\varphi''\rangle_{26}$ with the initial quantum state, and forms an equation that satisfies the formula $|\varphi''\rangle_{26}=c(Z)U(Z)^6\cdot|\varphi\rangle_{26}$. Assuming that the verifier performs exclusive OR operation on Z and $K_2\oplus K_3$, and the result is K_1, it can prove that the signer Bob_1 has indeed signed and the signature cannot be denied. Here, K_1 is equivalent to a signed label. Note that the verifier needs to process Z according to the number of signers in the above step, if the number is odd, Z is processed as $Z\oplus X$; if it is even, Z is not operated.

(III) Unforgeability: The signer's secret key is obtained from the verifier through the BB84 protocol which proves to be unconditionally secure, and no one else can forge the signature.

The signature cannot be forged. In a signature protocol, the secret key K_i is an important factor in generating the signature, so enhancing the security of the secret key transmission is to enhance the security of the signature. In our signature scheme, the secret key K_i is distributed by the BB84 protocol and the secret key K_i can be safely shared by Bob_i and Charlie, because the key distribution protocol proves to be unconditionally secure. On the other hand, the secret key K_i cannot be calculated from the message and the corresponding signature. Suppose that the Eve steals both particle 2 and $X\oplus K_1$ in the process of the signer sending the information to the collector, he cannot calculate $|\varphi'\rangle_{12}$ without particle 1 or the unitary operation $U(X\oplus K_1)$ with only particle 2. Therefore, attackers cannot steal the secret key K_i of the protocol with only particles $2i$ and $X\oplus K_i$ so that the signature cannot be forged.

4.3. Comparisons

Although quantum multi-signature has been studied for a long time, its research direction is mainly its applications in different signature scenarios, or its combination with other signature protocols. Here, we refer to previous signature protocols related to quantum multi-signature as traditional quantum multi-signature and compare it with our proposed quantum homomorphic multi-signature. We mainly compare the following three aspects, as shown in Table 1.

Table 1. Comparisons of proposed protocol with traditional protocols.

	Traditional quantum multi-signature	Quantum homomorphic multi-signature
Preparation of quantum states	$\|\phi^+\rangle, \|\phi^-\rangle, \|\psi^+\rangle, \|\psi^-\rangle$	$\|\phi^+\rangle$
Signature method	unitary operation	unitary operation and entanglement swapping
Verifiable kind	K_i	X, K_i

In the traditional quantum multi-signature scheme, the message holder first converts the message to be signed into a binary sequence, and then converts it into a quantum sequence. Taking the Bell state used in our paper for example, the message holder needs to prepare four different Bell states. But in our proposed signature scheme, the message holder only needs to convert the message to be signed into a binary sequence, the Bell state is prepared by the collector, and only one Bell state needs to be prepared, which can significantly improve the efficiency of Bell state preparation.

In the signature stage, in the traditional quantum multi-signature scheme, the signer's secret key is used to perform multiple unitary operations on the same quantum state. If the quantum state and related keys are stolen by Eve, the signature may be forged. In our scheme, the signer uses the unitary operation to sign different quantum states, and then uses the entanglement exchange to complete the aggregation of the signatures. Even if Eve steals the relevant information, he cannot obtain the key to forge the signature.

In the verification phase, the verifier only has the secret key shared with the signer. In the traditional multi-signature scheme, it can only verify whether the signer's key is used correctly, but cannot judge whether the signed message is correct. In our scheme, the verifier not only shares the key of the signer, but also has the binary sequence of the message to be signed, which can verify the correctness of the key and the authenticity of the message signed by the signer.

4.4. Tolerable number of dishonest users

In our scheme, the aggregator and the verifier are two important nodes that must be trusted, so dishonesty is assumed to occur to the signer. In the signature scheme, the signer owns the original message and the original key, so there may be two dishonest behaviors: one is to modify the original message, and the other is to modify the original key.

In both cases, we use the same method to find dishonest users. When the authentication fails, the verifier asks the aggregator for the signature key sent by each signer. Since the signature key is the result of the exclusive OR (XOR) of the original message and the original key, the aggregator cannot know the details, but the verifier can, so it can verify the aggregated key. Therefore, in theory, the number of faithless users that the scheme can tolerate is equal to the total number of signers, but this is an ideal situation, and it still requires trust in aggregators and validators.

4.5. Influence of quantum key distribution

In quantum key distribution, there is a definition called Plob boundary, which reflects the ability of the protocol to distribute the key. It can be expressed as $R = -\log_2(1-\eta)$, where R represents the key rate and η denotes the channel transmittance between users. In general, the key rate should be $O(\sqrt{\eta})$.

Owing to the large number of photons lost in the channel, *i.e.*, the low transmittance of the channel, the key rate of most quantum key distribution protocols is limited by the key capacity of the protocol. Some protocols overcome the key capacity through single photon interference to improve the key rate, and can make the transmission distance lengthen to a staggering 830 km, but the phase tracking and phase locking technology are needed to compensate for the related fluctuation problems, which will increase the complexity of the experiment, and may cause related security risks. Some protocols[39] did not need phase tracking or phase locking technology, but used two-photon interference, through the time multiplexing and post-matching methods to break through the key capacity, but the transmission distance would decrease. In the same environment, a transmission range of 450 km can be achieved without phase tracking, and 270 km can be achieved further without phase locking technology. It weighs practicality and performance.

4.6. Quantum memory device

As the core of quantum repeater, quantum memory can capture and store entangled quantum, but up to now only 4 entangled quantum operation have been realized, so the related

protocol relying on quantum memory is really not practical. In our scheme, the aggregator prepares quantum states according to the number of signers, and needs to conduct entanglement exchange of the signed quantum states, so it needs to store the quantum states it has, and with the increase of the number of signers and message length, the number of quantum states that need to be stored will increase, so this protocol cannot eliminate the quantum memory. It will take a long time for the protocol to move from theory to experiment.

5. Conclusions

In this work, we proposed a quantum homomorphic multi-signature scheme based on homomorphic aggregation, which reduces the dependence on the classical key, making it impossible for any attacker to forgery attack only by stealing the secret key and quantum state. In our scheme, the collector is able to aggregate multiple individual signatures consisting of quantum states into a new multi-signature, and the signature process conforms to additive homomorphism. According to the security analysis, the scheme is safe. Our scheme can produce fewer kinds of quantum states, higher signature complexity, and more kinds of verifiable information than traditional quantum multi-signature schemes.

Acknowledgement

Project supported by the National Natural Science Foundation of China (Grant No. 61762039).

References

[1] Shor P W 1994 *Proceedings of 35th Annual Symposium on the Foundations of Computer Science*, IEEE Computer Society Press, Los Alamitos, CA (1994) 124–134
[2] Bennett C H, Brassard G 1984 *Theoretical Computer Science* **560** 7
[3] Wang S, Yin Z Q, He D Y, Chen W, Wang R Q, Ye P, Zhou Y, Fan Yuan G J, Wang F X, Chen W, Zhu Y G, Morozov P V, Divochiy A V, Zhou Z, Guo G C and Han Z F 2022 *Nat. Photon.* **16** 154
[4] Fan Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Zhou Z, Teng J, Chen W, Guo G C and Han Z F 2021 *Photon. Res.* **9** 1881
[5] Fan Yuan G J, Lu F Y, Wang S, Yin Z Q, He D Y, Chen W, Zhou Z, Wang Z H, Teng J, Guo G C and Han Z F 2022 *Optica* **9** 812
[6] Yin H L, Fu Y and Chen Z B 2016 *Phys. Rev. A* **93** 032316
[7] Yin H L, Fu Y, Liu H, Tang Q J, Wang J, You L X, Zhang W J, Chen S J, Wang Z, Zhang Q, Chen T Y, Chen Z B and Pan J W 2017 *Phys. Rev. A* **95** 032334
[8] Yin H L, Wang W L, Tang Y L, Zhao Q, Liu H, Sun X X, Zhang W J, Li H, Puthoor I V, You L X, Andersson E, Wang Z, Liu Y, Jiang X, Ma X F, Zhang Q, Curty M, Chen T Y and Pan J W 2017 *Phys. Rev. A* **95** 042338
[9] 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
[10] 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
[11] Yin H L, Fu Y, Li C L, Weng C X, Li B H, Gu J, Lu Y S, Huang S and Chen Z B 2023 *National Science Review* **10** nwac228
[12] Cai Z Y, Liu S, Han Z Y, Wang R and Huang Y H 2021 *Entropy* **23** 1520
[13] Tiliwalidi K, Zhang J Z and Xie S C 2019 *Int. J. Theor. Phys.* **58** 3510
[14] Dai J Q, Zhang S B and Xia J Y 2020 *Int. J. Comput. Sci. Eng.* **22** 243
[15] Wen X J and Liu Y 2007 *Journal of Electronics* **35** 1079
[16] Wen X J, Liu Y and Zhang P Y 2007 *Wuhan University Journal of Natural Sciences.* **12** 29
[17] Wen X J, Liu Y and Zhou N R 2008 *Int. J. Mod. Phys. B* **22** 4251
[18] Du C B, Shi R H, Zhong H, Cui J, Zhang Shun and Xu Y 2016 *J. Quantum Electron.* **33** 329
[19] Jiang D H, Hu Z Q, Liang X Q and Xu G B 2019 *Quantum Information Processing* **18** 268
[20] He Q Q, Xin X J and Yang Q L 2021 *Quantum Information Processing* **20** 26
[21] Wang T Y, Wang X X, Cai X Q and Zhang R L 2020 *Quantum Information Processing* **19** 241
[22] Yu J and Zhang J H 2021 *Int. J. Theor. Phys.* **60** 2709
[23] Qin H W, Tang W K S and Tso R 2019 *Quantum Information Processing* **18** 53
[24] Zhang W, Rong Z B, Huang Z M and Zheng S G 2019 *Int. J. Theor. Phys.* **58** 2744
[25] Shao A X, Zhang J Z and Xie S C 2017 *Int. J. Theor. Phys.* **56** 1241
[26] Niu X F, Zhang J Z, Xie S C and Chen B Q 2018 *Commun. Theor. Phys.* **70** 529
[27] Shang T, Zhao X J, Wang C and Liu J W 2015 *Quantum Information Processing* **14** 393
[28] Luo Q B, Yang G W, She K, Li X Y and Fang J B 2016 *Quantum Information Processing* **15** 5051
[29] Li K, Shang T and Liu J W 2017 *Quantum Information Processing* **16** 246
[30] Shang T, Pei Z, Chen Liu R Y and Liu J W 2019 *Computers, Materials & Continua* **59** 149
[31] Lin Q, Yan H Y, Huang Z G and Chen W B 2018 *IEEE Access* **6** 20632
[32] Xie C G, Weng J, Lu W and Hou L 2020 *Science China Information Sciences* **63** 139107
[33] Niu P H, Chen Y and Li C 2016 *Int. J. Theor. Phys.* **55** 302
[34] Du Z L, Li X L and Liu X J 2020 *Int. J. Theor. Phys.* **59** 622
[35] Gao G and Wang Y 2017 *Commun. Theor. Phys.* **67** 33
[36] Zou H J, Zhang K J and Song T T 2013 *Quantum Information Processing* **12** 2343
[37] Yang Y G, Wang Y H and Wen Q Y 2010 *Chin. Phys. B* **19** 070304
[38] Yang Y T, Xue T and Li Z C 2011 *Journal of University of Science and Technology of China* **41** 924
[39] Xie Y M, Lu Y S, Weng C X, Cao X Y, Jia Z Y, Bao Y, Wang Y, Fu Y, Yin H L and Chen Z B 2022 *PRX Quantum* **3** 020315