IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 20, 2021, accepted March 7, 2021, date of publication March 18, 2021, date of current version May 3, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3067012

A Novel Quantum Sequential Signature Protocol With Y-SNOP States

XU ZHAO[1], KE-JIA ZHANG[1,2], AND BAO-MIN ZHOU[3]
[1]School of Mathematical Science, Heilongjiang University, Harbin 150080, China
[2]Department of Physics, Tsinghua University, Beijing 100084, China
[3]School of Cyberspace Security, University of Science and Technology of China, Hefei 230026, China

Corresponding author: Ke-Jia Zhang (zhangkejia.bupt@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61802118, in part by the Natural Science Foundation of Heilongjiang Province under Grant LH2019F031 and Grant YQ2020F013, and in part by the University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province under Grant UNPYSCT-2018015. The work of Ke-Jia Zhang was supported by the Outstanding Youth Fund of Heilongjiang University.

ABSTRACT With the development of quantum technology, an arising researching point is to solve some new cipher problems with quantum technology to ensure their security. As we know, the sequential signature means to sign a contract or a document by many signers one by one. It has been widely used to realize layered authentication. In this paper, we propose a quantum sequential signature protocol with a set of strongly nonlocal orthogonal product (Y-SNOP) states. It is proved that the present protocol is secure, i.e., anyone cannot deny or forge a valid signature even some of them conspire. Compared with the existing quantum multi signature with some nonlocal orthogonal product (NOP) states, the present protocol seems more efficient and easier to be realized in Noisy Intermediate-Scale Quantum (NISQ) device as no entangled resources are required.

INDEX TERMS Quantum sequential signature, strongly nonlocal orthogonal product, collusion attack.

I. INTRODUCTION

Digital signature is a basic method to authorize the data in modern cryptography, which has been widely used in e-commerce and other related fields [1]–[3]. As we know, the applied classical digital signature protocols depend on some difficult mathematical problems. However, with the development of quantum computing algorithms, especially Shor algorithm and Grover algorithm, classic signature protocols have to deal with potential security vulnerabilities. In order to ensure their security under the condition of quantum computing, the topic — quantum signature was proposed whose security based on quantum properties. Zeng and Keitel [4] first proposed a framework of quantum signature. Since then, the research of quantum signature has been developed rapidly [5]–[7]. Among them, quantum multi-party signature is an important aspect [8]–[13]. However, the communication efficiency of multi-party signature will decrease with more signers. In order to improve the efficiency, in 2018 Liang *et al.* [14] first proposed a multi-party quantum blind signature scheme based on graph states whose signature length does not grow longer when more signers are referred.

In the present multi-party signatures, each of the signers is supposed to sign the messages and send them to the receiver respectively. Since there is no information exchange between multiple signers, it is essentially similar to execute two-party signatures process multiple times. In practice, especially in the network, there is a more common multi-party authentication situation, that is, multiple signers sign a contract or a document one by one, and then conduct one-time verification. The process is called sequential signature, which can be widely used in the layered authentication. In 2008, Wen and Yun [15] proposed a quantum sequential signature protocol for the first time. In their protocol, each signer is not only the verifier of the previous signature, but also the signer of the next signature. In other words, their multi-party sequential signature is similar to multi-party sequential authentication. Therefore, its efficiency and the application scenarios cannot be so sufficient. In this case, we will discuss a practical case of quantum sequential signature. The last signer gives the document to the verifier for verification when all signers sign the same document in sequence. Furthermore, the security of existing sequential signature protocols is controversial. In this

The associate editor coordinating the review of this manuscript and approving it for publication was Remigiusz Wisniewski.

paper, we propose a secure quantum sequential signature protocol for the first time. A secure quantum sequential signature protocol should meet some requirements, i.e., anyone cannot deny or forge a valid signature even some of them conspire.

The research of nonlocal orthogonal product (NOP) states is one of hot spots in quantum information. Essentially, the part of the orthogonal product state can be prepared locally, but the whole state is nonlocal. Since no entangled resources are required, the proposed protocol may be easier to be realized in Noisy Intermediate-Scale Quantum (NISQ) device. Moreover, different particles of the orthogonal product state can be transformed separately. It means that only a part of the NOP states is transmitted each time, and the attacker cannot determine the accurate whole state even if he gets this transferred part from quantum channel. In this situation, if the private messages are encoded into NOP states, the security of the private messages will be ensured. This idea could be applied in quantum cryptography such as data hiding [16]–[19], quantum secret sharing [20] and quantum voting scheme [21]. In recent years, Xu *et al.* [22]–[27] designed some quantum cipher protocols with some NOP states. Specially, a quantum multi-party signature with some NOP states of $C^2 \otimes C^2 \otimes C^2 \otimes C^2$ is designed in 2019 [24].

Recently, Halder *et al.* [28] first proposed strong quantum nonlocality without entanglement, and presented two explicit strongly nonlocal sets of quantum states in $C^3 \otimes C^3 \otimes C^3$ and $C^4 \otimes C^4 \otimes C^4$ quantum system, respectively. For the sake of simplicity, we define these states as SNOP states. Compared with the NOP states, SNOP states have strong quantum nonlocality for tripartite, i.e., they are locally irreducible in every bipartition. In 2020, Yuan *et al.* [29] presented a new set of strongly nonlocal orthogonal product states (Y-SNOP) and proved these states are strongly nonlocal. They found and demonstrated that a smaller number of SNOP states have strong quantum nonlocality without entanglement in $C^3 \otimes C^3 \otimes C^3$. Combining with these Y-SNOP states, we propose a new quantum sequential signature protocol. Furthermore, the presented protocol does not only solve the problem to sign a message sequentially for several signers, but also give a potential application of NOP states.

The rest of the paper is arranged as follows. In Section. II, some preliminary theories are introduced. In Section. III, we describe the quantum sequential signature protocol including initializing phase, signing phase and verifying phase. The security analysis and further discussion of our protocol are proposed in Section. IV and V. Finally, a short conclusion is given in Section. VI.

II. PRELIMINARIES

In this section, we will firstly describe an encryption algorithm — Key-Controlled-'I'QOTP to generate signature. Then, a set of Y-SNOP states are introduced to encode the send messages. These necessary preliminaries are proposed as follows.

TABLE 1. Corresponding encryption operators in "Key-Controlled-'I' QOTP".

$K_i K_{2n-i+1}$	encryption operator
00	$W_{00} = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z)$
01	$W_{01} = \frac{1}{\sqrt{2}}(\sigma_y + \sigma_z)$
10	$W_{10} = \frac{1}{2}(I + i\sigma_x - i\sigma_y + i\sigma_z)$
11	$W_{11} = \frac{1}{2}(I + i\sigma_x + i\sigma_y + i\sigma_z)$

A. KEY-CONTROLLED-'I'QOTP

Encryption algorithm is an important way to generate quantum signature. Compared with One Time Pad in classical encryption, the corresponding Quantum One Time Pad (QOTP) was proposed in 2003 [30]. With the development of arbitrated quantum signature (AQS), QOTP is widely used in the design of AQS protocols [1], [4], [31]. However, Gao *et al.* [32] pointed out that there exist some security problems in these protocols. In the previous security analysis of AQS protocols, one of the most basic assumptions is that the signature is generated by encrypting bitwise messages. In this case, the receiver may forge a legal signature by performing a corresponding operator to the signature and message without secret keys.

In order to solve this problem, Zhang *et al.* [33] provided a series of encryption algorithms to improve the security of AQS protocols. Here, we briefly introduce one of a series of encryption algorithms — Key-Controlled-'I'QOTP in Ref [33].

Firstly, a set W with four Clifford operators is introduced to encrypt the message $|P_i'\rangle$ to get $|S\rangle$. And the two bits K_i and K_{2n-i+1} in the shared key string K are appointed to determine the corresponding encryption operators in Table 1. Secondly, the message $|P_i'\rangle$ is encrypted into $|S\rangle$ in the form of Eq.(1).

$$|S\rangle = \otimes_{i=1}^{n} \sigma_x^{k_{2i}} \sigma_z^{k_{2i-1}} W_{K_i K_{2n-i+1}} |P_i'\rangle \tag{1}$$

Zhang *et al.* proved that this encryption algorithm can be applied to generate signature which cannot be forged by the receiver. Therefore, in order to ensure the security, the Key-Controlled-'I'QOTP will be used in the following quantum sequential signature protocol.

B. Y-SNOP STATES

Recently, Yuan *et al.* [29] presented a new set of strongly nonlocal orthogonal product (Y-SNOP) states and proved these states are strongly nonlocal. The specific forms can be seen as follows.

$$\begin{aligned} &|0\rangle|i\rangle|0 \pm i\rangle,\ |i\rangle|0 \pm i\rangle|0\rangle,\ |0 \pm i\rangle|0\rangle|i\rangle \\ &|i\rangle|j\rangle|0 \pm i\rangle,\ |j\rangle|0 \pm i\rangle|i\rangle,\ |0 \pm i\rangle|i\rangle|j\rangle \end{aligned} \tag{2}$$

where $1 \leq i, j \leq d-1$ and $i \neq j$. Yuan *et al.* proved that these states are locally irreducible. Since local irreducibility is a sufficient condition for strongly nonlocal, these states are strongly nonlocal.

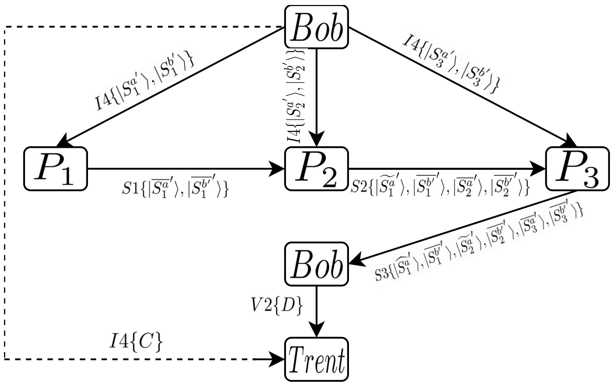


FIGURE 1. **Process of the sequential signature protocol. (The solid line represents the quantum channel, and the dotted line represents the classical channel).**

In quantum signature protocol, we encode the message into Y-SNOP states. In this case, attacker will not be able to restore all the information even he gets two particles of Y-SNOP states. In other words, forgery will not be possible even if any two parties conspire. In order to simply our quantum sequential signature, specific form of $C^3 \otimes C^3 \otimes C^3$ of Eq.(2) is given in Eq.(3).

$$\begin{aligned}
&|0\rangle|1\rangle|0 \pm 1\rangle,\ |1\rangle|0 \pm 1\rangle|0\rangle,\ |0 \pm 1\rangle|0\rangle|1\rangle \\
&|0\rangle|2\rangle|0 \pm 2\rangle,\ |2\rangle|0 \pm 2\rangle|0\rangle,\ |0 \pm 2\rangle|0\rangle|2\rangle \\
&|1\rangle|2\rangle|0 \pm 1\rangle,\ |2\rangle|0 \pm 1\rangle|1\rangle,\ |0 \pm 1\rangle|1\rangle|2\rangle \\
&|2\rangle|1\rangle|0 \pm 2\rangle,\ |1\rangle|0 \pm 2\rangle|2\rangle,\ |0 \pm 2\rangle|2\rangle|1\rangle \qquad (3)
\end{aligned}$$

III. QUANTUM SEQUENTIAL SIGNATURE WITH Y-SNOP STATES

In this section, a new quantum sequential signature with Y-SNOP states is proposed. This protocol includes three phases: initializing phase, signing phase and verifying phase.

Previously, there exist five roles in our protocol:

(1) Bob is the applicant;
(2) P_1 is the first signer;
(3) P_2 is the second signer;
(4) P_3 is the last signer;
(5) Trent is the arbitrator.

Bob wants to get an authorization of a document which should be signed by three levels of signers P_1, P_2 and P_3 in sequence. The specific process is shown in Fig. 1.

A. INITIALIZING PHASE

Step I1 (Secret Key Assignment): Trent shares three private key sequences K_{TP_1}, K_{TP_2}, K_{BT} with P_1, P_2, Bob respectively. Bob shares private key sequence K_{BP_3} with P_3. This can be achieved by quantum key distribution (QKD) protocol [34]–[36].

Step I2 (Message Encoding): The sending message M is divided into n groups $M = M_1 \| M_2 \| \cdots \| M_n$, here M_t is chosen from a set {0000, 0001, 0010, 0100, 1000, 1001, 1010, 1100, 0011, 0101, 0110, 0111, 1011, 1101, 1110, 1111},

TABLE 2. **Y-SNOP states used to encrypt messages.**

message	state
$M_t = 0000$	$\|\varphi_1\rangle = \|0\rangle\|1\rangle\|0+1\rangle$
$M_t = 0001$	$\|\varphi_2\rangle = \|0\rangle\|2\rangle\|0+2\rangle$
$M_t = 0010$	$\|\varphi_3\rangle = \|1\rangle\|2\rangle\|0+1\rangle$
$M_t = 0100$	$\|\varphi_4\rangle = \|2\rangle\|1\rangle\|0+2\rangle$
$M_t = 1000$	$\|\varphi_5\rangle = \|0+1\rangle\|0\rangle\|1\rangle$
$M_t = 1001$	$\|\varphi_6\rangle = \|0+2\rangle\|0\rangle\|2\rangle$
$M_t = 1010$	$\|\varphi_7\rangle = \|0+1\rangle\|1\rangle\|2\rangle$
$M_t = 1100$	$\|\varphi_8\rangle = \|0+2\rangle\|2\rangle\|1\rangle$
$M_t = 1111$	$\|\varphi_9\rangle = \|0\rangle\|1\rangle\|0-1\rangle$
$M_t = 1110$	$\|\varphi_{10}\rangle = \|0\rangle\|2\rangle\|0-2\rangle$
$M_t = 1101$	$\|\varphi_{11}\rangle = \|1\rangle\|2\rangle\|0-1\rangle$
$M_t = 1011$	$\|\varphi_{12}\rangle = \|2\rangle\|1\rangle\|0-2\rangle$
$M_t = 0111$	$\|\varphi_{13}\rangle = \|0-1\rangle\|0\rangle\|1\rangle$
$M_t = 0110$	$\|\varphi_{14}\rangle = \|0-2\rangle\|0\rangle\|2\rangle$
$M_t = 0101$	$\|\varphi_{15}\rangle = \|0-1\rangle\|1\rangle\|2\rangle$
$M_t = 0011$	$\|\varphi_{16}\rangle = \|0-2\rangle\|2\rangle\|1\rangle$

TABLE 3. **Y-SNOP states used to detect eavesdropping.**

detected eavesdropping state
$\|\varphi_{17}\rangle = \|1\rangle\|0+1\rangle\|1\rangle$
$\|\varphi_{18}\rangle = \|1\rangle\|0-1\rangle\|1\rangle$
$\|\varphi_{19}\rangle = \|2\rangle\|0+2\rangle\|0\rangle$
$\|\varphi_{20}\rangle = \|2\rangle\|0-2\rangle\|0\rangle$
$\|\varphi_{21}\rangle = \|2\rangle\|0+1\rangle\|1\rangle$
$\|\varphi_{22}\rangle = \|2\rangle\|0-1\rangle\|1\rangle$
$\|\varphi_{23}\rangle = \|1\rangle\|0+2\rangle\|2\rangle$
$\|\varphi_{24}\rangle = \|1\rangle\|0-2\rangle\|2\rangle$

where $t = 1, 2, 3, \cdots, n$. Bob encodes each M_t to a quantum sequence $|S\rangle$ with the 16 states in Table 2, the remaining 8 states are used for eavesdropping detection in Table 3.

Step I3 (Generating Quantum Sequence): Bob generates two identical sequences $|S\rangle$, where the first sequence is denoted by $|S^a\rangle$ and the other is denoted by $|S^b\rangle$. By picking out the i-th particle of each $|S^a\rangle$ ($|S^b\rangle$), the corresponding quantum sequences $|S_i^a\rangle$ ($|S_i^b\rangle$) are generated, where $i = 1, 2, 3$.

Step I4 (Sending Sequence): Bob first inserts the detected eavesdropping states randomly in sequences to get $|S_1^{a'}\rangle$, $|S_1^{b'}\rangle$, $|S_2^{a'}\rangle$, $|S_2^{b'}\rangle$, $|S_3^{a'}\rangle$, $|S_3^{b'}\rangle$. Then he sends $|S_1^{a'}\rangle$, $|S_1^{b'}\rangle$ to P_1, $|S_2^{a'}\rangle$, $|S_2^{b'}\rangle$ to P_2 and $|S_3^{a'}\rangle$, $|S_3^{b'}\rangle$ to P_3. Finally, he encrypts the message M with K_{BT} to get C and sends C to Trent.

$$C = E_{K_{BT}}\{M\} \qquad (4)$$

Step I5 (Detect Eavesdropping): After P_i ($i = 1, 2, 3$) announces that he has received the sequences $|S_i^{a'}\rangle$, $|S_i^{b'}\rangle$, Bob tells P_i the positions and the initial states of the decoy particles. Then, P_i measures each of the decoy particles with the corresponding basis and compares the measurement outcome with its initial state to check eavesdropping. If the error probability is within a certain threshold, P_i will recover the sequences $|S_i^a\rangle$, $|S_i^b\rangle$; otherwise, he will abort the protocol. (The subsequent detection of eavesdropping is the same as this step).

TABLE 4. The encryption process to generate signature.

sequence	signature
$\lvert\overline{S_1^a}\rangle$	$E_{K_{TP_1}}\{\lvert S_1^a\rangle\}$
$\lvert\widetilde{S_1^a}\rangle$	$E_{K_{TP_2}}\{\lvert\overline{S_1^a}\rangle\}$
$\lvert\widehat{S_1^a}\rangle$	$E_{K_{BP_3}}\{\lvert\widetilde{S_1^a}\rangle\}$
$\lvert\overline{S_1^{b'}}\rangle$	$E_{K_{TP_1}}\{\lvert S_1^{b'}\rangle\}$
$\lvert\overline{S_2^a}\rangle$	$E_{K_{TP_2}}\{\lvert S_2^a\rangle\}$
$\lvert\widetilde{S_2^a}\rangle$	$E_{K_{BP_3}}\{\lvert\overline{S_2^a}\rangle\}$
$\lvert\overline{S_2^{b'}}\rangle$	$E_{K_{TP_2}}\{\lvert S_2^{b'}\rangle\}$
$\lvert\overline{S_3^a}\rangle$	$E_{K_{BP_3}}\{\lvert S_3^a\rangle\}$
$\lvert\overline{S_3^{b'}}\rangle$	$E_{K_{BP_3}}\{\lvert S_3^{b'}\rangle\}$

TABLE 5. The transmission process of signature.

signer	signature	send signature	receiver
P_1	$\lvert\overline{S_1^a}\rangle, \lvert\overline{S_1^{b'}}\rangle$	$\lvert\overline{S_1^a}'\rangle, \lvert\overline{S_1^{b'}}'\rangle$	P_2
P_2	$\lvert\widetilde{S_1^a}\rangle, \lvert\overline{S_2^a}\rangle, \lvert\overline{S_2^{b'}}\rangle$	$\lvert\widetilde{S_1^a}'\rangle, \lvert\overline{S_1^{b'}}'\rangle, \lvert\overline{S_2^a}'\rangle, \lvert\overline{S_2^{b'}}'\rangle$	P_3
P_3	$\lvert\widehat{S_1^a}\rangle, \lvert\widetilde{S_2^a}\rangle, \lvert\overline{S_3^a}\rangle, \lvert\overline{S_3^{b'}}\rangle$	$\lvert\widehat{S_1^a}'\rangle, \lvert\overline{S_1^{b'}}'\rangle, \lvert\widetilde{S_2^a}'\rangle, \lvert\overline{S_2^{b'}}'\rangle, \lvert\overline{S_3^a}'\rangle, \lvert\overline{S_3^{b'}}'\rangle$	Bob

B. SIGNING PHASE

Step S1 (P_1's Signature): P_1 inserts the detected eavesdropping states randomly in $|S_1^b\rangle$ to get $|S_1^{b'}\rangle$. Then he encrypts the sequences with K_{TP_1} to get $|\overline{S_1^a}\rangle$ and $|\overline{S_1^{b'}}\rangle$ as $P_1's$ signature. Finally he inserts the detected eavesdropping states randomly in his signature to get $|\overline{S_1^a}'\rangle$, $|\overline{S_1^{b'}}'\rangle$ and sends them to P_2.

Step S2 (P_2's Signature): When P_2 has received the sequences, he will detect eavesdropping as Step I5. If it passes, he will insert the detected eavesdropping states randomly in $|S_2^b\rangle$ to get $|S_2^{b'}\rangle$. Then he encrypts the $|S_2^a\rangle$, $|S_2^{b'}\rangle$, $|\overline{S_1^a}\rangle$ with K_{TP_2} to get $|\overline{S_2^a}\rangle$, $|\overline{S_2^{b'}}\rangle$, $|\widetilde{S_1^a}\rangle$ as $P_2's$ signature. Finally he inserts the detected eavesdropping states randomly in his signature and $|\overline{S_1^{b'}}\rangle$ to get $|\overline{S_2^a}'\rangle$, $|\overline{S_2^{b'}}'\rangle$, $|\widetilde{S_1^a}'\rangle$, $|\overline{S_1^{b'}}'\rangle$ and sends them to P_3.

Step S3 (P_3's Signature): After eavesdropping detection, P_3 inserts the detected eavesdropping states randomly in $|S_3^b\rangle$ to get $|S_3^{b'}\rangle$. Then he encrypts $|S_3^a\rangle$, $|S_3^{b'}\rangle$, $|\overline{S_2^a}\rangle$, $|\widetilde{S_1^a}\rangle$ with the key K_{BP_3} to get $|\overline{S_3^a}\rangle$, $|\overline{S_3^{b'}}\rangle$, $|\widetilde{S_2^a}\rangle$, $|\widehat{S_1^a}\rangle$ as $P_3's$ signature. Finally P_3 inserts the detected eavesdropping states randomly in his signature and $|\overline{S_2^{b'}}\rangle$, $|\overline{S_1^{b'}}\rangle$ to get $|\overline{S_3^a}'\rangle$, $|\overline{S_3^{b'}}'\rangle$, $|\widetilde{S_2^a}'\rangle$, $|\overline{S_2^{b'}}'\rangle$, $|\widehat{S_1^a}'\rangle$, $|\overline{S_1^{b'}}'\rangle$ and sends them to Bob.

The generation process and specific form of signatures are shown in Table 4 and Table 5.

C. VERIFICATION PHASE

Step V1 (Bob's Detect Eavesdropping): Through eavesdropping detect, Bob recovers the quantum sequences $|\overline{S_3^a}\rangle$, $|\overline{S_3^{b'}}\rangle$, $|\widetilde{S_2^a}\rangle$, $|\overline{S_2^{b'}}\rangle$, $|\widehat{S_1^a}\rangle$, $|\overline{S_1^{b'}}\rangle$. Then he decrypts the sequences with K_{BP_3} to get $|S_3^a\rangle$, $|S_3^{b'}\rangle$, $|\overline{S_2^a}\rangle$, $|\overline{S_2^{b'}}\rangle$, $|\widetilde{S_1^a}\rangle$, $|\overline{S_1^{b'}}\rangle$. For $|S_3^{b'}\rangle$, Bob removes the decoy particles and gets $|S_3^b\rangle$.

Step V2 (Bob's Verification): Bob verifies whether $|S_3^a\rangle$ is equal to $|S_3^b\rangle$ with swap operation [37]–[39]. Here V_B represents the measurement result of swap operation.

$$V_B = \begin{cases} 1, & |S_3^a\rangle = |S_3^b\rangle \\ 0, & |S_3^a\rangle \neq |S_3^b\rangle \end{cases} \tag{5}$$

If $V_B = 0$, he will reject the quantum signature directly; otherwise, he will send D to Trent.

$$D = E_{K_{BT}}\{|S_3^a\rangle, |\overline{S_2^a}\rangle, |\overline{S_2^{b'}}\rangle, |\widetilde{S_1^a}\rangle, |\overline{S_1^{b'}}\rangle\} \tag{6}$$

Step V3 (Trent's Decryption): Trent decrypts D, C with K_{BT} to get the sequences $|S_3^a\rangle$, $|\overline{S_2^a}\rangle$, $|\overline{S_2^{b'}}\rangle$, $|\widetilde{S_1^a}\rangle$, $|\overline{S_1^{b'}}\rangle$ and message M. Then he decrypts the sequences with K_{TP_1} and K_{TP_2} to get $|S_1^a\rangle$, $|S_1^{b'}\rangle$, $|S_2^a\rangle$, $|S_2^{b'}\rangle$. Similarly, Trent removes the decoy particles and gets $|S_1^b\rangle$, $|S_2^b\rangle$.

Step V4 (Trent's Verification of the First Stage): Similarly, Trent verifies whether $|S_1^a\rangle$ ($|S_2^a\rangle$) is equal to $|S_1^b\rangle$ ($|S_2^b\rangle$) and generates V_T.

$$V_T = \begin{cases} 1, & |S_1^a\rangle = |S_1^b\rangle, |S_2^a\rangle = |S_2^b\rangle \\ 0, & |S_1^a\rangle \neq |S_1^b\rangle or |S_2^a\rangle \neq |S_2^b\rangle \end{cases} \tag{7}$$

If $V_T = 0$, he will reject the quantum signature directly; otherwise, the $|S\rangle$ will be recovered by $|S_1^a\rangle$, $|S_2^a\rangle$, $|S_3^a\rangle$.

Step V5 (Trent's Verification of the Second Stage): Trent measures $|S\rangle$ by the following rules in Table 6 to get $\overline{M}$. If $\overline{M} = M$, he will announce that the signature is valid; otherwise, the signature will be invalid.

D. BRIEF SUMMARY

Encryption algorithm is an important method to generate quantum signature. In our protocol, the quantum signature is also generated by quantum encryption algorithm based on the shared keys. Therefore, the efficiency of QKD determines the practical efficiency of our protocol to some extent. To date, real-time quantum key generation has been realized with over Gbps speed and security guarantees [40], [41]. In this view, the presented can be realized in the near future.

In our protocol, the Key-Controlled-'I'QOTP is used to generate signature. Encrypting a qubit requires two secret keys, therefore, encrypting n qubits requires 2n secret keys. The quantum communication efficiency and local computing efficiency of our protocol are summarized in Table 7 and Table 8. It is worth noting that quantum communication efficiency does not include the stage of sharing secret key.

IV. SECURITY ANALYSIS

As mentioned above, a secure quantum signature protocol has to meet at least two requirements, i.e., non-forgery, non-repudiation. In our protocol, Trent is the honest arbitrator who will perform authentication when dispute happens. In this case, the security of our protocol is shown, i.e., anyone cannot

TABLE 6. Trent's measurement rules.

message	basis
$M_t = 0000 \mapsto \lvert\varphi_1\rangle = \lvert 0\rangle\lvert 1\rangle\lvert 0+1\rangle$ $M_t = 1111 \mapsto \lvert\varphi_9\rangle = \lvert 0\rangle\lvert 1\rangle\lvert 0-1\rangle$	$\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0+1\rangle, \lvert 0-1\rangle, \lvert 2\rangle\}_3$
$M_t = 0001 \mapsto \lvert\varphi_2\rangle = \lvert 0\rangle\lvert 2\rangle\lvert 0+2\rangle$ $M_t = 1110 \mapsto \lvert\varphi_{10}\rangle = \lvert 0\rangle\lvert 2\rangle\lvert 0-2\rangle$	$\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0+2\rangle, \lvert 0-2\rangle, \lvert 1\rangle\}_3$
$M_t = 0010 \mapsto \lvert\varphi_3\rangle = \lvert 1\rangle\lvert 2\rangle\lvert 0+1\rangle$ $M_t = 1101 \mapsto \lvert\varphi_{11}\rangle = \lvert 1\rangle\lvert 2\rangle\lvert 0-1\rangle$	$\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0+1\rangle, \lvert 0-1\rangle, \lvert 2\rangle\}_3$
$M_t = 0100 \mapsto \lvert\varphi_4\rangle = \lvert 2\rangle\lvert 1\rangle\lvert 0+2\rangle$ $M_t = 1011 \mapsto \lvert\varphi_{12}\rangle = \lvert 2\rangle\lvert 1\rangle\lvert 0-2\rangle$	$\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0+2\rangle, \lvert 0-2\rangle, \lvert 1\rangle\}_3$
$M_t = 1000 \mapsto \lvert\varphi_5\rangle = \lvert 0+1\rangle\lvert 0\rangle\lvert 1\rangle$ $M_t = 0111 \mapsto \lvert\varphi_{13}\rangle = \lvert 0-1\rangle\lvert 0\rangle\lvert 1\rangle$	$\{\lvert 0+1\rangle, \lvert 0-1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_3$
$M_t = 1001 \mapsto \lvert\varphi_6\rangle = \lvert 0+2\rangle\lvert 0\rangle\lvert 2\rangle$ $M_t = 0110 \mapsto \lvert\varphi_{14}\rangle = \lvert 0-2\rangle\lvert 0\rangle\lvert 2\rangle$	$\{\lvert 0+2\rangle, \lvert 0-2\rangle, \lvert 1\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_3$
$M_t = 1010 \mapsto \lvert\varphi_7\rangle = \lvert 0+1\rangle\lvert 1\rangle\lvert 2\rangle$ $M_t = 0101 \mapsto \lvert\varphi_{15}\rangle = \lvert 0-1\rangle\lvert 1\rangle\lvert 2\rangle$	$\{\lvert 0+1\rangle, \lvert 0-1\rangle, \lvert 2\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_3$
$M_t = 1100 \mapsto \lvert\varphi_8\rangle = \lvert 0+2\rangle\lvert 2\rangle\lvert 1\rangle$ $M_t = 0011 \mapsto \lvert\varphi_{16}\rangle = \lvert 0-2\rangle\lvert 2\rangle\lvert 1\rangle$	$\{\lvert 0+2\rangle, \lvert 0-2\rangle, \lvert 1\rangle\}_1$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_2$ $\{\lvert 0\rangle, \lvert 1\rangle, \lvert 2\rangle\}_3$

TABLE 7. The efficiency of quantum communication for the presented protocol.

Communication efficiency	Quantum bits
Step I4	6n
Step S1	2n
Step S2	4n
Step S3	6n
Step V2	5n

TABLE 8. The efficiency of local computing for the presented protocol.

Computing efficiency	Maximum	Minimum
Signature phase	12n	4n
Verification phase	12n	4n

deny or forge a valid signature even if any two participants conspire. The specific analysis is described as follows.

A. NON-FORGERY

1) OUTSIDE ATTACK

For the external attacker Eve, he wants to forge a signature and evades Trent's authentication. As a rational attacker, he can only choose to intercept the signature through the channel of quantum transmission and replace it. For the classical channel is transmitted by broadcast, the attacker is not able to determine the message without secret key. Here, we will describe Eve's supposable attack strategies in the following steps.

a: EVE INTERCEPTS SEQUENCES IN STEP I4

Eve intercepts the Y-SNOP states and performs joint measurements of quantum sequences based on Eq.(3). He wants to send the fake quantum sequences to P_i, trying to get P_i to sign on the fake message. Since the quantum sequences which Bob sends to P_i in Step I4 are inserted with two types of Y-SNOP states, he cannot distinguish the intercepted quantum states used to encode message or detect eavesdropping. If he changes the quantum sequence and sends it to P_i, there will be an error in Step I5. Even though he is lucky to modify the quantum states used to encode message and sends to P_i, he would not succeed. Because the classic message M was sent to Trent from Bob by secret key K_{BT} in the initial stage, he will be found in Trent's verification phase as $\overline{M} \neq M$.

b: EVE FORGES SIGNATURE OF P_i

With the example of P_1, Eve intercepts sequences $\lvert\overline{S_1^{a'}}\rangle$, $\lvert\overline{S_1^{b'}}\rangle$ in Step S1. Since the encryption algorithm — Key-Controlled-'I'QOTP is applied to generate signature in our protocol, Eve may perform forgery attacks in the following ways.

i) Eve attempts to eavesdrop the K_{TP_1} distributed between signers and verifiers. However, the original keys are shared with QKD protocol, it is impossible for him to succeed.

ii) Eve attempts to modify P_1's signature to make $\lvert S_1^a\rangle$, $\lvert S_1^b\rangle$ are still equal after his modification. Similarly, due to insetting detected eavesdropping states in P_1's signature, Eve cannot distinguish the intercepted quantum states used to encode message or detect eavesdropping. Furthermore, Key-Controlled-'I'QOTP is used to generate signature, he is not able to identify the forms of encryption operators without key K_{TP_1}. For detailed analysis, it can be seen in Bob's attack.

c: EVE INTERCEPTS SEQUENCES IN STEP V2

Similar to the analysis above, Eve cannot know the secret key K_{BT}. If he changes one of the four sequences $\lvert\widetilde{S_1^a}\rangle$, $\lvert\overline{S_1^{b'}}\rangle$, $\lvert\overline{S_2^a}\rangle$, $\lvert\overline{S_2^{b'}}\rangle$ in D, Trent will find errors in Step V3. If he changes $\lvert S_3^a\rangle$, there will be an error in Step V5 as $\overline{M} \neq M$. Therefore, Eve's forgery will be discovered by Trent once he just changes only a small part of D.

2) PARTICIPANT'S ATTACK–INDIVIDUAL ATTACK

For individual attacker, the attacker may be Bob or one of the signers.

a: BOB'S FORGERY

i)BOB FORGES SIGNATURE OF P_1/P_2

Without loss of generality, Bob attempts to forge a signature of P_1. If Bob chooses to attack in Step S2, the situation will be the same as an external attacker. According to the analysis above, the attack strategy is infeasible. Therefore, he has to forge a signature in Step V2. In order to achieve this goal,

TABLE 9. The possible of encrytion and decryption in"Key-Controlled-'I' QOTP".

encryption	decryption
I	$W_i^\dagger Q W_i$
σ_z	$W_i^\dagger \sigma_z Q \sigma_z W_i$
σ_x	$W_i^\dagger \sigma_x Q \sigma_x W_i$
σ_y	$W_i^\dagger \sigma_y Q \sigma_y W_i$

TABLE 10. Attacker's successful forgery attack in "Key-Controlled-'I' QOTP".

operation	signature
	00 01 10 11
σ_z	σ_z σ_x σ_y σ_z
σ_x	σ_y σ_z σ_z σ_x
σ_y	σ_x σ_y σ_x σ_y

he should preform a corresponding operator to the signature and message. However, the Key-Controlled-'I'QOTP is used to generate signature $|\overline{S_1^a}'\rangle, |\overline{S_1^{b'}}'\rangle$ directly, he cannot identify the forms of encryption operators except for P_1 and Trent, and this can be shown in Table 9. Here W_i is selected from the set W.

From Table 10, it is shown that if Bob wants to forge the one qubit of P_1' signature with σ_x or σ_y, he should perform Pauli operation randomly, the successful probability will be $\frac{1}{3}$. And the probability will be $\frac{1}{2}$ if the forgery operation is σ_z. Furthermore, if he wants to forge m qubits of the message to satisfy his needs, the probability P_B of his successful forgery will be shown as:

$$P_B = (\frac{1}{3})^k (\frac{1}{2})^{m-k} \tag{8}$$

here $k(0 \leq k \leq m, 0 \leq m \leq n)$ represents the total number of qubits he wants to forge the sequence by σ_x and σ_y, and $(m-k)$ represents the number of qubits forged by σ_z. With this encryption algorithm, he cannot successfully achieve forgery attack without introducing the errors in the Trent's verification phase.

ii)BOB FORGES SIGNATURE OF P_3

It is different from forging a signature of P_1/ P_2 because Bob has secret key K_{BP_3} with P_3. Similarly, he has to replace the $|S_3^a\rangle$ with $|S_3^{a''}\rangle$ in Step V2. However, the classic message M was sent to Trent in the initial stage. Therefore, it will be found by Trent in Step V5 as $\overline{M} \neq M$. So it is impossible for him to succeed.

b: P_i'S FORGERY

i)P_1/P_2 FORGES SIGNATURE OF P_2/P_3

Without loss of generality, we take P_1 forge signature of P_2 as an example. According to the analysis above, P_1 should perform attack in Step S2. Since we use Key-Controlled-'I'QOTP, under this encryption algorithm, he cannot successfully achieve forgery attack. Furthermore, since P_2 insets detected eavesdropping states in his signature. If P_1 intercepts and replaces $|\widetilde{S_2^a}'\rangle, |\overline{S_2^{b'}}'\rangle$ with $|\widetilde{S_2^a}''\rangle, |\overline{S_2^{b'}}''\rangle$, he will be found in Step V4 as $|S_2^a\rangle \neq |S_2^b\rangle$.

ii)P_3 FORGES SIGNATURE OF P_1/P_2

Differently, P_3 does not need to intercept the sequences because he has secret key K_{BP_3} with Bob and sends all quantum sequences to Bob in Step S3. He wants to forge a signature of P_1 in Step S3. Based on the analysis above, the Key-Controlled-'I'QOTP is used in our protocol and P_1 insets detected eavesdropping states in his signature. If P_3 replaces $|\widetilde{S_1^a}\rangle, |\overline{S_1^{b'}}\rangle$ with $|\widetilde{S_1^a}''\rangle, |\overline{S_1^{b'}}''\rangle$, he will be found in the Trent's verification phase. It is as P_3 forges P_2' signature.

3) PARTICIPANT'S ATTACK–COLLUSION ATTACK

Previously, we guarantee that at least half of the participants are honest except for the arbitrator. This assumption is satisfied with the actual situation. In fact, if more than half of the participants are dishonest, the protocol will be insecure and impractical. Here, we will discuss the dishonest collusion of any two participants. Specifically, they want to forge a signature and evade Trent's authentication.

a: BOB AND P_i COLLUSION ATTACK

Without loss of generality, Bob and P_1 conspire to forge signature of P_2. Similarly, they should perform attack in Step V2. They want to replace the $|\overline{S_2^a}\rangle, |\overline{S_2^{b'}}\rangle$ with $|\overline{S_2^a}''\rangle, |\overline{S_2^{b'}}''\rangle$. According to the analysis of the individual attack for Bob, as the Key-Controlled-'I'QOTP is used in our protocol, it is impossible to successfully implement a forgery attack. Furthermore, they cannot know the positions and the initial states of the decoy states since P_2 insets detected eavesdropping states in his signature. Their collusion attack is unlikely to succeed.

b: P_i AND P_j COLLUSION ATTACK ($i \neq j$)

Based on the analysis above, P_1 and P_2 should restore all the Y-SNOP states through the sequences in their hands. If they choose the correct measurement basis, they will determine the state. It is not difficult to find that there are three possible cases in Eq.(9). The specific measurement results are shown in Table 11.

$$\begin{aligned} B1 &= \{|0\rangle, |1\rangle, |2\rangle\} \\ B2 &= \{|0+1\rangle, |0-1\rangle, |2\rangle\} \\ B3 &= \{|0+2\rangle, |0-2\rangle, |1\rangle\} \end{aligned} \tag{9}$$

TABLE 11. The possible measurement results for the attacker.

state	$\|0\rangle$	$\|1\rangle$	$\|2\rangle$	$\|0+1\rangle$	$\|0-1\rangle$	$\|0+2\rangle$	$\|0-2\rangle$
$B1$	1	1	1	0	0	0	0
$B2$	0	0	1	1	1	0	0
$B3$	0	1	0	0	0	1	1

They can only choose the measurement basis randomly. In other words, their probability of choosing any basis is $\frac{1}{3}$. From table 11, we can deduce that the probability that they choose the correct measurement basis and get one bit as:

$$p_1 = \frac{1}{3} \times 1 = \frac{1}{3}, \quad p_2 = \frac{1}{3} \times 2 = \frac{2}{3}, \ p_3 = \frac{1}{3} \times 2 = \frac{2}{3}$$
$$p_4 = \frac{1}{3} \times 1 = \frac{1}{3}, \quad p_5 = \frac{1}{3} \times 1 = \frac{1}{3}, \ p_6 = \frac{1}{3} \times 1 = \frac{1}{3}$$
$$p_7 = \frac{1}{3} \times 1 = \frac{1}{3} \tag{10}$$

According to our protocol, the 16 states of Y-SNOP are used to encode message. The probability P which they get one state is:

$$P = \frac{p_1 + p_2 + p_3 + p_4 + p_5 + p_6 + p_7}{16} = \frac{3}{16} \tag{11}$$

If the length of the quantum sequence is n, the probability of getting the P' sequence is:

$$P' = P^n = (\frac{3}{16})^n \tag{12}$$

If $n = 1000$, we have

$$P' = P^{1000} = (\frac{3}{16})^{1000} \tag{13}$$

The number is too small to imagine. So they will not attack successfully.

B. NON-REPUDIATION

The denial of the signer is also a very important issue which needs to be discussed in signature protocol. In our protocol, the denial of P_3 is different from P_1 and P_2. The specific analysis is described.

1) THE DENIAL OF P_1 (THE SAME AS P_2)

P_1 attempts to deny that his signature $|\overline{S_1^a}\rangle$, $|\overline{S_1^{b'}}\rangle$. In fact, P_1 encrypts the quantum sequences $|S_1^a\rangle$, $|S_1^b\rangle$ with K_{TP_1}. Therefore, he cannot deny that he has generated the signature $|\overline{S_1^a}\rangle$, $|\overline{S_1^{b'}}\rangle$ since no one knows the key K_{TP_1} except Trent and P_1. Moreover, we use Key-Controlled-'I'QOTP, no one can find the corresponding location without knowing the K_{TP_1}. If $|S_1^a\rangle = |S_1^b\rangle$, it is impossible for P_1 to deny success.

2) THE DENIAL OF P_3

P_3 attempts to deny that his signature $|\overline{S_3^a}\rangle$, $|\overline{S_3^{b'}}\rangle$. In our protocol, only Bob and P_3 share the secret key K_{BP_3}. According to the analysis of the individual attack for Bob, if Bob attempts to modify the signature of P_3, Trent will be found in Step V5. Therefore, if $\overline{M} = M$, P_3 will not be able to deny his signature.

V. FURTHER DISCUSSION

As a topic of quantum multi-party signature, quantum sequential signature requires the messages can be signed sequentially by more than one signer. However, the protocol flow and security requirement of each multi-party signature protocol are different. Therefore, we compare efficiency from the perspective of resource consumption with Eq.(14) in Ref. [42]–[48] as:

$$\eta = \frac{b_s}{q_t + b_t} \tag{14}$$

where q_t is the number of the qubits exchanged in the protocol (the qubits used for checking eavesdropping are not counted), b_t is the number of classical bits exchanged for decoding the message and b_s is the total number of the transmitted message bits. In our protocol, there are three signers who would like to sign a message with n bits. In the initializing phase, the number of shared secret keys is $8n$, the classical bits transmitted is $2n$, the quantum bits transmitted is $6n$; in the signing phase, the number of quantum bits transmitted is $12n$; and in the verifying phase, the number of quantum bits transmitted is $5n$ (These are summarized in Table 7). It means that $b_t = 10n$, $b_s = 25n$ and $q_t = 23n$. Therefore, the efficiency of our quantum sequential signature is:

$$\eta = \frac{25n}{10n + 23n} = 75.76\% \tag{15}$$

It is worth mentioning that we take three signers as an example to compare the efficiency of multi-party signature with Refs. [14], [15]. The specific results are shown in Table 12.

TABLE 12. The efficiency of some different quantum multi-party signature protocols.

	Quantum resource	Efficiency
Wen et al. [15]	GHZ state	60.00%
Liang et al. [14]	Graph state	61.54%
Xu et al. [24]	NOP states	64.29%
Our scheme	Y-SNOP states	75.76%

Moreover, compared with the multi-party signature protocol based on NOP states proposed by Xu *et al.*, the applicant Bob's function has been added to make him more involved in verification of our protocol. It reduces the participation of arbitration in the protocol.

We propose a secure sequential quantum signature protocol for the first time since the idea was pointed out. In the presented protocol, the messages can be signed sequentially by several signers. The function has widely applications in practical management. According to our analysis, the protocol is immune to the attacks from inside and outside. Furthermore, in the process of protocol, the Y-SNOP states of $C^3 \otimes C^3 \otimes C^3$ have been applied to ensure its security. In this view, we give a potential application for the Y-SNOP states proposed by Yuan *et al.* and put forward a series of ideas for the security proof of quantum signature. It may promote the application of quantum information theory in security information, and it is a new topic of quantum cryptography which requires further research. Moreover, this paper has also left some interesting questions for further works, such as how to design other quantum cryptography protocols under the premise of ensuring efficiency and security according to the different properties of NOP states, and the implementation of physical system is still a problem which needs further attention. We believe that the NOP states must have better application scenarios in future.

VI. CONCLUSION

In this paper, we discuss the situation of quantum signature to sign a document with several signers in sequence. By introducing the Y-SNOP states, a novel quantum sequential signature protocol has been designed. Security analysis shows that no one can deny or forge a valid signature, whether the attackers are from outside or inside (independent or joint). Furthermore, compared with the existing quantum multi signature with some NOP states, the present protocol is more efficient and easier to be realized in NISQ device as no entangled resources are required. Finally, we hope that our results will be instructive to the further research of other quantum cryptographic protocols.

REFERENCES

[1] Q. Li, W. H. Chan, and D.-Y. Long, "Arbitrated quantum signature scheme using bell states," *Phys. Rev. A, Gen. Phys.*, vol. 79, no. 5, May 2009, Art. no. 054307.

[2] J.-L. Zhang, M.-S. Hu, Z.-J. Jia, G. Bei, and L.-P. Wang, "A novel E-payment protocol implented by blockchain and quantum signature," *Int. J. Theor. Phys.*, vol. 58, no. 4, pp. 1315–1325, Apr. 2019.

[3] H. Qin, W. K. S. Tang, and R. Tso, "Batch quantum multi-proxy signature," *Opt. Quantum Electron.*, vol. 50, no. 12, Dec. 2018, Art. no. 450, doi: 10.1007/s11082-018-1707-6.

[4] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 4, Apr. 2001, doi: 10.1103/PhysRevA.65.042312.

[5] J.-H. Tian, J.-Z. Zhang, and Y.-P. Li, "A quantum multi-proxy blind signature scheme based on genuine four-qubit entangled state," *Int. J. Theor. Phys.*, vol. 55, no. 2, pp. 809–816, Feb. 2016.

[6] A.-X. Shao, J.-Z. Zhang, and S.-C. Xie, "A quantum multi-proxy multi-blind-signature scheme based on genuine six-qubit entangled state," *Int. J. Theor. Phys.*, vol. 55, no. 12, pp. 5216–5224, Dec. 2016.

[7] H. Qin, W. K. S. Tang, and R. Tso, "Efficient quantum multi-proxy signature," *Quantum Inf. Process.*, vol. 18, no. 2, Feb. 2019, Art. no. 53, doi: 10.1007/s11128-018-2169-2.

[8] X.-J. Wen, Y. Liu, and Y. Sun, "Quantum multi-signature protocol based on teleportation," *Zeitschrift für Naturforschung A*, vol. 62, nos. 3–4, pp. 147–151, Apr. 2007.

[9] Y. Yu-Guang, "Multi-proxy quantum group signature scheme with threshold shared verification," *Chin. Phys. B*, vol. 17, no. 2, pp. 415–418, Feb. 2008.

[10] Y. Yang and Q. Wen, "Threshold proxy quantum signature scheme with threshold shared verification," *Sci. China Ser. G, Phys., Mech. Astron.*, vol. 51, no. 8, pp. 1079–1088, Aug. 2008.

[11] Y. Yu-Guang, W. Yuan, T. Yi-Wei, C. Hai-Ping, and W. Qiao-Yan, "Scalable arbitrated quantum signature of classical messages with multi-signers," *Commun. Theor. Phys.*, vol. 54, no. 1, pp. 84–88, Jul. 2010.

[12] Y. Tian, H. Chen, Y. Gao, H. Zhuang, H. Lian, Z. Han, P. Yu, X. Kong, and X. Wen, "A broadcasting multiple blind signature scheme based on quantum GHZ entanglement," *Int. J. Modern Phys., Conf. Ser.*, vol. 33, Jan. 2014, Art. no. 1460369.

[13] W. Zhang, D. Qiu, X. Zou, and P. Mateus, "Analyses and improvement of a broadcasting multiple blind signature scheme based on quantum GHZ entanglement," *Quantum Inf. Process.*, vol. 16, no. 6, Jun. 2017, Art. no. 150, doi: 10.1007/s11128-017-1602-2.

[14] L. Jian-Wu, L. Xiao-Shu, S. Jin-Jing, and G. Ying, "Multiparty quantum blind signature scheme based on graph states," *Int. J. Theor. Phys.*, vol. 57, no. 8, pp. 2404–2414, Aug. 2018.

[15] X. J. Wen and L. Yun, "A realizable quantum sequential multi-signature scheme," *Acta. Electronica. Sinica.*, vol. 35, no. 6, pp. 1079–1083, 2007.

[16] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, "Hiding bits in bell states," *Phys. Rev. Lett.*, vol. 86, no. 25, pp. 5807–5810, Jun. 2001.

[17] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, "Quantum data hiding," *IEEE Trans. Inf. Theory.*, vol. 48, pp. 580–598, 2002.

[18] T. Eggeling and R. F. Werner, "Hiding classical data in multipartite quantum states," *Phys. Rev. Lett.*, vol. 89, no. 9, Aug. 2002, Art. no. 097905.

[19] W. Matthews, S. Wehner, and A. Winter, "Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding," *Commun. Math. Phys.*, vol. 291, no. 3, pp. 813–843, Nov. 2009.

[20] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 78, no. 4, Oct. 2008, Art. no. 042309, doi: 10.1103/PhysRevA.78.042309.

[21] D.-H. Jiang, J. Wang, X.-Q. Liang, G.-B. Xu, and H.-F. Qi, "Quantum voting scheme based on locally indistinguishable orthogonal product states," *Int. J. Theor. Phys.*, vol. 59, no. 2, pp. 436–444, Feb. 2020.

[22] D.-H. Jiang, Q.-Z. Hu, X.-Q. Liang, and G.-B. Xu, "A trusted third-party E-payment protocol based on locally indistinguishable orthogonal product states," *Int. J. Theor. Phys.*, vol. 59, no. 5, pp. 1442–1450, May 2020.

[23] Y. Xu, G. Xu, and D. Jiang, "Novel quantum proxy signature scheme based on orthogonal quantum product states," *Modern Phys. Lett. B*, vol. 34, no. 16, Jun. 2020, Art. no. 2050172.

[24] D.-H. Jiang, Q.-Z. Hu, X.-Q. Liang, and G.-B. Xu, "A novel quantum multi-signature protocol based on locally indistinguishable orthogonal product states," *Quantum Inf. Process.*, vol. 18, no. 9, Sep. 2019, Art. no. 268, doi: 10.1007/s11128-019-2382-7.

[25] D.-H. Jiang and G.-B. Xu, "Nonlocal sets of orthogonal product states in an arbitrary multipartite quantum system," *Phys. Rev. A, Gen. Phys.*, vol. 102, no. 3, Sep. 2020, Art. no. 032211, doi: 10.1103/PhysRevA.102.032211.

[26] D.-H. Jiang, Y.-L. Xu, and G.-B. Xu, "Arbitrary quantum signature based on local indistinguishability of orthogonal product states," *Int. J. Theor. Phys.*, vol. 58, no. 3, pp. 1036–1045, Mar. 2019.

[27] D.-H. Jiang and G.-B. Xu, "Multiparty quantum key agreement protocol based on locally indistinguishable orthogonal product states," *Quantum Inf. Process.*, vol. 17, no. 7, Jul. 2018, Art. no. 180, doi: 10.1007/s11128-018-1951-5.

[28] S. Halder, M. Banik, S. Agrawal, and S. Bandyopadhyay, "Strong quantum nonlocality without entanglement," *Phys. Rev. Lett.*, vol. 122, no. 4, Feb. 2019, Art. no. 040403, doi: 10.1103/PhysRevLett.122.040403.

[29] P. Yuan, G. Tian, and X. Sun, "Strong quantum nonlocality without entanglement in multipartite quantum systems," *Phys. Rev. A, Gen. Phys.*, vol. 102, no. 4, Oct. 2020, Art. no. 042228, doi: 10.1103/PhysRevA.102.042228.

[30] P. O. Boykin and V. Roychowdhury, "Optimal encryption of quantum bits," *Phys. Rev. A, Gen. Phys.*, vol. 67, no. 4, Apr. 2003, doi: 10.1103/physreva.67.042317.

[31] X. Zou and D. Qiu, "Security analysis and improvements of arbitrated quantum signature schemes," *Phys. Rev. A, Gen. Phys.*, vol. 82, no. 4, Oct. 2010, Art. no. 042325, doi: 10.1103/PhysRevA.82.042325.

[32] F. Gao, S.-J. Qin, F.-Z. Guo, and Q.-Y. Wen, "Cryptanalysis of the arbitrated quantum signature protocols," *Phys. Rev. A, Gen. Phys.*, vol. 84, no. 2, Aug. 2011, Art. no. 022344, doi: 10.1103/PhysRevA.84.022344.

[33] K.-J. Zhang, W.-W. Zhang, and D. Li, "Improving the security of arbitrated quantum signature against the forgery attack," *Quantum Inf. Process.*, vol. 12, no. 8, pp. 2655–2669, Aug. 2013.

[34] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.* New York, NY, USA: IEEE Press, 1984, pp. 175–179.

[35] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, p. 661, 1991.

[36] L.-H. Gong, H.-C. Song, C.-S. He, Y. Liu, and N.-R. Zhou, "A continuous variable quantum deterministic key distribution based on two-mode squeezed states," *Phys. Scripta*, vol. 89, no. 3, Mar. 2014, Art. no. 035101.

[37] G.-F. Zhang and Y. Zhou, "Interplay between the Dzyaloshinskii–Moriya anisotropic antisymmetric interaction and the SWAP operation in a two-qubit heisenberg model," *Phys. Lett. A*, vol. 370, no. 2, pp. 136–138, Oct. 2007.

[38] D. Collins, N. Linden, and S. Popescu, "Nonlocal content of quantum operations," *Phys. Rev. A, Gen. Phys.*, vol. 64, no. 3, Aug. 2001, doi: 10.1103/PhysRevA.64.032302.

[39] Y. Zhou and G.-F. Zhang, "Swap operation in the presence of Zeeman inhomogeneity in coupled quantum dots," *Solid State Commun.*, vol. 178, pp. 28–32, Jan. 2014.

[40] F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, A. Santamato, G. Sinclair, D. Bonneau, M. G. Thompson, and J. C. F. Matthews, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," *Quantum Sci. Technol.*, vol. 3, no. 2, Apr. 2018, Art. no. 025003.

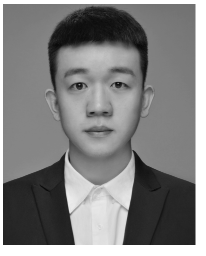
[41] X. M. Guo, C. Cheng, and M. C. Wu, "Parallel real-time quantum random number generator," *Opt. Letters.*, vol. 44, no. 22, pp. 5566–5569, Nov. 2019, doi: 10.1364/OL.44.005566.
[42] A. Cabello, "Quantum key distribution in the Holevo limit," *Phys. Rev. Lett.*, vol. 85, no. 26, pp. 5635–5638, 2000.
[43] Y.-F. He and W.-P. Ma, "Quantum key agreement protocols with four-qubit cluster states," *Quantum Inf. Process.*, vol. 14, no. 9, pp. 3483–3498, Sep. 2015.
[44] K.-J. Zhang, X. Zhang, H.-Y. Jia, and L. Zhang, "A new n-party quantum secret sharing model based on multiparty entangled states," *Quantum Inf. Process.*, vol. 18, no. 3, Mar. 2019, Art. no. 81, doi: 10.1007/s11128-019-2201-1.
[45] W. Huang, B.-J. Xu, J.-T. Duan, B. Liu, Q. Su, Y.-H. He, and H.-Y. Jia, "Authenticated quantum key distribution with collective detection using single photons," *Int. J. Theor. Phys.*, vol. 55, no. 10, pp. 4238–4256, Oct. 2016.
[46] H.-J. Cao, J.-F. Zhang, J. Liu, and Z.-Y. Li, "A new quantum proxy multi-signature scheme using maximally entangled seven-qubit states," *Int. J. Theor. Phys.*, vol. 55, no. 2, pp. 774–780, Feb. 2016.
[47] X.-B. Chen, X. Tang, G. Xu, Z. Dou, Y.-L. Chen, and Y.-X. Yang, "Cryptanalysis of secret sharing with a single d-level quantum system," *Quantum Inf. Process.*, vol. 17, no. 9, Sep. 2018.
[48] S. Lin, G.-D. Guo, F. Huang, and X.-F. Liu, "Quantum anonymous ranking based on the Chinese remainder theorem," *Phys. Rev. A, Gen. Phys.*, vol. 93, no. 1, Jan. 2016, Art. no. 012318, doi: 10.1103/PhysRevA.93.012318.

XU ZHAO is currently pursuing the M.S. degree with Heilongjiang University, China.

Her current research interests include quantum secret sharing, quantum signature, and quantum computing.

KE-JIA ZHANG received the Ph.D. degree in cryptography from the Beijing University of Posts and Telecommunications.

He is currently a Professor with the School of Mathematical Sciences, Heilongjiang University, China. His current research interests include quantum signature, quantum secret sharing, quantum secure multiparty computing, quantum machine learning, and quantum computing.



BAO-MIN ZHOU is currently pursuing the Ph.D. degree with the University of Science and Technology of China.

His current research interests include block cipher analysis and quantum cryptography.