A Quantum Dual-Signature Protocol Based on SNOP States without Trusted Participant

Kejia Zhang 1,2,3, Xu Zhao 1, Long Zhang 1,*, Guojing Tian 4 and Tingting Song 5,6

1 School of Mathematical Science, Heilongjiang University, Harbin 150080, China; zhangkejia@hlju.edu.cn (K.Z.); 2190972@163.com (X.Z.)
2 State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
3 Laboratory of Cryptology and Cyberspace Security, Heilongjiang University, Harbin 150080, China
4 Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China; tianguojing@ict.ac.cn
5 College of Information Science and Technology, Jinan University, Guangzhou 510632, China; tingtingsong@jnu.edu.cn
6 Guangxi Key Laboratory of Cryptography and Information Security, Guilin 54100, China
* Correspondence: lzhang@hlju.edu.cn

Abstract: Quantum dual-signature means that two signed quantum messages are combined and expected to be sent to two different recipients. A quantum signature requires the cooperation of two verifiers to complete the whole verification process. As an important quantum signature aspect, the trusted third party is introduced to the current protocols, which affects the practicability of the quantum signature protocols. In this paper, we propose a quantum dual-signature protocol without arbitrator and entanglement for the first time. In the proposed protocol, two independent verifiers are introduced, here they may be dishonest but not collaborate. Furthermore, strongly nonlocal orthogonal product states are used to preserve the protocol security, i.e., no one can deny or forge a valid signature, even though some of them conspired. Compared with existing quantum signature protocols, this protocol does not require a trusted third party and entanglement resources.

Keywords: quantum dual-signature; strongly nonlocal orthogonal product states; untrusted third party

1. Introduction

With the development of the Internet, network communications have become more and more frequent in daily life. Therefore, it is particularly important to improve the security of network communications. Digital signatures are not only widely employed to authenticate the identity of communication participants, but also ensure the integrity of legal messages. For example, encrypting and signing the transmitted messages, verifying the identity of all parties, are necessary to ensure the security of network communications.

As we know, the applied classic digital signature protocols are based on computational complexity, such as the decomposition of a large prime number. However, with the development of quantum algorithms [1], classic cryptographic protocols are becoming increasingly insecure. Fortunately, various quantum cryptography protocols, such as quantum key distribution (QKD) [2–4], controlled quantum teleportation [5–10], quantum secret sharing [11–15] and quantum secure direct communication [16–19], can be implemented on quantum networks [20–24]. Since their security is based on the laws of quantum mechanics, they are immune to the attacks on quantum computers. During them, designing digital signature protocols based on quantum technology is an important research aspect of quantum cryptographic protocols.
In 2001, Gottesman et al. [25] first proposed a quantum digital signature based on the fundamental principles of quantum physics, i.e., a quantum analogue of one-way functions which required $O(m)$ qubits is used to encrypt an $m$-bit message. In 2002, Zeng et al. [26] put forward a signature protocol based on the GHZ states, whose realization depends upon a trust arbitrator. Since then, many variations of quantum signature protocols have been presented. For example, Li et al. [27] proposed an arbitrated quantum signature protocol using Bell states instead of GHZ states. Zou et al. [28] presented an arbitrated quantum signature protocol without using entangled states. In 2016, Liu et al. [29] proposed a quantum dual-signature protocol, which combines two signed messages expected to be sent to two different recipients. In their protocol, the entanglement swapping with coherent states is applied. Compared to classic signatures, the quantum signature which involves quantum algorithms, could be more secure and efficient. As we know, quantum signatures also have wide applications in the ecommerce system as classic signatures.

All these protocols are based on the assumption that a trusted third party exists in the quantum network, though this is not practical. In 2015, Kang et al. [30] first proposed a controlled mutual quantum entity authentication using entanglement swapping by introducing an untrusted third party. However, the controller may perform an internal attack, because the others do not test the correlation of the entangled state. In order to prevent this security loophole, a checking procedure was added to confirm the correlation of the entangled state (see Ref. [31]). Nevertheless, Wang et al. [32] pointed out that there is still a secure flaw in Kang’s improved protocol [31], that is, the untrusted third party can obtain the shared key between the other participants without being detected. In 2016, Li et al. [33] proposed a secure quantum blind dual-signature scheme without arbitrators. It does not rely on an arbitrator in the verification phase as the previous quantum signature schemes do. The security is guaranteed by the entanglement in quantum information processing. Compared with the existing quantum signature protocols, it reduces the over rights of the third party in verification. However, the research on quantum digital signatures without arbitrators is still in its infancy.

The existing quantum digital signatures without arbitrators are usually implemented by entangled states. As we know, the preparation of entanglement in experiments is difficult. Therefore, it is very urgent to propose a more practical quantum signature protocol without arbitrators. Recently, the expression of quantum nonlocality has attracted more attention. In 2019, Halder et al. [34] first proposed a 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 systems. For the sake of simplicity, we define these states as SNOP states. Compared with normal nonlocal orthogonal product states, SNOP states have strong quantum nonlocality for tripartite, i.e., they are locally irreducible in every bipartition. In this situation, if the private messages are encoded into SNOP states, the security of the private messages is ensured. This means that the attacker cannot determine the accurate whole state even if they obtain two particles of the SNOP states. A secure quantum signature protocol has to meet at least two requirements, i.e., non-forgery and non-repudiation. In this case, we propose a quantum dual-signature protocol based on SNOP states without a trusted third party. The security of our protocol is guaranteed by the secret encryption algorithm [35] and SNOP states. The encryption algorithm is mainly used to resist external attackers. Furthermore, each bipartite of the SNOP states is locally irreducible to resist internal attacks. In this case, the security of our protocol is shown, i.e., neither an external attacker nor an internal one can forge a signature. Moreover, no one can deny the signature.

The rest of the paper is arranged as follows: In Section 2, some preliminary theories are introduced. In Section 3, we describe the quantum dual-signature protocol including the initializing phase, signing phase and verification phase. The security of our protocol is analyzed in Section 4. Finally, a short conclusion is given in Section 5.
2. Preliminaries

In this section, we describe an encryption algorithm—Key-Controlled-'I'QOTP. Then, a set of SNOP states to encode messages are introduced.

2.1. Key-Controlled-'I'QOTP

As we know, the quantum one time pad (QOTP) is an important way to generate quantum signatures [36]. However, Gao et al. [37] pointed out that there exist some security problems in these protocols. In the above 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 2013, Zhang et al. [35] presented two types of improved encryption algorithms, called Key-Controlled-'T'QOTP and Key-Controlled-'I'QOTP, to prevent forgery attacks effectively. Here, we briefly introduce Key-Controlled-'I'QOTP.

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

**Table 1. Corresponding encryption operators in “Key-Controlled-'I'QOTP”**.

| $K_iK_{2n+i}$ | 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             | $W_{11} = \frac{1}{2} (I + i\sigma_x + i\sigma_y + i\sigma_z)$ |

$$|S\rangle = \bigotimes_{i=1}^n \sigma_x^{K_{2i}} \sigma_z^{K_{2i+1}} W_{K_iK_{2n+i}} |P\rangle$$ (1)

Here, we take $n = 1$, $i = 1$, $|P\rangle = \alpha |0\rangle + \beta |1\rangle$ and $K_1K_2 = 00$ as an example to demonstrate how to encrypt quantum states using secret keys. This is the way to generate quantum signatures in subsequent protocols.

$$|S\rangle = \bigotimes_{i=1}^1 \sigma_x^{K_{i}} \sigma_z^{K_{i+1}} W_{K_iK_{i+1}} (\alpha |0\rangle + \beta |1\rangle)$$

$$= \sigma_x \sigma_z W_{00} (\alpha |0\rangle + \beta |1\rangle)$$

$$= \frac{1}{\sqrt{2}} (|0\rangle|1\rangle + |1\rangle|0\rangle + |0\rangle|0\rangle - |1\rangle|1\rangle)(\alpha |0\rangle + \beta |1\rangle)$$

$$= \frac{1}{\sqrt{2}} (\alpha |1\rangle + \alpha |0\rangle + \beta |0\rangle - \beta |1\rangle)$$

$$= \frac{1}{\sqrt{2}} ((\alpha + \beta) |0\rangle + (\alpha - \beta) |1\rangle)$$ (2)
Zhang et al. proved that this encryption algorithm can be applied to generate signatures which cannot be forged by the receiver. Therefore, in order to ensure security, Key-Controlled-'I'QOTP is used in the following quantum dual-signature protocol.

2.2. SNOP States

In order to show our protocol, a type of SNOP states is introduced.

\[
|1\rangle |2\rangle |1\pm 2\rangle, |2\rangle |1\pm 2\rangle |1\rangle, |1\pm 2\rangle |1\rangle |2\rangle \\
|1\rangle |3\rangle |1\pm 3\rangle, |3\rangle |1\pm 3\rangle |1\rangle, |1\pm 3\rangle |1\rangle |3\rangle \\
|2\rangle |3\rangle |1\pm 2\rangle, |3\rangle |1\pm 2\rangle |2\rangle, |1\pm 2\rangle |2\rangle |3\rangle \\
|3\rangle |2\rangle |1\pm 3\rangle, |2\rangle |1\pm 3\rangle |3\rangle, |1\pm 3\rangle |3\rangle |2\rangle \\
|1\rangle |1\rangle |1\rangle, |2\rangle |2\rangle |2\rangle, |2\rangle |3\rangle |3\rangle
\]  

(3)

In Ref. [34], these states are proved to be locally irreducible in all bipartitions. Since local irreducibility is a sufficient condition for strong nonlocality, these states are strongly nonlocal. In this situation, as the messages are encoded into SNOP states, the security of the private messages is ensured. This means that the attacker cannot determine the accurate forms even if they obtain two particles of the SNOP states.

3. Quantum Dual-Signature Protocol with SNOP States

In this section, a quantum dual-signature protocol is given. Firstly, the identity of the participants and the process of the protocol are described in Section 3.1. Then, the specific protocol process is divided into the following three phases: the initializing phase, signing phase and verification phase.

3.1. Brief Description

There exist three roles in our protocol:

1. Alice is the applicant and signer;
2. Bob is the first verifier of the message;
3. Charlie is the second verifier.

When the applicant Alice needs to warrant a document, she first signs the application document; then, she sends the document to the first verifier Bob to verify one part of the document; next, Bob sends it to Charlie to verify the other part. The process of this protocol can be briefly seen in Figure 1.
3.2. Initializing Phase

Step I (Secret Key Assignment): Alice shares the two keys' sequences \( K_{ab} \) and \( K_{ac} \) with Bob and Charlie, respectively. Bob shares the key sequence \( K_{bc} \) with Charlie. This can be achieved with the quantum key distribution (QKD) technique [2–4].

Step II (Message Encoding): The message \( M \) is divided into \( n \) groups, \( M = M_1 \| M_2 \| \cdots \| M_n \); here \( M_t \) is a 4-bit of a classical bit sequence, where \( t = 1, 2, 3, \ldots, n \). Alice encodes each \( M_t \) to a quantum sequence \(| S \rangle \) with the 16 states in Table 2; the remaining 11 states are used to detect eavesdropping in Table 3.

| Message | States | Message | States |
|---------|--------|---------|--------|
| \( M_1 = 0000 \) | \(| \varphi_1 \rangle = |1\rangle |2\rangle |1+2\rangle \) | \( M_1 = 1111 \) | \(| \varphi_{10} \rangle = |1\rangle |2\rangle |1-2\rangle \) |
| \( M_2 = 0001 \) | \(| \varphi_2 \rangle = |1\rangle |3\rangle |1+3\rangle \) | \( M_2 = 1110 \) | \(| \varphi_{11} \rangle = |1\rangle |3\rangle |1-3\rangle \) |
| \( M_3 = 0010 \) | \(| \varphi_3 \rangle = |2\rangle |3\rangle |1+2\rangle \) | \( M_3 = 1101 \) | \(| \varphi_{12} \rangle = |2\rangle |3\rangle |1-2\rangle \) |
| \( M_4 = 0100 \) | \(| \varphi_4 \rangle = |3\rangle |2\rangle |1+3\rangle \) | \( M_4 = 1011 \) | \(| \varphi_{13} \rangle = |3\rangle |2\rangle |1-3\rangle \) |
| \( M_5 = 1000 \) | \(| \varphi_5 \rangle = |1+2\rangle |1\rangle |2\rangle \) | \( M_5 = 0111 \) | \(| \varphi_{14} \rangle = |1\rangle |2\rangle |1\rangle |2\rangle \) |
| \( M_6 = 1001 \) | \(| \varphi_6 \rangle = |1+3\rangle |1\rangle |3\rangle \) | \( M_6 = 0110 \) | \(| \varphi_{15} \rangle = |1\rangle |3\rangle |1\rangle |3\rangle \) |
| \( M_7 = 1010 \) | \(| \varphi_7 \rangle = |1+2\rangle |2\rangle |3\rangle \) | \( M_7 = 0011 \) | \(| \varphi_{16} \rangle = |1\rangle |3\rangle |3\rangle |2\rangle \) |
| \( M_8 = 1100 \) | \(| \varphi_8 \rangle = |1+3\rangle |3\rangle |2\rangle \) |

Table 3. SNOP states used to detect eavesdropping.

| Decoy State | States |
|-------------|--------|
| \(| \varphi_{10} \rangle = |2\rangle |1+2\rangle |2\rangle \) | \(| \varphi_{11} \rangle = |2\rangle |1-2\rangle |2\rangle \) |
| \(| \varphi_{01} \rangle = |3\rangle |1+3\rangle |1\rangle \) | \(| \varphi_{12} \rangle = |3\rangle |1-3\rangle |1\rangle \) |
| \(| \varphi_{02} \rangle = |3\rangle |1+2\rangle |2\rangle \) | \(| \varphi_{13} \rangle = |3\rangle |1-2\rangle |2\rangle \) |
| \(| \varphi_{03} \rangle = |2\rangle |1+3\rangle |3\rangle \) | \(| \varphi_{14} \rangle = |2\rangle |1-3\rangle |3\rangle \) |
| \(| \varphi_{04} \rangle = |1\rangle |1\rangle |1\rangle \) | \(| \varphi_{15} \rangle = |2\rangle |2\rangle |2\rangle \) |
| \(| \varphi_{05} \rangle = |3\rangle |3\rangle |3\rangle \) |

Step III (Generating Quantum Sequence): Alice generates three identical sequences \(| S \rangle \), where the first sequence is denoted by \(| S^a \rangle \), the second one is \(| S^b \rangle \) and the last one is \(| S^c \rangle \). By picking out each particle of above sequences, the corresponding quantum sequences \(| S_{i}^a \rangle , | S_{i}^b \rangle , | S_{i}^c \rangle , | S_{i}^b \rangle , | S_{i}^b \rangle , | S_{i}^b \rangle , | S_{i}^b \rangle , | S_{i}^b \rangle , | S_{i}^b \rangle \) and \(| S_{i}^c \rangle \) are generated.

For example, we suppose that \(| S \rangle = | \varphi_1 \rangle | \varphi_2 \rangle | \varphi_3 \rangle | \varphi_4 \rangle | \varphi_{13} \rangle | \varphi_{14} \rangle | \varphi_{15} \rangle | \varphi_{16} \rangle \). Then, the specific forms of \(| S^a \rangle , | S^b \rangle \) and \(| S^c \rangle \) are depicted in Equation (4).

\[
| S^a \rangle = |1\rangle |1\rangle |2\rangle |3\rangle |1-2\rangle |1-3\rangle |1-2\rangle |1-3\rangle \\
| S^b \rangle = |2\rangle |3\rangle |3\rangle |2\rangle |1\rangle |2\rangle |3\rangle \\
| S^c \rangle = |1+2\rangle |1+3\rangle |1+2\rangle |1+3\rangle |2\rangle |3\rangle |3\rangle |2\rangle \\
\text{(4)}
\]
3.3. Signing Phase

Step S (Sending Sequence to Bob): Firstly, Alice encrypts $|S^a_S\rangle$ and $|S^b_S\rangle$ with $K_{AB}$ to obtain $|\widetilde{S}^a_S\rangle$ and $|\widetilde{S}^b_S\rangle$; then, she encrypts $|S^a_S\rangle$, $|S^b_S\rangle$, $|\widetilde{S}^a_S\rangle$ and $|\widetilde{S}^b_S\rangle$ with $K_{AC}$ to obtain $S_{AC}$.

$$S_{AC} = E_{K_{AC}}\{|S^a_S\rangle, |S^b_S\rangle, |\widetilde{S}^a_S\rangle, |\widetilde{S}^b_S\rangle\} \quad (5)$$

Secondly, Alice encrypts $|S^a_S\rangle$ and $|S^c_S\rangle$ with $K_{AC}$ to obtain $|\widetilde{S}^a_S\rangle$ and $|\widetilde{S}^c_S\rangle$; then, she encrypts $|S^a_S\rangle$, $|S^b_S\rangle$, $|\widetilde{S}^a_S\rangle$, $|\widetilde{S}^b_S\rangle$ and $S_{AC}$ with $K_{AB}$ to obtain $S_{AB}$ as her signature. Finally, she inserts the decoy states randomly in $S_{AB}$ to obtain $S'_{AB}$ and sends it to Bob. The symbolic representation can be seen in Table 4.

$$S_{AB} = E_{K_{AB}}\{|S^a_S\rangle, |S^b_S\rangle, |\widetilde{S}^a_S\rangle, |\widetilde{S}^b_S\rangle, |\widetilde{S}^c_S\rangle, S_{AC}\} \quad (6)$$

| Sequence | Signature |
|----------|-----------|
| $|S^a_S\rangle$ | $E_{K_{AC}}\{|S^a_S\rangle\}$ |
| $|S^c_S\rangle$ | $E_{K_{AC}}\{|S^c_S\rangle\}$ |
| $|S^a_S\rangle$ | $E_{K_{AB}}\{|S^a_S\rangle\}$ |
| $|S^b_S\rangle$ | $E_{K_{AB}}\{|S^b_S\rangle\}$ |

3.4. Verification Phase

Step V1 (Detect Eavesdropping): After Bob announces that he has received the sequences $S'_{AB}$, Alice tells Bob the positions and the initial states of the decoy particles. Then, Bob measures each of the decoy particles with the corresponding basis and compares the measurement outcome with its initial state to check for eavesdropping. If the error probability is within a certain threshold, Bob recovers the sequences $S_{AB}$; otherwise, he aborts the protocol.

Step V2 (Bob’s Verification of the First Stage): Bob decrypts $S_{AB}$ and verifies whether $|S^a_S\rangle$ is equal to $|S^b_S\rangle$ with SWAP operations [38–40]. Here, $V_{B_V}$ represents the results.

$$D_{K_{AB}}\{S_{AB}\} = \{|S^a_S\rangle, |S^b_S\rangle, |\widetilde{S}^a_S\rangle, |\widetilde{S}^b_S\rangle, |\widetilde{S}^c_S\rangle, S_{AC}\} \quad (7)$$

$$V_{B_V} = \begin{cases} 1, & |S^a_S\rangle = |S^b_S\rangle \\ 0, & |S^a_S\rangle \neq |S^b_S\rangle \end{cases} \quad (8)$$

If $V_{B_V} = 0$, he rejects the quantum signature directly; otherwise, he sends $S_B$ to Charlie.

$$S_B = E_{K_{AC}}\{|\widetilde{S}^a_S\rangle, |\widetilde{S}^c_S\rangle, S_{AC}\} \quad (9)$$
Step V3 (Charlie’s Verification of the First Stage): Charlie decrypts $S_b$, verifies whether $|S_2^a\rangle$ is equal to $|S_2^c\rangle$ and generates $V_C$.

\[
D_{k_{bc}} \{S_b\} = \{|\widetilde{S}_2^a\rangle, |\widetilde{S}_2^c\rangle, S_{ac}\}
\]

(10)

\[
D_{k_{ac}} \{|\widetilde{S}_2^a\rangle, |\widetilde{S}_2^c\rangle\} = \{|S_2^a\rangle, |S_2^c\rangle\}
\]

(11)

\[
V_C = \begin{cases} 
1, & |S_2^a\rangle = |S_2^c\rangle \\
0, & |S_2^a\rangle \neq |S_2^c\rangle 
\end{cases}
\]

(12)

If $V_C$ is equal to 0, Charlie will reject the quantum signature directly; otherwise, he will decrypt $S_{ac}$ and send $S_C$ to Bob.

\[
D_{k_{ac}} \{S_{ac}\} = \{|S_1^a\rangle, |S_1^c\rangle, |\widetilde{S}_3^a\rangle, |\widetilde{S}_3^c\rangle\}
\]

(13)

\[
S_C = E_{k_{bc}} \{|\widetilde{S}_3^a\rangle, |\widetilde{S}_3^c\rangle\}
\]

(14)

Step V4 (Bob’s Verification of the Second Stage): Bob first decrypts $S_C$ with $K_{bc}$ and $K_{ab}$; then, he verifies whether $|S_1^a\rangle$ is equal to $|S_1^b\rangle$ and generates $V_{B_2}$.

\[
D_{k_{ac}} \{S_C\} = |S_1^a\rangle, |\widetilde{S}_3^a\rangle
\]

(15)

\[
D_{k_{ac}} \{|\widetilde{S}_3^a\rangle, |\widetilde{S}_3^c\rangle\} = |S_3^a\rangle, |S_3^c\rangle
\]

(16)

\[
V_{B_2} = \begin{cases} 
1, & |S_3^a\rangle = |S_3^c\rangle \\
0, & |S_3^a\rangle \neq |S_3^c\rangle 
\end{cases}
\]

(17)

If $V_{B_2}$ is equal to 0, Bob will reject the quantum signature directly; otherwise, he will recover the sequence $|S\rangle$ by $|S_1^a\rangle$, $|S_2^a\rangle$ and $|S_3^b\rangle$ to obtain $m_j^b$ according to the rule in Table 5.

Step V5 (Charlie’s Verification of the Second Stage): Similarly, Charlie recovers the sequence $|S\rangle$ according to $|S_1^a\rangle$, $|S_2^c\rangle$ and $|S_3^c\rangle$, by the rules in Table 5, to obtain $m_j^c$. If $m_j^b = m_j^c$, Charlie will announce it is the valid signature of $m_j$; otherwise, he will reject this signature. The process can be briefly seen in Figure 2.
Figure 2. Brief summary of protocol process.

Table 5. Verifier’s measurement rules.

| Message | Bases |
|---------|-------|
| $M_r = 0000 \mapsto |\phi_1\rangle = |1\rangle |2\rangle |1+2\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_1$ |
| $M_r = 1111 \mapsto |\phi_2\rangle = |1\rangle |2\rangle |1-2\rangle$ | $\{|1+2\rangle, |1-2\rangle, |3\rangle\}_3$ |
| $M_r = 0001 \mapsto |\phi_3\rangle = |1\rangle |3\rangle |1+3\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_1$ |
| $M_r = 1110 \mapsto |\phi_{10}\rangle = |1\rangle |3\rangle |1-3\rangle$ | $\{|1+3\rangle, |1-3\rangle, |2\rangle\}_3$ |
| $M_r = 0010 \mapsto |\phi_4\rangle = |2\rangle |3\rangle |1+2\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_1$ |
| $M_r = 1101 \mapsto |\phi_{11}\rangle = |2\rangle |3\rangle |1-2\rangle$ | $\{|1+2\rangle, |1-2\rangle, |3\rangle\}_3$ |
| $M_r = 0100 \mapsto |\phi_5\rangle = |3\rangle |2\rangle |1+3\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_1$ |
| $M_r = 1011 \mapsto |\phi_{12}\rangle = |3\rangle |2\rangle |1-3\rangle$ | $\{|1+3\rangle, |1-3\rangle, |2\rangle\}_3$ |
| $M_r = 1000 \mapsto |\phi_6\rangle = |1+2\rangle |1\rangle |2\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_1$ |
| $M_r = 0111 \mapsto |\phi_{13}\rangle = |1-2\rangle |1\rangle |2\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_3$ |
| $M_r = 1001 \mapsto |\phi_7\rangle = |1+3\rangle |1\rangle |3\rangle$ | $\{|1+3\rangle, |1-3\rangle, |2\rangle\}_1$ |
| $M_r = 0110 \mapsto |\phi_{14}\rangle = |1-3\rangle |1\rangle |3\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_2$ |
| $M_r = 1010 \mapsto |\phi_8\rangle = |1+2\rangle |2\rangle |3\rangle$ | $\{|1+2\rangle, |1-2\rangle, |3\rangle\}_1$ |
| $M_r = 0101 \mapsto |\phi_{15}\rangle = |1-2\rangle |2\rangle |3\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_3$ |
| $M_r = 1100 \mapsto |\phi_{16}\rangle = |1+3\rangle |3\rangle |2\rangle$ | $\{|1+3\rangle, |1-3\rangle, |2\rangle\}_1$ |
| $M_r = 0011 \mapsto |\phi_{17}\rangle = |1-3\rangle |3\rangle |2\rangle$ | $\{|1\rangle, |2\rangle, |3\rangle\}_3$ |
4. Security and Efficiency Analysis

As mentioned above, a secure quantum signature protocol has to meet at least two requirements, i.e., non-forgery and non-repudiation. In our protocol, the above requirements are completely satisfied. The security of our protocol is guaranteed by the secret encryption algorithm Key-Controlled-TQOTP and SNAP states. The encryption algorithm is mainly used to resist external attackers. Furthermore, each bipartite of the SNAP states is locally irreducible to resist internal attacks. In this case, the security of our protocol is shown, i.e., neither an external attacker nor an internal one can forge a signature. Moreover, no one can deny the signature. The specific analysis can be seen in the following subsections.

4.1. Non-Forgery

4.1.1. Resistance to Outside Attacks Based on Encryption Algorithm

(i) Eve Forges Alice’s Signature.

In order to forge Alice’s signature, Eve has to intercept the sequences in Step 5. Then, he could change Alice’s signature and replace \( S'_{AB} \) with \( S''_{AB} \). However, since the original keys are shared with QKD, it is impossible for her to succeed. If he attempts to forge Alice’s signature without \( K_{AB} \), he will perform an operator corresponding to the signature and message. In our protocol, as Key-Controlled-TQOTP is used to generate signature \( S'_{AB} \), he would not be able to identify the forms of encryption operators except for Alice and Bob, as shown in Table 6.

| Encryption | Eve’s Possible Decryptions | Eve’s Forgery of Operation | Signature |
|------------|----------------------------|--------------------------|-----------|
| \( I \)    | \( W_i^+ QW_i \)            | \( \sigma \)             | 00 01 10 11 |
| \( \sigma_z \) | \( W_i^+ \sigma_z Q\sigma_z W_i \) | \( \sigma_z \) | \( \sigma_z \sigma_z \sigma_z \) |
| \( \sigma_x \) | \( W_i^+ \sigma_x Q\sigma_x W_i \) | \( \sigma_x \) | \( \sigma_x \sigma_x \sigma_x \) |
| \( \sigma_y \) | \( W_i^+ \sigma_y Q\sigma_y W_i \) | \( \sigma_y \) | \( \sigma_x \sigma_y \sigma_x \sigma_y \) |

From Table 6, it can be seen that, if Eve wants to forge one qubit of Alice’s signature with \( \sigma_x \) or \( \sigma_y \), the probability of success will be \( \frac{1}{3} \). Moreover, the probability will be \( \frac{1}{2} \) if the forgery operation is \( \sigma_z \). Furthermore, if the length of the message is \( m \), the probability \( P_E \) of Eve’s forgery’s success will be

\[
P_E = \left( \frac{1}{3} \right)^k \left( \frac{1}{2} \right)^{m-k}
\]

(18)

where \( k (0 \leq k \leq m, 0 \leq m \leq n) \) represents the total number of qubits which Eve wants to forge the sequence by \( \sigma_x \) and \( \sigma_y \); \( m-k \) represents the number of qubits forged by \( \sigma_z \). With this encryption algorithm, Eve can be detected during Bob’s verification phase.

(ii) Eve Forges Bob’s Verification Results.

For Eve to intercept the sequences in Step V2, he has to change the sequence \( S_B \) with \( S_B' \) and send it to Charlie. Similarly, Eve cannot know the secret key \( K_{BC} \). Therefore, Eve’s forgery will be discovered by Charlie once Eve changes only a small part of
Similarly, if Eve forges Charlie’s verification results, similarly, his forgery will be found by Bob.

4.1.2. Resistance to Inside Attacks Based on SNOP States

Above, we guarantee that two verifiers are not dishonest at the same time. This assumption is satisfied with the actual situation. In fact, if both verifiers are dishonest, the protocol will be insecure and impractical. Here, we discuss the dishonesty of the verifier, specifically in the case in which one verifier wants to forge a signature to evade the verification of the other one.

According to our analysis above, the encryption algorithm can resist some forgery attacks, but, for internal attackers who know the secret key, the security needs to be further discussed as follows. Here, SNOP states provides a nature property for resisting internal attacks, i.e., they are locally irreducible in every bipartition. This means that the attacker cannot determine the accurate whole state even if they obtain two particles of the SNOP states. The specific analysis can be seen in the following subsections.

(i) Bob’s Forgery.

This is different from Eve’s forgery of Alice’s signature; Bob does not need to intercept the sequences because he has the secret key $K_{AB}$. If he attempts to replace $S_{AC}$ with $S'_{AC}$ in Step V2, his forgery will not succeed. Since the sequences $S_{AC}$ are generated by Key-Controlled-TQOTP with the key $K_{AC}$, Bob cannot identify the forms of encryption operators, except for Alice and Charlie. Similar to the analysis above, Bob’s forgery will be discovered by Charlie in Step V3.

Based on the analysis above, we assume that Bob attempts to restore all the SNOP states by the sequences $|S^A_1\rangle$ and $|S^B_1\rangle$. He can only choose the measurement basis randomly. There are three possible cases seen in Table 7. The probability that he chooses any basis is $\frac{1}{3}$. From Table 7, we can deduce that the probability of choosing the correct measurement basis and obtain one bit, as shown in Equation (19).

| Table 7. Measurement basis and possible measurement results of attackers. |
|---|---|---|---|---|---|---|---|
| State | $|1\rangle$ | $|2\rangle$ | $|3\rangle$ | $|1+2\rangle$ | $|1-2\rangle$ | $|1+3\rangle$ | $|1-3\rangle$ |
| $A_1 = \{|1\rangle, |2\rangle, |3\rangle\}$ | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| $A_2 = \{|1+2\rangle, |1-2\rangle, |3\rangle\}$ | 0 | 0 | 1 | 1 | 1 | 0 | 0 |
| $A_3 = \{|1+3\rangle, |1-3\rangle, |2\rangle\}$ | 0 | 1 | 0 | 0 | 1 | 1 | 1 |

$$P = \frac{1}{3} \times 1 + \frac{1}{3} \times 2 + \frac{1}{3} \times 1 + \frac{1}{3} \times 2 + \frac{1}{3} \times 1 + \frac{1}{3} \times 1 + \frac{1}{3} \times 1 = \frac{3}{16} \quad (19)$$

For the $n$ length of the quantum sequence, it is not difficult to see that the probability of Bob’s successful attack $P'$ tends to be zero with the increase in $n$ in Equation (20).

$$P' = P^n = \left(\frac{3}{16}\right)^n \quad (20)$$

(ii) Charlie’s Forgery.

We assume Charlie tries to modify $|S^A_1\rangle$ and $|S^B_1\rangle$ according to the sequence $|S^A_1\rangle$ in his hands to make $|S^A_1\rangle$ and $|S^B_1\rangle$ equal. Similarly, Charlie cannot identify the
forms of the encryption operators without the key $K_{AB}$. If $|S_x^a \neq |S_x^b\rangle$, Charlie’s forgery will be discovered by Bob in Step V4. The process can be briefly seen in Figure 3.

**Figure 3.** The process of verification phase.

### 4.2. Non-Repudiation

Alice could attempt to deny her signature in two ways. One is directly denying her signature. Here Alice’s signatures $S_{AB}$ and $S_{AC}$ are generated by $K_{AB}$ and $K_{AC}$, only known to Bob and Charlie. Once Bob and Charlie have verified the validity of the signatures, she will not be able to deny them. Moreover, since Key-Controlled-'I'QOTP is used, no one can find the corresponding location without knowing $K_{AB}$ and $K_{AC}$. If $|S_x^a \neq |S_x^b\rangle$ and $|S_x^c \neq |S_x^c\rangle$, it will be impossible for Alice to deny.

The other way is that Alice denied the signature after Bob verified it. If $m_j^b = m_j^c$, Bob and Charlie will be able to judge whether Alice denies. The sequences $|S_x^a\rangle$ and $|S_x^c\rangle$ are encrypted with the key $K_{AB}$ and the key $K_{AB}$ is generated by Key-Controlled-'I'QOTP. Therefore, Charlie cannot know the secret key $K_{AB}$. If Charlie attempts to modify the sequence, Bob will find this attack in Step V4. Similarly, Alice will not succeed in denying the signature after Charlie’s verification.

### 5. Discussion and Conclusions

We summarize and compare our protocol with the quantum signature protocols proposed above in Table 8. Compared with the existing quantum signature protocols, our protocol does not need a trusted third party and entanglement resources for the first time.

**Table 8.** Comparison among some different quantum signature protocols.

| Protocol            | Resources   | Trust Third Party | Contribution                                      |
|---------------------|-------------|-------------------|--------------------------------------------------|
| Zeng et al. [26]    | GHZ states  | Yes               | Arbitrated quantum signature (AQS) protocol is proposed for the first time. |
Comparing with the existing quantum signature protocols, the signature of our protocol requires the cooperation of two verifiers to complete the whole verification process without an arbitrator. In this case, the function has wide applications in practical management. By introducing SNOP states, the present protocol seems more efficient and easier to be realized in noisy intermediate-scale quantum (NISQ) devices, as no entangled resources are required. According to our analysis, the protocol based on SNOP states is immune to attacks from the inside and outside. In other words, the attacker cannot determine the accurate whole state even if they obtain two particles of the SNOP states. Furthermore, we give a potential application for the SNOP states and put forward a series of ideas. We think SNOP states could also be applied to electronic payments, voting systems and so on. Moreover, we believe that SNOP states must have better application scenarios in the future. Finally, we hope that our results are instructive to further research on other quantum cryptographic protocols.

**Author Contributions:** Conceptualization, X.Z. and K.Z.; methodology, X.Z.; software, X.Z.; validation, X.Z., K.Z., L.Z., G.T. and T.S.; writing—original draft preparation, X.Z.; writing—review and editing, X.Z., K.Z. and L.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the National Natural Science Foundation of China under Grant No. 61802118 and No. 61801459, the National Postdoctoral Program for Innovative Talent Grant No. BX20190335, the Natural Science Foundation of Heilongjiang Province under Grant No. YQ2020-F013, the University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province under Grant No. UNPYSCT-2018015, the Anhui Initiative in Quantum Information Technologies Grant No. AHY150100, the Central Universities Grant No. 21620433, the Guangxi Key Laboratory of Cryptography and Information Security Grant No. GCIS201922 and the open Foundation of State key Laboratory of Networking and Switching Technology (BUPT) under Grant No. SKLNST-2018-1-07. The Outstanding Youth Fund of Heilongjiang University supported Kejia Zhang, the Heilongjiang University Innovation Fund Grant No.YJSCX2021-082HIJU.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

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

The following abbreviations are used in this manuscript:

- QKD: quantum key distribution
- SNOP: strongly nonlocal orthogonal product
- QOTP: quantum one time pad
- AQS: arbitrated quantum signature
- NISQ: noisy intermediate-scale quantum

References

1. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 1999, 41, 303–332.
2. Bennet, C.H.; Brassard, G. An update on quantum cryptography. LNCS 1984, 196, 475–480.
3. Ekert, A.K. Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 1991, 67, 661.
4. Gong, L.H.; Song, H.C.; He, C.S.; Liu, Y.; Zhou, N.R. A continuous variable quantum deterministic key distribution based on two-mode squeezed states. Phys. Scr. 2014, 89, 035101.
5. Zhao, Z.; Chen, Y.A.; Zhang, A.N.; Yang, T. Experimental demonstration of five-photon entanglement and open-destination teleportation. Nature 2004, 430, 54–58.
6. Deng, F.G.; Li, C.Y.; Li, Y.S.; Zhou, H.Y. Symmetric multiparty-controlled teleportation of an arbitrary two-particle entanglement. Phys. Rev. A 2009, 72, 022338.
7. Gao, T.F.; Yan, L.; Wang, Z.X. Controlled quantum teleportation and secure direct communication. Chin. Phys. 2005, 14, 893–897.
8. Yang, K.; Huang, L.; Yang, W.; Song, F. Quantum teleportation via GHZ-like states. Int. J. Theor. Phys. 2009, 48, 516–521.
9. Wang, X.W.; Su, Y.H.; Yang, G.J. Controlled teleportation against uncooperation of part of supervisors. Quantum Inf. Process. 2009, 8, 319–330.
10. Wang, T.Y.; Wen, Q.Y. Controlled quantum teleportation with Bell states. Chin. Phys. B 2011, 20, 040307.
11. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 1999, 59, 162–168.
12. Xiao, L.; Long, G.L.; Deng, F.G.; Pan, J.W. Efficient multiparty quantum–secret–sharing schemes. Phys. Rev. A 2004, 69, 052307.
13. Deng, F.G.; Li, X.H.; Li, C.Y.; Zhou, P. Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein–Podolsky–Rosen pairs. Phys. Rev. A 2005, 72, 044301.
14. Deng, F.G.; Li, X.H.; Zhou, H.Y. Improving the security of multiparty quantum secret sharing against trojan horse attack. Phys. Rev. A 2005, 72, 044302.
15. Li, X.H.; Zhou, P.; Li, C.Y. Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B At. Mol. Opt. Phys. 2006, 39, 1975–1983.
16. Gao, T.; Yan, F.L.; Wang, Z.X. Deterministic secure direct communication using GHZ states and swapping quantum entanglement. J. Phys. A 2005, 38, 5761.
17. Wang, C.; Deng, F.; Long, G. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt. Commun. 2005, 253, 15–20.
18. Lee, H.; Lim, J.; Yang, H. Quantum direct communication with authentication. Phys. Rev. A 2006, 73, 042305.
19. Jin, X.R.; Ji, X.; Zhang, Y.Q.; Zhang, S. Three-party quantum secure direct communication based on GHZ states. Phys. Rev. A 2006, 354, 67–70.
20. Tang, Y.L.; Yin, H.L.; Zhao, Q.; Liu, H. Measurement-device-independent quantum key distribution over untrustful metropolitan network. Phys. Rev. X 2016, 6, 011024.
21. Hong, C.H.; Heo, J.; Khym, G.L.; Lim, J.I. N quantum channels are sufficient for multi-user quantum key distribution protocol between n users. Opt. Commun. 2010, 283, 2644–2646.
22. Nguyen, D.M.; Kim, S. Multi-Bits Transfer Based on the Quantum Three-Stage Protocol with Quantum Error Correction Codes. Int. J. Theor. Phys. 2019, 58, 2043–2053.
23. Hong, C.H.; Heo, J.; Lim, J.L.; Yang, H.J. Quantum secure direct communication network with hyperentanglement. Chin. Phys. B 2014, 23, 090309.
24. Li, J.; Chen, X.B.; Xu, G.; Yang, Y.X. Perfect quantum network coding independent of classical network solutions. IEEE Commun. Lett. 2015, 19, 115–118.
25. Gottesman, D.; Chuang, I. Quantum Digital Signature. arXiv 2001, arXiv:0105032.
26. Zeng, G.; Christoph, H. Keitel. Arbitrated quantum signature scheme. Phys. Rev. A 2002, 65, 042312.
27. Li, Q.; Chan, W.H.; Long, D.Y. Arbitrated quantum signature scheme using Bell states. Phys. Rev. A 2009, 75, 054307.
28. Zou, X.F.; Qin, D.W. Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A 2010, 82, 042325.
29. Liu, J.L.; Shi, R.H.; Shi, J.J.; Lv, G.L.; Guo, Y. Quantum dual signature scheme based on coherent states with entanglement swapping. Chin. Phys. B 2016, 25, 080306.
30. Kang, M.S.; Hong, C.H.; Heo, J.; Lim, J.I. Controlled mutual quantum entity authentication using entanglement swapping. Chin. Phys. B 2015, 24, 120–128.
31. Kang, M.S.; Heo, J.; Hong, C.H.; Yang, H.J. Controlled mutual quantum entity authentication with an untrusted third party. Quantum. Inf. Process. 2018, 17, 159.
32. Wang, Q.; Zhang, S.; Wang, S.L.; Shi, R.H. Comment on “Controlled mutual quantum entity authentication with an untrusted third party”. Quantum. Inf. Process. 2020, 19, 125.
33. Li, W.; Shi, R.H.; Huang, D.Z.; Shi, J.J.; Guo, Y. Quantum blind dual-signature scheme without arbitrator. Phys. Scr. 2016, 91, 035101.
34. Halder, S.; Banik, M.; Agrawal, S. Strong quantum nonlocality without entanglement. Phys. Rev. Lett. 2019, 122, 040403.
35. Zhang, K.J.; Zhang, W.W.; Li, D. Improving the security of arbitrated quantum signature against the forgery attack. Quantum. Inf. Process. 2013, 12, 2655–2669.
36. Boykin, P.O.; Roychowdhury, V. Optimal encryption of quantum bits. Phys. Rev. A 2003, 67, 645–648.
37. Gao, F.; Qin, S.J.; Guo, F.Z.; Wen, Y.Q. Cryptanalysis of the arbitrated quantum signature protocols. Phys. Rev. A 2011, 84, 022344.
38. Zhang, G.F.; Zhou, Y. Interplay between the Dzyaloshinskii-Moriya anisotropic antisymmetric interaction and the SWAP operation in a two-qubit Heisenberg model. Phys. Lett. A 2007, 370, 136–138.
39. Collins, D.; Linden, N.; Popescu, S. Nonlocal content of quantum operations. Phys. Lett. A 2001, 264, 032302.
40. Zhou, Y.; Zhang, G.F. Swap operation in the presence of Zeeman inhomogeneity in coupled quantum dots. Solid. State. Communicaions 2014, 178, 28–32.