Quantum Dual Signature with Coherent States Based on Chained Phase-Controlled Operations

Jinjing Shi 1,*†, Shuhui Chen 1,⁠†, Jiali Liu 2, Fangfang Li 1,*†, Yanyan Feng 1 and Ronghua Shi 1

1 School of Computer Science and Engineering, Central South University, Changsha 410083, China; shuhuichen1996@163.com (S.C.); fengyanyanhu@163.com (Y.F.); shirh@csu.edu.cn (R.S.)
2 Wuhan Maritime Communication Research Institute, Wuhan 430205, China; JLL247@126.com
* Correspondence: shijinjing@csu.edu.cn (J.S.); lifangfang@csu.edu.cn (F.L.)
† These authors contributed equally to this work.

Received: 20 January 2020; Accepted: 12 February 2020; Published: 17 February 2020

Abstract: A novel encryption algorithm called the chained phase-controlled operation (CPCO) is presented in this paper, inspired by CNOT operation, which indicates a stronger correlation among message states and each message state depending on not only its corresponding key but also other message states and their associated keys. Thus, it can prevent forgery effectively. According to the encryption algorithm CPCO and the classical dual signature protocols, a quantum dual signature scheme based on coherent states is proposed in this paper. It involves three participants, the customer Alice, the merchant Bob and the bank Trent. Alice expects to send her order message and payment message to Bob and Trent, respectively. It is required that the two messages must be linked to guarantee the payment is paid for the corresponding order. Thus, Alice can generate a quantum dual signature to achieve the goal. In detail, Alice firstly signs her two messages with the shared secret key. Then She connects the two signatures into a quantum dual signature. Finally, Bob and Trent severally verify the signatures of the order message and the payment message. Security analysis shows that our scheme can ensure its security against forgery, repudiation and denial. In addition, simulation experiments based on the Strawberry Fields platform are performed to valid the feasibility of CPCO. Experimental results demonstrate that CPCO is viable and the expected coherent states can be acquired with high fidelity, which indicates that the encryption algorithm of the scheme can be implemented on quantum devices effectively.

Keywords: the chained phase-controlled operations; quantum dual signature; coherent states; e-payment system

1. Introduction

The digital signature, which is an important way to realize identity and message authentication, is one of the significant cryptographic building blocks and has been extensively employed in secure electronic commerce. A digital signature is considered to be additional information to the message [1] and it can prevent cheating legitimate users, including forging the sender’s signature by the receiver, and repudiating the signature by the sender [2]. There are lots of classical digital signature schemes [3–5] including post-quantum signature [6], whose security depends on complex algorithms or unresolved mathematical problems, such as the discrete logarithm problem [7] and the prime factorization problem [8]. However, with the advent of quantum computing and quantum algorithms [9,10], these classical signature schemes are likely to be compromised [11,12]. For example, the security of the signature with prime factorization may be quickly broken [13,14] by Shor’s algorithm [15] in the near future. Hence research imminently needs to blaze a trail in the security improvement of signature schemes with another way. The product of combination of quantum
cryptography and classical signature schemes, the so-called quantum signature, can effectively contend with the attacks brought by quantum computation. With physical properties, such as Heisenberg uncertainty [16] and the quantum no-cloning theorem [17], a quantum signature can have unconditional security in theory, so that more and more scholars invest in research on this topic [18–20]. For adjusting to diverse application scenarios, arbitrated quantum signature (AQS) [11,12,21], quantum group signature (QGS) [22,23], quantum proxy signature (QPS) [24,25], quantum blind signature (QBS) [26,27] or their combinations [28–30], have been proposed, which are apparently corresponding to various classical digital signature schemes.

In 2001, Gottesman et al. [31] first proposed a quantum digital signature based on fundamental principles of quantum physics, i.e., a quantum analogue of one-way functions, which required $O(m)$ qubits to encrypt $m$-bit message. On the basis of Greenberger-Horne-Zeilinger (GHZ) triplet states, Zeng et al. [32] and Keitel [33] put forward a quantum signature scheme, whose realization depends upon a trusty arbitrator, namely AQS schemes [21,34] which can be adapted to both known and unknown quantum states and still provide certain degree of security by employing quantum key distribution (QKD) protocols and quantum one-time pads (QOTPs) [35,36]. Ref. [2,34] pointed out that forgery attacks may occur in AQS schemes which use QOTP. On the one hand, the QOTP encrypts data qubit by qubit and the key bits are independent of each other. On the other hand, Pauli operations commute or anticommute with each other, i.e., the Pauli operators can exchange each other. Therefore, the recipient Bob may forge the sender’s signature under known message by using the encryption features of QOTP. Xu et al. [37] designed a quantum group blind signature scheme to provide anonymity of voters in an e-voting system and Ref. [22] proposed a QGS scheme without the help of arbitrator, which can be used in e-government and e-business. Dunjko et al. [38] introduced a quantum digital signature scheme applying coherent states which is experimentally feasible to access. For pushing the limit of single stream in quantum networks, Shang et al. [39] first proposed a quantum homomorphic signature protocol by using entanglement swapping, which is used to authenticate data packets of multiple stream for quantum networks. Then other quantum homomorphic [40,41] signatures have been proposed successively.

It is common knowledge that account information and trading activities of a consumer are required to not be leaked to others. A dual signature [42–44], which combines the customer’s order information and payment information that are encrypted with separate secret keys, can be used to solve the problem that the customer’s order information (payment information) should be hidden from the bank (business) while the payment information should be blindly forwarded to the bank by the business. It is a new way to sign on transaction information and plays an important role in e-payment system to ensure the secure communication among the consumer, merchant, and bank. The dual signature has a good development in classical cryptography, and a quantum dual signature scheme [44] was introduced based on coherent states with entanglement swapping in 2016. Compared to the classical dual signatures, the quantum dual signature which involves quantum algorithms and QKD protocols could be more secure and efficient, and it also has a wide application to the ecommerce system as a classical dual signature.

In 2103, Zhang et al. [45] presented two types of improved encryption algorithms which are called Key-Controlled-‘I’ QOTP and Key-Controlled-‘T’ QOTP determined by the shared key and can prevent forgery attacks effectively. In 2015, Li et al. [46] proposed a novel chained CNOT operations encryption where one qubit is encrypted not only based on the corresponding qubit and key but also based on other qubits and keys, which is more secure compared with QOTP. Therefore, inspired by the chained CNOT operations and classical dual signature, we design a new encryption algorithm for signatures, i.e., the chained phase-controlled operation (CPCO) to construct a quantum dual signature scheme. Meanwhile, coherent states that can be easily generated [47,48] by current quantum technologies are used as the input resources. Strong analysis we present proves that the scheme can resist the attacks on forging sender’s signature, disavowing own signature, denying the received signature, and also the Gao’s attack in Ref. [2]. Simulation experiments of the CPCOs are performed on quantum software.
platform, namely Strawberry Fields [49], and the experimental results declares that the designed encryption algorithm can be implemented by quantum devices.

It is worth mentioning that a secure quantum signature protocol must meet the following security conditions [8]: (1) Non-forgery: The signature cannot be forged by any attacker. Only the legitimate signer can generate a valid signature. (2) Non-repudiation: Any participant cannot deny what she/he has done. That is to say, the signer cannot later successfully disavow that she/he has signed a message and the receiver cannot deny her/his receiving or the integrity of the signature. (3) Quantum properties: Quantum signature algorithms contain pure quantum mechanics properties, and there are no classical counterparts. In this paper, we mainly focus on these security conditions to verify the feasibility of our scheme.

2. Methods

2.1. The Preparation of Keys

In our proposed scheme, the keys are used with the permutation of the decimal sequence like (1, 2, . . . , n) rather than binary sequence. So we should process the original key which are obtained from the QKD protocols [50–53]. Detailedly, if Alice wants to share secret keys with Bob (Trent), the steps can be generalized as follows:

1. Alice shares n-bit string \( K_{\text{original}} \) = \{\( K_{\text{original}}^l \mid 1 \leq l \leq n \} \) with Bob (Trent) via a QKD protocol, where \( K_{\text{original}}^l \in \{0, 1\} \).
2. The final key \( K_{\text{final}} \) is obtained according to the positions of 0 and 1.

   (1) The position of the first, the second and the last 0 is assigned to \( K_{\text{final}}^l, K_{\text{final}}^2 \) and \( K_{\text{final}}^l \) respectively, where \( l = 0 \).

   (2) The positions of 1 are assigned to the remaining \( K_{\text{final}}^{l+1}, \ldots, K_{\text{final}}^n \). Then we have \( K_{\text{final}} = \{K_{\text{final}}^l \mid 1 \leq l \leq n \} \).

For example, if \( K_{\text{original}} = \{00101\} \), then \( K_{\text{final}} = \{1, 2, 4, 3, 5\} \).

2.2. The Chained Phase-Controlled Operations

As we know, the CNOT operator is a two-qubit gate and its function is given by

\[
|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle,
\]

where the two qubits \(|c\rangle\) and \(|t\rangle\) are the control qubit and the target qubit, respectively. The notation \( \oplus \) stands for summation mod 2. The target bit flips when \(|c\rangle = |1\rangle\), otherwise, the target bit stays unchanged. We draw inspiration from CNOT operation and put forward a new encryption algorithm, namely the CPCO. A phase-controlled operation (PCO) can be defined as \( PCO(\{|M\}_j, |M\rangle_{K_j}) \), where \( K_j \) is the \( j \)-th value of the final key, \(|M\rangle_j \) is the control coherent state and \(|M\rangle_{K_j} \) is the target coherent state, and \(|M\rangle_j, |M\rangle_{K_j} \in \{|a\rangle, |−a\rangle, |ia\rangle, |−ia\rangle\} \) [54]. In addition, the coherent state \(|M\rangle_j \) satisfies \(|M\rangle_j = |x_j + ip_j\rangle\), where \( x_j \in \mathbb{R} \) and \( p_j \in \mathbb{R} \) are separately the amplitude and phase of \(|M\rangle_j \). The results of PCO operations applied to message \(|M\rangle_j \) can be derived as follows.

\[
PCO(\{|M\}_j, |M\rangle_{K_j})|M\rangle_{K_j} = \begin{cases} 
P(\frac{\pi}{2})|M\rangle_{K_j}, & K_j \neq j, x_j \neq 0 \text{ and } p_j = 0, \\
P(\pi)|M\rangle_{K_j}, & K_j \neq j, x_j = 0 \text{ and } p_j \neq 0, \\
P(0)|M\rangle_{K_j}, & K_j = j,
\end{cases}
\]

where \( P(\theta) \) is a phase shift operator which fulfils \( P(\theta) = \exp(i\theta \hat{a}^\dagger \hat{a}) \), and \( \theta \in \{\frac{\pi}{2}, \pi\} \) is angle of phase changed, \( \hat{a}^\dagger \) and \( \hat{a} \) are bosonic creation and annihilation operators, respectively. The 50/50 beam splitter can be used to achieve the measurements of amplitude and phase. Two coherent states \(|\mu\rangle\) and
where \( K \) is acquired from one of the two output modes according to the judgement \(|M\rangle_3\) is equal to \(|\alpha\rangle \) or \(|-\alpha\rangle \). Otherwise, both output of modes are not vacuum states.

Suppose the message which is composed of coherent states is \(|M\rangle = \otimes^N_{j=1} |M\rangle_j\), where \( N \) stands for the message length and the secret key is \( K \). Then the encryption process based on the CPCO is deduced as:

\[
|C\rangle = E_K|M\rangle = PCO(|M\rangle_{n}, |M\rangle_{K_0})PCO(|M\rangle_{n-1}, |M\rangle_{K_{n-1}}) \ldots PCO(|M\rangle_1, |M\rangle_{K_1})|M\rangle,
\]

where \( E_K \) means the encryption algorithm. Meanwhile, the corresponding decryption process is

\[
|M\rangle = D_K|C\rangle = DPCO(|M\rangle_1, |M\rangle_{K_1})DPCO(|M\rangle_2, |M\rangle_{K_2}) \ldots DPCO(|M\rangle_n, |M\rangle_{K_n})|C\rangle,
\]

where \( D_K \) and \( DPCO \) stands for decryption algorithm and the phase-controlled operation for decryption respectively. The detailed functions of \( DPCO(|M\rangle_j, |M\rangle_{K_j}) \) are

\[
DPCO(|M\rangle_j, |M\rangle_{K_j}) = \begin{cases} 
P(-\frac{\pi}{2})|M\rangle_{K_j}, & K_j \neq j, x_j \neq 0 \text{ and } p_j = 0, \\
P(-\pi)|M\rangle_{K_j}, & K_j \neq j, x_j = 0 \text{ and } p_j \neq 0, \\
P(0)|M\rangle_{K_j}, & K_j = j. 
\end{cases}
\]

For example, suppose \( n = 4 \), the key \( K = \{1, 4, 2, 3\} \) and the message \( |M\rangle = |\alpha\rangle_1 - \alpha\rangle_2 | -\alpha\rangle_3 |\alpha\rangle_4 \). Then the encoded message is

\[
|C\rangle = E_K|M\rangle = PCO(|M\rangle_4, |M\rangle_{K_4})PCO(|M\rangle_3, |M\rangle_{K_3}) \ldots PCO(|M\rangle_1, |M\rangle_{K_1})(|\alpha\rangle_1 - \alpha\rangle_2 \\
| -\alpha\rangle_3 |\alpha\rangle_4 \\
= PCO(|M\rangle_4, |M\rangle_3)PCO(|M\rangle_3, |M\rangle_2) \ldots PCO(|M\rangle_1, |M\rangle_1)(|\alpha\rangle_1 - \alpha\rangle_2 \\
| -\alpha\rangle_3 |\alpha\rangle_4 \\
= |\alpha\rangle_1 |\alpha\rangle_2 |\alpha\rangle_3 | -\alpha\rangle_4.
\]

Also the decoded message is acquired as:

\[
|M\rangle = D_K|C\rangle = DPCO(|M\rangle_1, |M\rangle_{K_1})DPCO(|M\rangle_2, |M\rangle_{K_2}) \ldots DPCO(|M\rangle_4, |M\rangle_{K_4})(|\alpha\rangle_1 \\
|\alpha\rangle_2 |\alpha\rangle_3 | -\alpha\rangle_4 \\
= DPCO(|M\rangle_1, |M\rangle_1)DPCO(|M\rangle_2, |M\rangle_2) \ldots DPCO(|M\rangle_4, |M\rangle_4)(|\alpha\rangle_1 |\alpha\rangle_2 \\
|\alpha\rangle_3 | -\alpha\rangle_4 \\
= |\alpha\rangle_1 | -\alpha\rangle_2 | -\alpha\rangle_3 |\alpha\rangle_4.
\]

It can be seen that one state is not only related to its corresponding key bit and message state but also related to the key and state in other positions. Thus, this new method in our scheme makes a stronger correlation between message states, and in later section, we prove that the encryption algorithm based on CPCO can avoid attacker’s forgery.
2.3. Quantum Dual Signature Scheme

The schematic representation of the propounded scheme is shown in Figure 1. The signatory Alice firstly signs the messages $|M_O\rangle$ and $|M_P\rangle$ which are required to be separately received by Bob and Trent, and she combines the two signatures into a quantum dual signature. Next, Bob verifies the signature of order message and derives the parameter $V_B$ which is a reference point for Bob to judge whether transmit relevant information to Trent or reject the signature directly. Subsequently, Trent completes the verification for the signature of $|M_P\rangle$ and sends a parameter $V_T$ to Bob. The quantum dual signature scheme involves three participants, i.e., the signatory Alice, the order message verifier Bob and the payment message verifier Trent, and three phases, i.e., the initial phase, the signing phase and the verification phase that can be described in detail as follows.

2.3.1. Initial Phase

In this phase, the participants share the necessary keys and Alice blinds her messages based on agreed principles. The procedures are described as below:

1. Alice has two classical messages, i.e., the order message $M_O = \otimes_{i=1}^{x} m^O_i$ and the payment message $M_P = \otimes_{i=1}^{y} m^P_i$, where $m^O_i, m^P_i \in \{0, 1\}$. $x$ and $y$ separately stand for the lengths of $M_O$ and $M_P$.
2. Based on QKD protocols, the original keys $K_{ori}^{AB}$, $K_{ori}^{AT}$ and $K_{ori}^{BT}$ are shared between Alice and Bob, Alice and Trent, and Bob and Trent, respectively. $K_{ori}^{AB}$ has $x+y$ bits. The lengths of $K_{ori}^{AT}$ and $K_{ori}^{BT}$ are $y$ bits.
3. According to the method mentioned in the section of preparation of the key, the final keys $K_{AB}$, $K_{AT}$ and $K_{BT}$ are obtained. Each of them is a disorderly permutation of $(1, 2, \ldots, n)$.
4. Alice selects a random $x$-bit binary sequence $K_{RO}$. According to each $m_O^iK_{RO}^i$, Alice prepares the relevant coherent state. The corresponding relationships are shown in Table 1. Therefore, the order information is blinded into $|M⟩_O^i = \otimes_{s=1}^x |M⟩_O^i$. 
5. Similarly, Alice generates another $y$-bit binary sequence $K_{RP}$. Based on each $m_P^iK_{RP}^i$, she acquires blind payment message $|M⟩_P^i = \otimes_{t=1}^y |M⟩_P^i$. The corresponding relations are shown in Table 2.

### Table 1. The corresponding relations between $m_O^iK_{RO}^i$ and $|M⟩_O^i$. 

| $m_O^iK_{RO}^i$ | $|M⟩_O^i$ |
|-----------------|-----------|
| 00              | $|a⟩$     |
| 01              | $|−a⟩$    |
| 10              | $|−ia⟩$   |
| 11              | $|ia⟩$    |

### Table 2. The corresponding relations between $m_P^iK_{RP}^i$ and $|M⟩_P^i$. 

| $m_O^iK_{RO}^i$ | $|M⟩_O^i$ |
|-----------------|-----------|
| 00              | $|ia⟩$    |
| 01              | $|−ia⟩$   |
| 10              | $|−a⟩$    |
| 11              | $|a⟩$     |

#### 2.3.2. Signing Phase

This phase gives a specific description of the signature algorithm, i.e., Alice signs the message states by implementing CPCO and merges these two signatures into a quantum dual signature. The signing phase is carried out by following procedures.

1. Alice signs $|M⟩_P^i$ based on the CPCOs with secret key $K_{AT}$ and obtains $|S⟩_P = E_{K_{AT}}(|M⟩_P^i)$. 
2. Alice signs $|M⟩_O^i$ and acquires signature $|S⟩_O = E_{K_{AB(x)}}(|M⟩_O^i)$ according to $K_{AB}$, where $K_{AB(x)}$ represents the front $x$ numbers of $K_{AB}$. 
3. Alice connects $|S⟩_O$ and $|S⟩_P$ together and acquires $|S⟩_{OP} = |S⟩_O \otimes |S⟩_P$ whose length is $x + y$. 
4. Alice signs $|M⟩_{OP}$ based on the key $K_{AB}$. Then she gets the quantum dual signature $|S⟩_D = E_{K_{AB}}(|M⟩_{OP})$. 
5. Alice transmits $|S⟩_D$ and $|M⟩_{OP}$ to Bob. Meanwhile, she sends $|M⟩_P^i$ to Trent.

#### 2.3.3. Verification Phase

The verification phase requires Bob (Trent) to verify the signature of order message (payment message) and judge whether the signature $|S⟩_O$ ($|S⟩_P$) is valid. The detailed steps are as displayed follows.

1. Once receiving Alice’s signature, Bob randomly chooses $n_a (n_a < x + y)$ states from it and records the numbers. Simultaneously, Alice and Bob negotiate the correspondence between signatures and binary bits. For example, they use 00, 01, 10 and 11 to stand for $|a⟩$, $|ia⟩$, $|−a⟩$ and $|−ia⟩$, respectively. 
2. Bob sends numbers and corresponding bits of the chosen states to Alice. Alice judges whether the signatures are right based on the correspondence between signatures and binary bits. If $\varepsilon_{forgery} < \varepsilon_B$, subsequent steps continue. Otherwise the protocol is terminated. $\varepsilon_{forgery}$ represents the probability of mistakes between the recovered signatures and the original signatures, and $\varepsilon_B$ represents the error threshold. 
3. Bob decodes $|S⟩_P$ and derives $|M⟩_{OP}$. Then Bob divides $|M⟩_{OP}$ into two parts with length $x$ and $y$ respectively. Thus, Bob obtains $|S⟩_O$ and $|S⟩_P$. 

---

**Table 1:** The corresponding relations between $m_O^iK_{RO}^i$ and $|M⟩_O^i$. 

**Table 2:** The corresponding relations between $m_P^iK_{RP}^i$ and $|M⟩_P^i$. 

4. Bob encodes $|M\rangle'_O$ and derives $|S\rangle'_O = E_{K_{AB(x)}}(|M\rangle'_O)$ with CPCO based on secret key $K_{AB(x)}$.

5. Bob verifies whether $|S\rangle'_O$ is matched to $|S\rangle_O$. Then he obtains the parameter

$$V_B = \begin{cases} 1, & |S\rangle'_O = |S\rangle_O, \\ 0, & |S\rangle'_O \neq |S\rangle_O. \end{cases}$$

(8)

If $V_B$ is equal to 0, Bob rejects the quantum dual signature directly; otherwise, Bob encrypts $|S\rangle_P$ with the key $K_{BT}$ and acquires

$$|M\rangle_T = E_{K_{AB}}(|S\rangle_P).$$

(9)

Then he sends $|M\rangle_T$ to Trent. Here we need to emphasize that the business Bob needs to validate the identity of the customer Alice and the details of order before the bank Trent verifies the signature of payment message. This is the reason the payment message is forwarded to Trent by Bob.

6. Trent decrypts $|M\rangle_T$ with $K_{AT}$ and obtains $|S\rangle_P$.

7. Trent randomly selects $m_a$ states from $|S\rangle_P$ and records their numbers. Trent and Alice negotiate the correspondence between signatures and $m_a$-length binary bits. Trent transmits numbers and corresponding bits of the chosen states to Alice. Alice judges whether the signatures are right and acquires the error probability $\epsilon_{\text{forgery}}^T$. If $\epsilon_{\text{forgery}}^T < \epsilon_T$, next steps continue, otherwise the protocol is stopped, where $\epsilon_{\text{forgery}}^T$ represents the error probability of signatures of payment messages, and $\epsilon_T$ represents the error threshold.

8. Trent computes $|S\rangle'_P = E_{K_{AT}}(|M\rangle'_P)$ and judges whether $|S\rangle'_P = |S\rangle_P$ to determine the parameter

$$V_T = \begin{cases} 1, & |S\rangle'_P = |S\rangle_P, \\ 0, & |S\rangle'_P \neq |S\rangle_P. \end{cases}$$

(10)

Next Trent sends the result $V_T$ to Bob.

9. Bob can draw a conclusion that Alice’s signatures are valid if $V_B = V_T = 1$. In this situation, Bob can require Alice to inform the key $K_{RO}$.

10. Alice receives Bob’s demand which means the successful verification of $|S\rangle_O$ and $|S\rangle_P$. Then Alice informs Bob (Trent) the key $K_{RO}$ ($K_{RP}$).

11. Bob recovers $M_O$ from $|M\rangle'_O$ on the basis of principles which are negotiated between them in advance. In detail, the principles of recovering messages are

$$m_O^\_ = \begin{cases} K^4_{RO} \oplus 0, & x_{M_O^\_} \geq 0 \text{ and } p_{M_O^\_} \geq 0, \\ K^4_{RO} \oplus 1, & \text{others}, \end{cases}$$

(11)

where $x_{M_O^\_}$ and $p_{M_O^\_}$ are amplitude and phase of the coherent state $|M\rangle'_O$, respectively.

12. Trent also can recover $M_P$ from $|M\rangle'_P$ based on the principles that

$$m_P^\_ = \begin{cases} K^4_{RP} \oplus 0, & x_{M_P^\_} \geq 0 \text{ and } p_{M_P^\_} \geq 0, \\ K^4_{RP} \oplus 1, & \text{others}, \end{cases}$$

(12)

where $x_{M_P^\_}$ and $p_{M_P^\_}$ are amplitude and phase of the coherent state $|M\rangle'_P$, separately. In this case, the transaction is completed.
3. Results

As mentioned above, a secure quantum signature scheme should meet at least three requirements, i.e., non-forgery, non-repudiation and quantum properties [8]. In general, the requirement that protocol has quantum properties is easy to achieve. However, non-forgery and non-repudiation are difficult to meet. In our scheme, the above three requirements are completely satisfied. Any attacker cannot obtain the whole information about the secret key. Neither the external attacker nor the signature receiver can forge the signature. Furthermore, the signatory is unable to disavow the signature after she has signed on the messages. The receiver is failed to deny the received signature after he has performed operations as well.

It should be noted that the bank Trent is always honest. He plays an important role in judging whether Alice has disavowed her signatures when there are disputes or disagreements. Subsequently, the security analyses of the proposed scheme are described in detail.

3.1. Security of Keys

Original keys are acquired with the security QKD protocols in this scheme. Therefore, it is impossible for an attacker to crack the keys which are shared between the signer and the verifier. In fact, two situations that make encryption with CPCO have no influence on the message $|M\rangle$ need to be considered. One is that the bits of the original key are all 0 (1), i.e., $K_{\text{original}} = \{00\ldots0\}$ or $K_{\text{original}} = \{11\ldots1\}$. The other is that only the last bit of the original key is 1, i.e., $K_{\text{original}} = \{00\ldots001\}$. For example, if $n = 5$, $|M\rangle = |\alpha\rangle_1 - i|a\rangle_2|\alpha\rangle_3 - a\rangle_4|ia\rangle_5$ and $K_{\text{original}} = \{00000\}$ or $K_{\text{original}} = \{00001\}$, then $K_{\text{final}} = \{1, 2, 3, 4, 5\}$. According to the negotiated rules and Equation (2), the phase-shift operation $P(0)$ is performed. Hence the signature $|S\rangle$ finally equals to the original message $|M\rangle$ referred to Equation (13).

$$
|S\rangle = E_{K_{\text{AT}}}(|M\rangle_P') = \text{PCO}(|M\rangle_5, |M\rangle_5)\text{PCO}(|M\rangle_4, |M\rangle_4)\ldots\text{PCO}(|M\rangle_1, |M\rangle_1)
(\langle\alpha\rangle_1 - ia\rangle_2|\alpha\rangle_3 - a\rangle_4|ia\rangle_5)
= |\alpha\rangle_1 - ia\rangle_2|\alpha\rangle_3 - a\rangle_4|ia\rangle_5 = |M\rangle.
$$

However, the probability of the two situations above is very small. Here, denote the probability which corresponds to the first (second) situation as $P$ ($P'$). $P$ and $P'$ can be calculated as Equation (14).

$$
P = \left(\frac{1}{2}\right)^n, P' = \left(\frac{1}{2}\right)^{n-1}.
$$

As shown in Figure 2, the probability $P$ becomes smaller with the increase of $n$, if the length of original key can remain greater than 10-bit, $P$ tends to zero, thus the final key is extremely efficient. No doubt that the same analyses can be applied to the second situation. Moreover, CPCO can involve a huge difference between plain and cipher even the number of swap in $K_{\text{final}}$ is just one, which can ensure the security of the quantum dual signature scheme.
Figure 2. The probability that all bits of the original key are 0 or 1 as a function of the length of the original key. It shows that the larger $n$ is, the smaller probability is. Such as $n$ is greater than 10-bit, the probability of $P = (\frac{1}{2})^n$ approaches to 0.

3.2. Impossibility of Forgery

If the attacker Eve attempts to forge Alice’s signatures $|S\rangle_O$ or $|S\rangle_P$, she has to know the corresponding secret keys $K_{AB}$ or $K_{AT}$. However, the original keys are shared with unconditionally secure QKD protocol [55], it is impossible for her to eavesdrop the secret keys distributed between signatory and verifiers. Moreover, the final keys are obtained according to the rules which are consensuses among legal participants. The attacker is completely unaware of the rules, so Eve cannot know the keys $K_{AB}$ and $K_{AT}$. Thus, we describe two theorems of our encryption algorithm which are used to valid the security of our signature scheme.

Theorem 1. Several errors in the final secret key $K$ may cause an obvious deviation in the result of encryption.

For example, if $n = 4, K = \{3, 1, 2, 4\}$ and $|M\rangle = |\alpha\rangle_1 - i|\alpha\rangle_2|\alpha\rangle_3 - \alpha\rangle_4$, the result of encryption is

$$|C\rangle = PCO(M_4, M_4)PCO(M_3, M_2)PCO(M_2, M_1)PCO(M_1, M_3)(|\alpha\rangle_1 - i\alpha\rangle_2|\alpha\rangle_3 - \alpha\rangle_4)$$

$$= |\alpha\rangle_1|\alpha\rangle_2 - \alpha\rangle_3 - \alpha\rangle_4.$$

(15)

When the key is changed into $K = \{1, 3, 2, 4\}$, the result will become,

$$|C\rangle = PCO(M_4, M_4)PCO(M_3, M_2)PCO(M_2, M_3)PCO(M_1, M_1)(|\alpha\rangle_1 - i\alpha\rangle_2|\alpha\rangle_3 - \alpha\rangle_4)$$

$$= |\alpha\rangle_1|\alpha\rangle_2 - \alpha\rangle_3 - \alpha\rangle_4.$$

(16)

According to Equations (15) and (16), we realize that any error in the key may lead to a chain reaction in the encryption result. In Table 3, we enumerate all the encryption results based on different keys in the case of $|M\rangle = |\alpha\rangle_1 - i\alpha\rangle_2|\alpha\rangle_3 - \alpha\rangle_4$. In accordance with Table 3, we know that any result is different from others. So the Theorem 1 is reasonable.
Table 3. Encryption results based on different secret keys in the case of $|M⟩ = |α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4$.

| $K$       | $E_K(|M⟩)$                          |
|-----------|-------------------------------------|
| 1,2,3,4   | $|α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4$            |
| 1,2,4,3   | $|α⟩_1| - iα⟩_2| - α⟩_3| - α⟩_4$           |
| 1,3,2,4   | $|α⟩_1| - iα⟩_2| - iα⟩_3| - α⟩_4$          |
| 1,3,4,2   | $|α⟩_1| - α⟩_2| - iα⟩_3| - α⟩_4$         |
| 1,4,2,3   | $|α⟩_1| - iα⟩_2| - α⟩_3| - α⟩_4$         |
| 2,1,3,4   | $|α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4$         |
| 2,3,1,4   | $|α⟩_1| - iα⟩_2| - α⟩_3| - α⟩_4$         |
| 2,3,4,1   | $|α⟩_1| - iα⟩_2| - α⟩_3| - iα⟩_4$       |
| 2,4,1,3   | $|α⟩_1| - iα⟩_2| - α⟩_3| - iα⟩_4$       |
| 3,1,2,4   | $|α⟩_1| - iα⟩_2| - α⟩_3| - iα⟩_4$       |
| 3,4,1,2   | $|α⟩_1| - iα⟩_2| - α⟩_3| - iα⟩_4$       |
| 4,1,2,3   | $|α⟩_1| - iα⟩_2| - α⟩_3| - iα⟩_4$       |

Theorem 2. Errors in the message $|M⟩$ may cause an obvious deviation in the result of encryption.

We also suppose $n = 4$ and $K = \{3, 1, 2, 4\}$. However, the message $|M⟩ = |α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4$ is replaced by $|M⟩ = |α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4$. Then the result of encryption is

$$|C⟩ = PCO(M_4, M_4)PCO(M_3, M_2)PCO(M_2, M_1)PCO(M_1, M_3)$$

$$(|α⟩_1| - iα⟩_2|ia⟩_3| - α⟩_4)$$

$$= |−iα⟩_1|α⟩_2|−α⟩_3| − α⟩_4.$$  (17)

Comparing Equation (15) with Equation (17), it is easy to prove that a discrepancy in message may cause some errors in the ciphertext. Therefore, the Theorem 2 is tenable. According to the above two Theorems, it is concluded that any changes to the message or the key may lead to a wrong signature and the attack can be definitely detected. Once the forgery behavior is discovered, the honest correspondents may terminate this communication.

Even if Eve intercepts part of $K_{AB}$ ($K_{AT}$), she may fail to forge the signature of message $M_O$ ($M_P$) because Alice blinds her order message (payment message) based on the secret key $K_{RO}$ ($K_{RP}$). Therefore, only Alice knows the complete information about original messages. The operation that blinding the message is benefit to prevent the recipient or the eavesdropper forging messages in quantum signature procedures. Moreover, even though Eve intercepts some keys, she also needs to conjecture the rest to maximize the probability of success. As described in Theorem 1, an incorrect key may cause noticeable errors so that $\epsilon_f^e$ is greater than $\epsilon_f$, thus the forgery behaviors can be discovered. For a more powerful attacker who is not the internal communicator, the success probability of forging Alice’s signature is $P_f = (\frac{1}{2})^{n_a + m_a + m_b} \frac{1}{x + y} Pro(|M⟩_O, |S⟩_O) Pro(|M⟩_P, |S⟩_P)$, where $Pro$ is the probability of successful match between forged $|M⟩_O$ and $|S⟩_O$ ($|M⟩_P$ and $|S⟩_P$). It means that $P_f$ can be 0 with unconditional secure QKD protocols. Furthermore, leave the security probability (Pro) of QKD aside, we analyse the impossible forgery with specific conditions seen in Figure 3, in which we can discover the maximum value of $P_f$ is just 0.007 for a powerful attacker when $x + y = 2$ and $n_a + m_a + m_b = 3$. When the length of $x + y$ or $n_a + m_a + m_b$ reaches to 100 bits, $P_f$ may approach to 0. No doubt that the scheme can better resist forgery with the addition of QKD.

If the receiver Bob is malicious and he attempts to forge Alice’s signature $|S⟩_P$ for his own benefit. The success probability of forging Alice’s signature for Bob is $P_{f_b} = (\frac{1}{2})^{n_a} Pro(|M⟩_P, |S⟩_P)$. Even though Bob can intercept and forge $|M⟩_P$ and $|S⟩_P$, his forgery is unsuccessful since he knows nothing about $K_{AT}$, i.e., $P_{f_b} ≡ 0$. However, Ref. [2] pointed out that forgery attack against QOTP can
be successful even if the attacker does not know $K_{AT}$. Here, we prove that our scheme also can resist this kind of attack. In our protocol,

$$
|S\rangle_P = E_{K_{AT}} |M\rangle_P' = PCO(|M\rangle_P'_{P_{1}}, |M\rangle_P'_{P_{1a}}) \cdots PCO(|M\rangle_P'_{P_{1}}, |M\rangle_P'_{P_{1a}}) |M\rangle_P'
= |S\rangle_P |S\rangle_P \cdots |S\rangle_P_{P_{1}}.
$$

(18)

Figure 3. The success probability of forging Alice’s signature when leaving the security probability of QKD aside. $x$ and $y$ represent the length of order message and payment message respectively, and $x + y \geq 2$ (bits), $(n_{a} + m_{a} + m_{b}) \geq 3$ (bits). In the light yellow box, $X$, $Y$ and $Z$ denote the values of $x + y$ axis, $n_{a} + m_{a} + m_{b}$ axis and $P_{fa}$ axis respectively.

Due to the PCO operations, the $|S\rangle_{P_{j}}$ is not only depended on $|M\rangle_{P_{j}}$ for $j = 1, 2, \ldots, n$, but also determined by other qubits of $|M\rangle_{P_{j}}$. According to Gao’s [2] analyses, Bob may forge Alice’s signature without $K_{AT}$ with following operations:

$$
|S\rangle_{P_{j}} = U |S\rangle_{P_{j}}
= U |S\rangle_{P_{1}} |S\rangle_{P_{2}} \cdots |S\rangle_{P_{j}} \cdots |S\rangle_{P_{n}}
= |S\rangle_{P_{1}} |S\rangle_{P_{2}} \cdots |S\rangle_{P_{j}} \cdots |S\rangle_{P_{n}},
$$

(19)

where $U = I \otimes I \otimes \cdots U_{j} \otimes \cdots I$ represents any unitary operations and the $U$ is only applied to $|S\rangle_{P_{j}}$ to convert it to $|S\rangle_{P_{j}}$. Bob then sends $|S\rangle_{P_{j}}$ to Trent for the purpose of forging signature. Trent verifies message from Bob according to whether $E_{K_{AT}} |M\rangle_{P}$ is matched to $|S\rangle_{P}$ which is actually replaced with $|S\rangle_{P_{j}}$. It is apparent that $E_{K_{AT}} |M\rangle_{P} \neq |S\rangle_{P}$ for the correspondence among the plaintext $|M\rangle_{P}$, the key $E_{K_{AT}}$, and the ciphertext $|S\rangle_{P}$.

What happens if Bob replaces the plain with $|M\rangle_{P}'' = U |M\rangle_{P}'' = \bigotimes_{j=1}^{n} U_{j} |M\rangle_{P_{j}}''$. Trent can perform the following verifications in this situation, i.e.,

$$
|S\rangle_{T} = E_{K_{AT}} |M\rangle_{P}''
= PCO(|M\rangle_{P_{1}}'' |M\rangle_{P_{1a}}) \cdots PCO(|M\rangle_{P_{1}}'' |M\rangle_{P_{1a}}) \cdots PCO(|M\rangle_{P_{1}}'' |M\rangle_{P_{1a}}) |M\rangle_{P}'
= |S\rangle_{T_{1}} |S\rangle_{T_{2}} \cdots |S\rangle_{T_{n}}.
$$

(20)

According to Theorem 2, a few changes in the message $|M\rangle_{P_{j}}''$ may cause an obvious deviation in the result of encryption $|S\rangle_{P_{j}}''$. That is to say, many $|S\rangle_{P_{j}}$ for $j = 1, 2, \ldots, n$ are changed which leads to $|S\rangle_{T} \neq |S\rangle_{P_{j}}''$. Hence the forgery signature cannot pass Trent’s verification even if the equation $\epsilon_{ Forgery}^{T} < \epsilon^{T}$ holds, i.e., such an attack is invalid in the scheme. Based on the analysis, we can conclude that any forgery would be failed in our scheme.
3.3. Impossibility of Disavowal by the Signatory

In the proposed scheme, Alice can try two methods to disavow her signature. One is directly denying signature. Then Trent judges whether the formula $E_{K_{AT}} |S\rangle_p = |S\rangle_p$ holds. Due to the fact that the key $K_{AT}$ is only distributed between Alice and Trent (Bob), the trusted Trent can confirm that Alice has already signed the payment message since $|S\rangle_p$ contains the information of Alice’s secret key $K_{AT}$. The other is replacing correct quantum states. Message $|M\rangle_T$ may be intercepted and replaced with $|M\rangle'_T$ by powerful Alice. Trent decrypts the message and obtains the signature $|S\rangle'_p$ which can be derived according to Equation (21).

$$
|S\rangle'_p = D_{K_{BT}} |M\rangle'_T
= D_{PCO}(|M\rangle_{T1}, |M\rangle'_{I1}) \cdots D_{PCO}(|M\rangle_{Tn}, |M\rangle'_{In}).
$$

Then $E_{K_{AT}} |M\rangle'_p \neq |S\rangle'_p$ holds. Because $|S\rangle_p$ can be quite different from $|S\rangle'_p$ according to Theorem 2, Trent may admit that the signature is not from Alice indeed. However, there is the phase of error probability judgement in the scheme. When Alice disavows the signature and the equation $\epsilon_{\text{forgery}}^T < \epsilon_T$ is not satisfied, Trent would randomly select $m_b$ states from $|S\rangle'_p$ and record their numbers, then negotiate the correspondence between the signature and $m_b$-length binary bits with Bob. Trent transmits numbers and corresponding bits of the chosen states to Bob who can return the judgement that whether $\epsilon_{\text{forgery}}^T$ is less than $\epsilon_T$. Obviously, if the signature is indeed from Alice, the equation $\epsilon_{\text{forgery}}^T < \epsilon_T$ must be satisfied. Alice cannot disavow her signature anyway. Moreover, if Alice disavows her signature $|S\rangle_O$, Bob can require Trent to make a judgment. In detail, Bob sends the key $K_{AB}$ and the encoded message $|M\rangle'_O$ to Trent. Then Trent verifies whether the equation $|S\rangle_O = E_{K_{AB}}(|M\rangle'_O)$ is satisfied. If the equation holds, the signature is signed by Alice and her behavior of disavowing the signature is ended in failure.

3.4. Impossibility of Denial by the Verifier

The verifier Bob cannot deny after he has received $|S\rangle_D$ and $|M\rangle'_O$. If Bob sends $|M\rangle_T$ to Trent in the verification phase, it implies that he has already received $|S\rangle_D$ and carried out some operations on it. In addition, if Bob asks Alice to publish the key $K_{RO}$, it means that Bob has verified whether the equation $|S\rangle'_O = E_{K_{AB}}(|M\rangle'_O)$ is equal to $|S\rangle_O$. Then Trent also has verified $|S\rangle_p$. Thus, Bob has verified the signature indeed without later denying his involvement and actions. In another situation, Bob cannot acquire $K_{RO}$ from Alice if he claims $|S\rangle'_O \neq |S\rangle_O$ maliciously, and the original message $M_O$ is impossible to be cracked. In addition, Trent is reliable and that the verifier denies the received signature is out of question.

4. Discussion

Quantum dual signature which involves three parties, Alice, Bob and Trent, is suitable for e-commerce. With QKD protocols, communicators can share secret keys with each other for signaturing or de-signaturing massage. Assume that the process of QKD is secure, the quantum dual signature scheme may mainly face three threats, i.e., forging, disavowing, denying Alice’s signature. For forging signature, we analyze the situation and discover that when the attackers are strongly powerful, the success probability of forging signature Alice’s is also small. Actually, three methods can be introduced for reducing $P_{\text{for}}$: one is increasing the length of randomly choosing states in the step 1 of the verification phase, the second is increasing the length of message, and the last is improving the security of QKD. In fact, with the current quantum technologies, attackers find it more difficult to forge the signature since they cannot capture transmitted information, such as $|S\rangle_D$ and $|M\rangle'_O$, without any error.

Denial may lead to delaying or even stopping communication, which should be avoided in practice. In the scheme, a situation that Bob claims he receives nothing but he has already received Alice’s
signature may occur and it can be alleviated as follows: Alice waits for a moment then she sends another signature to him again, which may lengthen the communication time, while the scheme is still secure because $K_{RO}$ is only known by Alice. In other words, Alice never sends original keys to Bob unless she accepts these verifications from Bob and Trent. i.e., Bob cannot deny Alice’s signature when he has sent verifications, since the loyal Trent knows the communication process.

In addition, the simulations of the CPCOs are implemented on Strawberry Fields [49] interactive web app to validate the feasibility of the scheme. The related parameters for the experiment are shown in Table 4, and the schematic is shown in Figure 4. In particular, four input coherent states are designed as $|0 + 2i\rangle$, $|-1 + 0i\rangle$, $|4 + 0i\rangle$ and $|0 + 3i\rangle$, and $K_{final} = \{2, 4, 1, 3\}$. According to the CPCO rule, the encryption process can be stated as

$$PCO(M_3, M_4)PCO(M_1, M_3)PCO(M_4, M_2)PCO(M_2, M_1)|0 + 2i\rangle|-1 + 0i\rangle|4 + 0i\rangle|0 + 3i\rangle$$ (22)

$$= |-2 + 0i\rangle|1 + 0i\rangle|0 + 4i\rangle|0 - 3i\rangle.$$

In $PCO(M_2, M_1)|0 + 2i\rangle|-1 + 0i\rangle$, for example, the output phase of the first port is shifted by $\pi$. As a consequence, the control-phase gate $P_{21}$ in Figure 4 can be set to achieve the goal in the simulation. Simulated results are presented in Figure 5 where the subfigures (a), (b), (c), and (d) separately represent the quadrature outputs of the first, the second, the third and the forth port and $x, p \in (-5, 5)$, i.e., the cutoff dimension is 5. It can be seen that the correct quantum coherent states can be acquired with the 80% fidelity. For example, in Figure 5a, the probability of $x = -2$ is 0.8 and the probability of $p = 0$ is also 0.8. Therefore, the coherent state $|-2 + 0i\rangle$ will be output with the high probability 0.8.

**Table 4.** Experimental results with the the key-length $n = 4$, $K_{final} = \{2, 4, 1, 3\}$. “Modes” represent the position of input and output ports of the design schematic, such as, $q[k]_{k=0,1,2,3}$ is the $k$-th port.

| Modes | $q[0]$ | $q[1]$ | $q[2]$ | $q[3]$ |
|-------|--------|--------|--------|--------|
| Input | $|0 + 2i\rangle$ | $|-1 + 0i\rangle$ | $|4 + 0i\rangle$ | $|0 + 3i\rangle$ |
| Expected Output | $|-2 + 0i\rangle$ | $|1 + 0i\rangle$ | $|0 + 4i\rangle$ | $|0 - 3i\rangle$ |

**Figure 4.** Design schematic on the CPCOs with four input ports whose values are $|0 + 2i\rangle$, $|-1 + 0i\rangle$, $|4 + 0i\rangle$ and $|0 + 3i\rangle$ respectively. $P_{hk}$ represents the PCO where the $h$-th coherent state controls the $k$-th coherent state. Square dots ■ in the gray virtual box represents multiple judgement conditions referred to Equation (2). “HD” in the red box is the heterodyne detection [56].
Figure 5. Experimental results. The subfigures (a–d) represent the output of the first mode, the second mode, the third mode and the forth mode, respectively. The vertical axis indicates the probability that $x$ or $p$ takes a value on the horizontal axis. Besides, $x$ and $p$ can take the corresponding value under the maximum probability to form a coherent state .

5. Conclusions

A quantum dual signature scheme based on CPCOs and coherent states is presented in this paper, which can be used to guarantee the communication security between customer, merchant, and bank. The customer Alice has an order message and payment message which are separately sent to the merchant Bob and the bank Charlie. For preventing eavesdropping and attacking, Alice signs her two messages based on the CPCO encryption which can defend attacker’s forgery effectively. To ensure that the payment corresponds to the order, Alice then aggregates the two signatures to generate a quantum dual signature. The receiver Bob verifies the order message’s signature to confirm the identity of Alice and the information of order. When the signature of order message is valid, Bob transmits the payment message’s signature which is blind to him and Trent. Then Trent verifies whether the signature of payment message is authentic and sends the result to Bob. Security analysis shows that our scheme satisfies the security criteria of quantum signature. In other words, impossibility of forging, disavowing or denying for the signature protocol are observed in our scheme. In addition, simulation experiments are performed on the Strawberry Fields platform. The experimental results show that the proposed CPCOs are feasible and expected coherent states are obtained with high fidelity, which demonstrates that the scheme could be implemented on real quantum devices.

Author Contributions: Conceptualization, J.S. and S.C.; methodology, S.C. and J.L.; software, S.C. and Y.F.; validation, J.S., S.C. and J.L.; formal analysis, J.S., S.C. and J.L.; investigation, J.S., J.L., and Y.F.; resources, S.C. and J.L.; data curation, J.L. and F.L.; writing—original draft preparation, S.C. and J.L.; writing—review and editing, J.S., S.C., and F.L.; visualization, S.C. and F.L.; supervision, F.L. and R.S.; project administration, J.S. and S.C.; funding acquisition, J.S., J.L., F.L., and R.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61972418, 61872390, 61977062), the Natural Science Foundation of Hunan Province (2017JJ3415), the Training Program for Excellent Young Innovators of Changsha (Grant Nos. kq1905058).

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

The following abbreviations are used in this manuscript:

AQS  Arbitrated Quantum Signature
QGS  Quantum Group Signature
QPS  Quantum Proxy Signature
QBS  Quantum Blind Signature
GHZ  Greenberger-Horne-Zeilinger
QKD  Quantum Key Distribution
QOTPs Quantum One-Time Pads
PCO  Phase-Controlled Operation
CPCO Chained Phase-Controlled Operation
DPCO Phase-Controlled Operation for Decryption

References

1. Zeng, G.; Lee, M.; Guo, Y.; He, G. Continuous variable quantum signature algorithm. *Int. J. Quantum Inf.* 2007, 5, 553–573. [CrossRef]
2. Gao, F.; Qin, S.J.; Guo, F.Z.; Wen, Q.Y. Cryptanalysis of the arbitrated quantum signature protocols. *Phys. Rev. A* 2011, 84, 022344. [CrossRef]
3. Faz-Hernández, A.; Fujii, H.; Aranha, D.F.; López, J. A secure and efficient implementation of the quotient digital signature algorithm (qdsa). In Proceedings of the International Conference on Security, Privacy, and Applied Cryptography Engineering, Goa, India, 13–17 December 2017; pp. 170–189.
4. Jaju, S.A.; Chowhan, S.S. A Modified RSA algorithm to enhance security for digital signature. In Proceedings of the 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, BC, Canada, 15–17 October 2015; pp. 1–5.
5. Somani, U.; Lakhani, K.; Mundra, M. Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing. In Proceedings of the 2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010), Solan, India, 28–30 October 2010; pp. 211–216.
6. Yoo, Y.; Azarderakhsh, R.; Jalali, A.; Jao, D. A post-quantum digital signature scheme based on supersingular isogenies. In Proceedings of the International Conference on Financial Cryptography and Data Security, Sliema, Malta, 3–7 April 2017; pp. 163–181.
7. Galbraith, S.D.; Gaudry, P. Recent progress on the elliptic curve discrete logarithm problem. *Des. Codes Cryptogr.* 2016, 78, 51–72. [CrossRef]
8. Xiao, M.; Li, Z. Quantum broadcasting multiple blind signature with constant size. *Quantum Inf. Process.* 2016, 15, 3841–3854. [CrossRef]
9. Shi, R. A generic quantum protocol for one-sided secure two-party classical computations. *Quantum Inf. Process.* 2020, 19, 22. [CrossRef]
10. Shi, J.; Chen, S.; Lu, Y.; Feng, Y.; Shi, R.; Yang, Y.; Li, J. An Approach to Cryptography Based on Continuous-Variable Quantum Neural Network. *Sci. Rep.* 2020, 10, 1–3. [CrossRef]
11. Feng, Y.Y.; Shi, R.H.; Shi, J.J.; Guo, Y. Arbitrated quantum signature scheme based on quantum walks. *Acta Phys. Sin.* 2019, 68, 120302. [CrossRef]
12. Feng, Y.; Shi, R.; Shi, J.; Zhou, J.; Guo, Y. Arbitrated quantum signature scheme with quantum walk-based teleportation. *Quantum Inf. Process.* 2019, 18, 154. [CrossRef]
13. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 10th ed.; Cambridge University Press (CUP): Cambridge, UK, 2011.
14. Wang, B.; Wu, X.; Meng, F. Trigonometric collocation methods based on Lagrange basis polynomials for multi-frequency oscillatory second-order differential equations. *J. Comput. Appl. Math.* 2017, 313, 185–201. [CrossRef]
15. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* 1999, 41, 303–332. [CrossRef]
16. Busch, P.; Heinonen, T.; Lahti, P. Heisenberg’s uncertainty principle. *Phys. Rep.* 2007, 452, 155–176. [CrossRef]
17. Greenberger, D.; Klaus, H.; Friedel, W. (Eds.) *Compendium of Quantum Physics: Concepts, Experiments, History and Philosophy*; Springer Science and Business Media: Berlin, Germany, 2009.

18. Giordani, T.; Flamini, F.; Pompili, M.; Viggianiello, N.; Spagnolo, N.; Crespi, A.; Osellame, R.; Wiebe, N.; Walschaers, M.; Buchleitner, A.; et al. Experimental statistical signature of many-body quantum interference. *Nat. Photonics* **2018**, *12*, 173. [CrossRef]

19. Kang, M.S.; Choi, H.W.; Pramanik, T.; Han, S.W.; Moon, S. Universal quantum encryption for quantum signature using the swap test. *Quantum Inf. Process.* **2018**, *17*, 254. [CrossRef]

20. Yang, Y.G.; Lei, H.; Liu, Z.C.; Zhou, Y.H.; Shi, W.M. Arbitrated quantum signature scheme based on cluster states. *Quantum Inf. Process.* **2016**, *15*, 2487–2497. [CrossRef]

21. Guo, Y.; Feng, Y.; Huang, D.; Shi, J. Arbitrated quantum signature scheme with continuous-variable coherent states. *Int. J. Theor. Phys.* **2016**, *55*, 2290–2302. [CrossRef]

22. Xu, G.B.; Zhang, K.J. A novel quantum group signature scheme without using entangled states. *Quantum Inf. Process.* **2015**, *14*, 2577–2587. [CrossRef]

23. Shi, J.; Chen, H.; Zhou, F.; Huang, L.; Chen, S.; Shi, R. Quantum blind signature scheme with cluster states based on quantum walk cryptosystem. *Int. J. Theor. Phys.* **2019**, *58*, 1337–1349. [CrossRef]

24. Shi, J.; Shi, R.; Guo, Y.; Peng, X.; Tang, Y. Batch proxy quantum blind signature scheme. *Sci. China Inf. Sci.* **2013**, *56*, 1–9. [CrossRef]

25. Xu, G. Novel quantum proxy signature without entanglement. *Int. J. Theor. Phys.* **2015**, *54*, 2605–2612. [CrossRef]

26. Fan, L.; Zhang, K.J.; Qin, S.J.; Guo, F.Z. A novel quantum blind signature scheme with four-particle GHZ states. *Int. J. Theor. Phys.* **2016**, *55*, 1028–1035. [CrossRef]

27. Shi, J.; Shi, R.; Tang, Y.; Lee, M.H. A (t, n)-threshold scheme of multi-party quantum group signature with irregular quantum fourier transform. *Int. J. Theor. Phys.* **2012**, *51*, 1038–1049. [CrossRef]

28. Tian, J.H.; Zhang, J.Z.; Li, Y.P. A quantum multi-proxy blind signature scheme based on genuine four-qubit entangled state. *Int. J. Theor. Phys.* **2016**, *55*, 809–816. [CrossRef]

29. Guo, W.; Zhang, J.Z.; Li, Y.P.; An, W. Multi-proxy strong blind quantum signature scheme. *Int. J. Theor. Phys.* **2016**, *55*, 3524–3536. [CrossRef]

30. Shi, J.; Shi, R.; Tang, Y.; Lee, M.H. A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform. *Quantum Inf. Process.* **2011**, *10*, 653–670. [CrossRef]

31. Gottesman, D.; Chuang, I. Quantum digital signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.

32. Zeng, G. Reply to Comment on Arbitrated quantum-signature scheme. *Phys. Rev. A* **2008**, *78*, 016301. [CrossRef]

33. Zou, X.; Qiu, D. Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A* **2010**, *82*, 042325. [CrossRef]

34. Brandão, F.G.S.L.; Oppenheim, J. Quantum One-Time Pad in the Presence of an Eavesdropper. *Phys. Rev. Lett.* **2012**, *108*, 040504. [CrossRef]

35. Wang, C.; Liu, X.; Liu, J.; Shang, T.; Chen, X. Improved arbitrated quantum signature scheme using Bell states. In *Proceedings of the Communications Security Conference (CSC 2014)*, Beijing, China, 22–24 May 2014; pp. 1–6.

36. Dunjko, V.; Wallden, P.; Andersson, E. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.* **2012**, *108*, 040504. [CrossRef]

37. Luo, Q.B.; Yang, G.W.; She, K.; Li, X.Y.; Fang, J.B. Quantum homomorphic signature based on Bell-state measurement. *Quantum Inf. Process.* **2016**, *15*, 5051–5061. [CrossRef]

38. Hwang, J.J.; Yeh, T.C.; Li, J.B. Securing on-line credit card payments without disclosing privacy information. *Comput. Stand. Interfaces* **2003**, *25*, 119–129. [CrossRef]
43. Hassinen, M.; Hypponen, K. Strong mobile authentication. In Proceedings of the 2005 2nd International Symposium on Wireless Communication Systems, Siena, Italy, 5–9 September 2005; pp. 96–100.

44. 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. [CrossRef]

45. 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. [CrossRef]

46. Li, F.G.; Shi, J.H. An arbitrated quantum signature protocol based on the chained CNOT operations encryption. Quantum Inf. Process. 2015, 14, 2171–2181. [CrossRef]

47. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 2002, 88, 057902. [CrossRef]

48. Sanders, B.C. Review of entangled coherent states. J. Phys. A Math. Theor. 2012, 45, 244002. [CrossRef]

49. Killoran, N.; Izaac, J.; Quesada, N.; Bergholm, V.; Amy, M.; Weedbrook, C. Strawberry Fields: A Software Platform for Photonic Quantum Computing. Quantum 2019, 129, 3. [CrossRef]

50. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. Phys. Rev. Lett. 2006, 97, 190503. [CrossRef] [PubMed]

51. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J. Phys. B Atom. Mol. Opt. Phys. 2009, 42, 114014. [CrossRef]

52. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. Nat. Photonics 2014, 8, 595–604. [CrossRef]

53. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photonics 2013, 7, 378–381. [CrossRef]

54. Becerra, F.E.; Fan, J.; Migdall, A. Implementation of generalized quantum measurements for unambiguous discrimination of multiple non-orthogonal coherent states. Nat. Commun. 2013, 4, 1–6. [CrossRef]

55. Leverrier, A.; García-Patrón, R.; Renner, R.; Cerf, N.J. Security of Continuous-Variable Quantum Key Distribution Against General Attacks. Phys. Rev. Lett. 2013, 110, 030502. [CrossRef]

56. Campagne-Ibarcq, P.; Six, P.; Bretheau, L.; Sarlette, A.; Mirrahimi, M.; Rouchon, P.; Huard, B. Observing quantum state diffusion by heterodyne detection of fluorescence. Phys. Rev. X 2016, 6, 011002. [CrossRef]