applied sciences

MDPI

Article

Quantum Proxy Signature Scheme with Discrete Time Quantum Walks and Quantum One-Time Pad CNOT Operation

Yanyan Feng [†], **Qian Zhang** [†], **Jinjing Shi** [*], **Shuhui Chen and Ronghua Shi**

School of Computer Science and Engineering, Central South University, Changsha 410083, China; fengyanyanhenu@163.com (Y.F.); 15274999982@163.com (Q.Z.); shuhuichen1996@163.com (S.C.); shirh@csu.edu.cn (R.S.)

* Correspondence: shijinjing@csu.edu.cn

† These authors contributed equally to this work.

Received: 23 July 2020; Accepted: 19 August 2020; Published: 20 August 2020

Abstract: The quantum proxy signature is one of the most significant formalisms in quantum signatures. We put forward a quantum proxy signature scheme using quantum walk-based teleportation and quantum one-time pad CNOT (QOTP-CNOT) operation, which includes four phases, i.e., initializing phase, authorizing phase, signing phase and verifying phase. The QOTP-CNOT is achieved by attaching the CNOT operation upon the QOTP and it is applied to produce the proxy signature state. The quantum walk-based teleportation is employed to transfer the encrypted message copy derived from the binary random sequence from the proxy signer to the verifier, in which the required entangled states do not need to be prepared ahead and they can be automatically generated during quantum walks. Security analysis demonstrates that the presented proxy signature scheme has impossibility of denial from the proxy and original signers, impossibility of forgery from the original signatory and the verifier, and impossibility of repudiation from the verifier. Notably, the discussion shows the complexity of the presented algorithm and that the scheme can be applied in many real scenarios, such as electronic payment and electronic commerce.

Keywords: quantum communication; quantum proxy signature; quantum walks; quantum one-time pad CNOT operation

1. Introduction

Digital signature has been prevalent in past decades and applied in lots of scenes, such as electronic payment, electronic commerce and electronic government affairs, with strict demands for security. To satisfy the special requirements for diverse application scenarios, many ramifications of classical signature have occurred. The most concerning issue is the security of the classical signature scheme, which depends on computational complexity of some intractable problems involving the factorization of large numbers and the discrete logarithm. However, these problems can be efficiently solved by quantum algorithms with the development of quantum computation. For example, the former can be solved in polynomial time by Shor's quantum prime factorization algorithm [1]. Grover's algorithm [2] poses a great threat to symmetric cryptography by designing a more optimized brute force attack. Consequently, the classical signature schemes based on computational complexity are seriously struck and become insecure.

Motivated by the merits of quantum technology, many scholars converted their attention from classical signature into quantum signature, the security of which is guaranteed by quantum non-cloning theorem [3] and Heisenberg's uncertainty principle [4]. The development of quantum signature mainly relies on two essential techniques involving quantum teleportation and quantum encryption algorithm. Recently, quantum walks have been developed as an approach to realize quantum teleportation protocols [5,6], which can improve the efficiency of quantum teleportation in terms of entanglement generation and measurements. Afterwards, Shang and Li [7] showed the experimental realization of state transfer based on quantum walks with two coins. Chatterjee et al. [8] investigated the experimental implementation of quantum teleportation using coined quantum walks. Li et al. [9] also proposed a quantum teleportation scheme for transmitting an arbitrary multi-qubit state via multi-walker quantum walks. In addition, in 2017, Vlachou et al. [10] introduced the idea of developing quantum key distribution protocol using quantum walks. Inspired by the above-mentioned work, enthusiastic scholars have presented several achievements in quantum signature. For example, in 2019 Shi et al. [11] presented a quantum blind signature scheme based on quantum walk-based cryptosystem. In the same year, Feng et al. put forward an arbitrated quantum signature protocol with quantum walks on complete graphs [12] and on a closed cycle [13], in which the necessary entangled states do not need to be prepared in advance and they can be created naturally via quantum walks. Furthermore, when transmitting a d-dimensional quantum state, two projective measurements with d elements instead of one joint measurement with d^2 elements are required. The projective measurements are much easier to implement than the joint measurement in real experiments [5,6]. In 2020, Feng et al. [14] suggested another arbitrated quantum signature protocol, where quantum walk-based teleportation is applied to transfer the encrypted message copy and boson sampling-based random unitary encryption is used to generate the signature. Quite recently, Li et al. [15] applied quantum walks into quantum blind signature and presented the corresponding quantum blind signature scheme. Furthermore, quantum walks have been demonstrated to be realizable in different physical systems [16–18] and real experiments [19–21]. This stimulates us to explore more possibility of quantum walks into other types of quantum signature.

Quantum proxy signature is an important type or branch of quantum signature and its concept was first proposed by Mambo et al. [22] in 1996. In 2001, Gottesman and Chuang [23] introduced quantum mechanics into digital signature and proposed a quantum digital signature scheme based on one-way function. Soon later, Zeng and Keitel [24] proposed an arbitrated quantum signature scheme based on three-qubit Green-Horne-Zeilinger (GHZ) states, which provides an elegant framework for designing quantum signature schemes with the participation of a trusted arbitrator. Notably, quantum proxy signature is a special class in arbitrated quantum signature with distinct original signatory and proxy signatory. In 2010, Chang et al. [25] presented a proxy signature scheme by employing Einstein-Podolsky-Rosen (EPR) states as the quantum channel for teleportation. In 2011, Zhou et al. [26] proposed a quantum proxy signature scheme based on public verifiability, in which EPR states are combined with the unitary transformation to generate proxy signature. In 2014, Cao et al. [27] raised a quantum weak blind signature scheme with a genuinely entangled six-qubit state. Subsequently, Zhang and Jia [28] analyzed the cryptanalysis of Cao et al.'s work [27] and pointed out that the verifier can forge the signature by modifying the received message without being caught. Next year, Cao et al. [29] put forward a proxy weak blind signature using the controlled teleportation scheme with five-qubit entangled states as quantum channels. Based on the above-described research, it is known that entangled states take up a significant position in designing quantum signature schemes. Yet, the challenge is that the generation of the ideal entanglement resource is difficult in experiments. To this end, many scholars began to seek for other methods to evade this challenge. For example, in 2015, Xu et al. [30] brought forward a quantum proxy signature scheme in line with single-particle states instead of entangled states. In the next year, Guo et al. [31] suggested a strong blind quantum signature scheme with multi-proxy by executing appropriate unitary operators. In 2018, Qin et al. [32] brought forward a batch quantum multi-proxy signature, in which quantum controlled-not (CNOT) gates are employed to encode the information to be signed. Recently, Niu et al. [33] developed a quantum proxy blind signature based on superdense coding, where various unitary operators are used to blind two-bit classical information.

Compared to quantum proxy signature schemes without entanglement, it can be seen that the entanglement-based quantum proxy signature schemes have more ability to resist risks or attacks due to the disturbance detection owing to the existence of entanglement. In addition, we mentioned that the most challenge is the difficult generation of entanglement resource with the state-of-the-art technology, fortunately, which can be efficiently addressed using the models of quantum walks. On the other hand, in the existing quantum proxy signature schemes, the involved encryption algorithm is quantum one-time pad (QOTP), which may lead to different aspects of disavowal and forgery attacks [34,35]. To solve this issue, we improve the QOTP by introducing the CNOT operation. Therefore, motivated by quantum walk-based teleportation, we present a proxy signature scheme using quantum walks and QOTP-CNOT operation. The presented quantum proxy signature scheme makes the following contributions.

- Before generating the proxy signature, the random binary sequence is circularly used to encrypt the original message. Then the QOTP-CNOT operation is used to generate the proxy signature state with the length of the secret keys being the same as that of the message to be encrypted, which reduces the length of the required keys by three times in terms of efficiency and improves the security of the presented scheme. The introduction of CNOT operation into the QOTP makes the encrypted qubit related to not only the qubit and the key of the current position but also other qubits and keys of other positions, which can resist against the proxy signatory's disavowal attack and the receiver's forgery attack on the proxy signature by modifying the qubits of particular positions in it.
- Quantum walks on circles are used to transfer the random sequence to verify the validity of the proxy warranty and the corresponding quantum teleportation protocol is performed to transmit the message copy of ciphertext from the proxy signatory to the verifier, which assists the verifier to complete the verification of the validity of the proxy signature, in which it is unnecessary to generate entangled states in advance as quantum channels and the essential entangled states can be created by quantum walks. We note that this model differs from the formalisms of quantum walks employed in [12,14] and that it is firstly employed in quantum proxy signature.
- The proposed scheme may be easy to implement owing to the experimental realizations of quantum walks [7,8] and the designed QOTP-CNOT encryption. Furthermore, it may be applied into electronic payment or electronic commerce.

The paper is organized as follows. In Section 2, we present the methods involving the employed models, i.e., quantum walks on circles and the corresponding quantum teleportation, and the designed quantum proxy signature scheme consisting of initializing phase, authorizing phase, signing phase and verifying phase. In Section 3, we elaborate on the results referring to the security of the scheme. In Section 4, we discuss the complexity and the applications of the presented scheme. In Section 5, a conclusion is shown.

2. Methods

Quantum walk is the quantum counterpart of classical random walk such as Brownian motion. In 1993, Aharonov et al. [36] first proposed the formalism of quantum walk. Then in 2001 Ambainis et al. and Aharonov et al. presented the formalisms of quantum walks on the line [37] and on the general graphs [38]. According to the time evolution, quantum walk is distinguished into discrete time quantum walk [39] and continuous time quantum walk [40]. In the following, we first focus on the discrete time quantum walk models we use in the subsequent process. Then we describe the proposed quantum proxy signature scheme.

2.1. Quantum Walks on Circles

In discrete time setting, the properties of quantum walk depend on quantum coins and shift operators. In this model, we assume that the walker hops along discrete positions on a circle graph.

The corresponding Hilbert space H is the tensor product of the position Hilbert space H_p and the coin Hilbert space H_c, i.e.,

$$H = H_p \otimes H_c, \tag{1}$$

where H_p is spanned by the vertices on the circle with $H_p = \{|x\rangle | x \in \{0, 1, \ldots, P-1\}\}$ and P is the number of vertices, and H_c is spanned by the two possible coin states $\{|R\rangle, |L\rangle\}$ corresponding to the head and tail of a quantum coin [10]. The evolution for one step of the quantum walk is given by the unitary operator with

$$U_k = O \cdot (I_p \otimes R_c), \tag{2}$$

where I_p is the identity operator acting on H_p, R_c is a rotation gate acting on H_c that is expressed as in terms of matrix

$$R_c = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \tag{3}$$

where $\theta \in [0, 2\pi]$ refers to the rotation angle, and O is a conditional shift operator with the form of

$$O = \sum_{x=0}^{P-1} [|(x+1) \mod P\rangle\langle x| \otimes |R\rangle\langle R| + |(x-1) \mod P\rangle\langle x| \otimes |L\rangle\langle L|], \tag{4}$$

which simulates the movement of walker on the circle [41], as shown in Figure 1. In the following, we use this model to transmit the involved random sequence from the proxy signatory to the arbitrator to complete the validity of the proxy warranty.

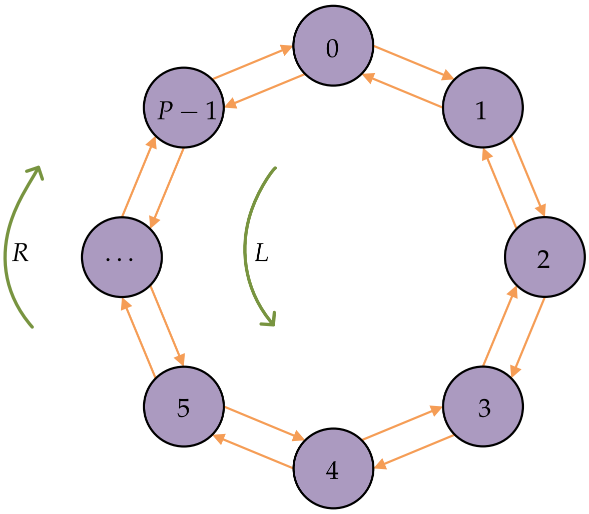


Figure 1. Shift rules of quantum walks on a circle with P vertices.

2.2. Teleportation with Quantum Walks on Circles

In view of the model of quantum walks on circles above, we describe the teleportation based on quantum walks on circles with two coins and $P = 4$ vertices. We postulate that Alice and Bob are the sender and the receiver, respectively, who participate in the communication, in which Alice wants to transfer an unknown qubit $|\phi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ to Bob. Alice holds two particles $a1$ and $a2$, which separately carry the state of the first coin and the state of the position. While the state of the second coin is encoded onto particle b, which is possessed by Bob. The initial states of $a1$, $a2$ and b are denoted as $|\phi_i\rangle$, $|0\rangle$ and $|+\rangle$. Thus, the whole initial state of the quantum walk system is

$$|\psi\rangle^0 = |0\rangle \otimes (\alpha_i|0\rangle + \beta_i|1\rangle) \otimes |+\rangle, \tag{5}$$

with the particle order $a2$, $a1$, b and $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

We formulate the first step of the quantum walk as

$$U_1 = W_1 \cdot (I_p \otimes C_1 \otimes I_2), \tag{6}$$

where $W_1 = Q \otimes |0\rangle_1\langle 0| \otimes I_2 + Q^\dagger \otimes |1\rangle_1\langle 1| \otimes I_2 = O' \otimes I_2$, C_1 is the coin operator employed on the first coin state, $Q = \sum_x |x+1\rangle\langle x|$ is the shift operator employed on the position space and $Q^\dagger$ is the Hermitian operator of Q. According to Equation (4), for convenience of calculation, we equate $|R\rangle$ to $|0\rangle$ and $|L\rangle$ to $|1\rangle$ and then we can express the notation O' with $P = 4$ as

$$O' = \sum_{x=0}^{2} |x+1\rangle\langle x| \otimes |0\rangle\langle 0| + \sum_{x=1}^{3} |x-1\rangle\langle x| \otimes |1\rangle\langle 1| + |0\rangle\langle 3| \otimes |0\rangle\langle 0| + |3\rangle\langle 0| \otimes |1\rangle\langle 1|. \tag{7}$$

If $C_1 = I$, the initial system state $|\psi\rangle^0$ transforms into

$$|\psi\rangle^1 = \frac{1}{\sqrt{2}}(\alpha_i|1\rangle|0\rangle|0\rangle + \beta_i|3\rangle|1\rangle|1\rangle), \tag{8}$$

which produces the entanglement between position space and coin space referring to Alice and Bob.

We describe the second step of the quantum walk as

$$U_2 = W_2 \cdot (I_p \otimes I_1 \otimes C_2), \tag{9}$$

where

$$W_2 = Q \otimes I_1 \otimes |0\rangle_2\langle 0| + Q^\dagger \otimes I_1 \otimes |1\rangle_2\langle 1| = O' \otimes I_1 \tag{10}$$

and C_2 is the coin operator employed on the second coin state. If $C_2 = I$, the state of the system evolves into

$$|\psi\rangle^2 = \frac{|0\rangle \otimes (\alpha_i|01\rangle + \beta_i|10\rangle)}{\sqrt{2}} + \frac{|2\rangle \otimes (\alpha_i|00\rangle + \beta_i|11\rangle)}{\sqrt{2}}. \tag{11}$$

Subsequently, Alice first measures particle $a2$ using basis $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ corresponding to the classical results $\{0, 1, 2, 3\}$. Then Alice measures particle $a1$ using basis $\{|+\rangle, |-\rangle\}$ corresponding to the classical results $\{1, -1\}$. In the light of the measurement results of $a2$ and $a1$, Bob implements corresponding unitary operations to recover the qubit to be teleported, which is listed in Table 1. In the following, this teleportation scheme is employed to transfer the encrypted qubit message copy from the signatory to the verifier, which helps to complete the validity verification of the completed proxy signature.

Table 1. The relationship of the measurement results of $a2$ and $a1$ from Alice and Bob's local unitary operations.

*a*2	*a*1	Unitary Operation
2	1	I
2	−1	Z
0	1	X
0	−1	ZX

2.3. *Quantum Proxy Signature Scheme*

The designed scheme involves four participants, i.e., the arbitrator Trent, the original signer Charlie, the proxy signer Alice and the verifier Bob, who cooperatively perform four desired phases, including the initializing phase, the authorizing phase, the signing phase and the verifying phase. The schematic of the scheme is depicted in Figure 2 and the details are elaborated in the respective four phases in the following. Remarkably, we suppose that the interactive communications among participants are executed via authenticated classical and quantum channels, which can be realized by means of current error correction and privacy amplification technologies [42] in secure communication protocols [43,44]. Thus, we mainly concentrate on the denial and the forgery attacks from the internal participants.

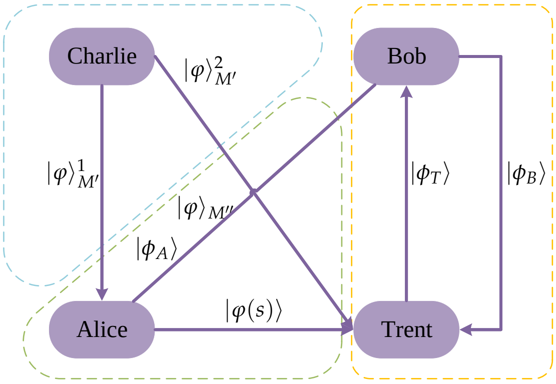


Figure 2. Schematic of the designed quantum proxy signature scheme. Charlie, Alice, Bob, and Trent are the original signer, the proxy signer, the verifier and the arbitrator, respectively. Notably, blue dashed box represents the initializing phase and authorizing phase, and green represents the signing phase and orange represents the verifying phase.

2.3.1. Initializing Phase

In initializing phase, Charlie is required to prepare the quantum carriers of the original message and all the secret keys for encryption and decryption processes are produced.

Step 1 Charlie holds a classical binary string M with $n1$ bits, which is the original message to be signed and can be expressed as

$$M = \{M_1, M_2, \dots, M_i, \dots, M_{n1}\}, \tag{12}$$

where $M_i \in \{0, 1\}$, $i = 1, \dots, n1$. Then he or she encodes M into the corresponding qubit sequence $|\varphi\rangle_M$ with $n1$ qubits in the form of

$$|\varphi\rangle_M = \{|\varphi_1\rangle_M, |\varphi_2\rangle_M, \dots, |\varphi_i\rangle_M, \dots, |\varphi_{n1}\rangle_M\}, \tag{13}$$

where $|\varphi_i\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle + m|1\rangle)$, in which $m = 1$ or $m = -1$ corresponds to $M_i = 0$ or $M_i = 1$.

Step 2 Alice shares secret keys $\{K_{AT}, K_{AC}\}$ with Trent and Charlie, respectively. Similarly, Trent shares secret keys $\{K_{BT}, K_{CT}\}$ with Bob and Charlie. This procedure can be completed through QKD system [10,45,46].

2.3.2. Authorizing Phase

In authorizing phase, Charlie generates the warranty allowing Alice to execute the proxy signature.

Step 1 Charlie produces a quantum state $|\varphi\rangle_W$ with $n2$ qubits, which contains the information of Charlie's and Alice's identification and the warranty of proxy signature. In addition, $|\varphi\rangle_W$ is described as

$$|\varphi\rangle_W = \{|\varphi_1\rangle_W, |\varphi_2\rangle_W, \dots, |\varphi_i\rangle_W, \dots, |\varphi_{n2}\rangle_W\}, \tag{14}$$

where $|\varphi_i\rangle_W = \frac{1}{\sqrt{2}}(|0\rangle + m|1\rangle)$ with $m = 1$ or -1, $i = 1, \dots, n2$. Then he combines $|\varphi\rangle_M$ with $|\varphi\rangle_W$ to acquire a new quantum state $|\varphi\rangle_{M'}$ with

$$|\varphi\rangle_{M'} = (|\varphi\rangle_M, |\varphi\rangle_W) = \{|\varphi_1\rangle_{M'}, \dots, |\varphi_i\rangle_{M'}, \dots, |\varphi_n\rangle_{M'}\}, \tag{15}$$

which contains $n = n1 + n2$ qubits. We assume the dimension n of $|\varphi\rangle_{M'}$ to be large enough, which enables small enough error probability of two rounds of comparisons for any two unknown qubit states and failure probability of the validity verification for the completed signature in the verifying phase.

Step 2 Charlie separately encrypts two copies of the new quantum state $|\varphi\rangle_{M'}$ with K_{AC} and K_{CT} and gets $|\varphi\rangle^1_{M'} = E_{K_{AC}}(|\varphi\rangle_{M'})$ and $|\varphi\rangle^2_{M'} = E_{K_{CT}}(|\varphi\rangle_{M'})$. Next he sends $|\varphi\rangle^1_{M'}$ to Alice and $|\varphi\rangle^2_{M'}$ to Trent.

Step 3 After receiving $|\varphi\rangle^1_{M'}$, Alice obtains $|\varphi\rangle_{M'}$ by decrypting it and thus she has the authority to help Charlie and Bob complete the signature as a proxy signer.

2.3.3. Signing Phase

In signing phase, Alice generates the proxy signature based on chosen signing algorithm, which is expected to ensure Alice's undeniability, the integrity and authenticity of the message to be signed.

Step 1 Alice randomly chooses from $\{0, 1\}$ to generate an n-bit classical sequence

$$S = \{S_1, S_2, \ldots, S_i, \ldots, S_n\}. \tag{16}$$

Step 2 Alice encrypts $|\varphi\rangle_{M'}$ through appropriate encryption algorithm based on S and obtains $|\varphi\rangle_{M''}$ with

$$|\varphi\rangle_{M''} = E_S(|\varphi\rangle_{M'}). \tag{17}$$

For an arbitrary qubit $|\varphi_i\rangle_{M'}$ in $|\varphi\rangle_{M'}$, it can be expressed as follows,

$$|\varphi_i\rangle_{M''} = E_S(|\varphi_i\rangle_{M'}) = |\varphi_i\rangle_{M'} \otimes (I)^{\bar{S}_i \cdot \bar{S}_{i+1}} \otimes (\sigma_x)^{\bar{S}_i \cdot S}_{i+1} \otimes (\sigma_y)^{S_i \cdot \bar{S}_{i+1}} \otimes (\sigma_z)^{S_i \cdot S_{i+1}}, \tag{18}$$

where $i+1 = (i+1) \mod n$. Concretely, according to (S_i, S_{i+1}) in S, Alice performs the corresponding unitary operator on the qubit $|\varphi_i\rangle_{M'}$ [33], which is listed in Table 2. The relationship of $|\varphi\rangle_{M'}$, S and $|\varphi\rangle_{M''}$ is shown in Figure 3, in which it can be seen that the operation on the last qubit $|\varphi_n\rangle_{M'}$ of $|\varphi\rangle_{M'}$ is controlled by (S_n, S_1), which shows the random sequence is used circularly. Then Alice needs to broadcast the value of n. It should be noted that, in our scheme, three copies of $|\varphi\rangle_{M''}$ are required. One of them is employed to create proxy signature state, the other is delivered to Bob along with the proxy signature state at the last step in the signing phase and the third one is transmitted by teleportation based on quantum walks on circles with two coins described in Section 2.2.

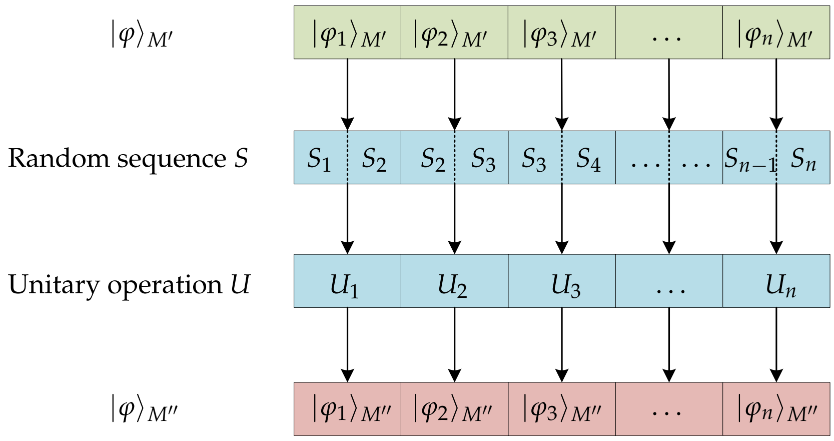


Figure 3. Alice packages $|\varphi\rangle_{M'}$ with unitary operation U governed by the random sequence S to obtain $|\varphi\rangle_{M''}$.

Table 2. The relationship of (S_i, S_{i+1}) in the sequence S and the corresponding unitary operation.

(S_i, S_{i+1})	Unitary Operator	Matrix Representation
00	I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
01	σ_x	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
10	σ_y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
11	σ_z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Step 3 Alice generates proxy signature state $|S_A\rangle$ by encrypting $|\varphi\rangle_{M''}$ with K_{AT}, i.e.,

$$|S_A\rangle = E'_{K_{AT}}(|\varphi\rangle_{M''}), \tag{19}$$

where $E'_{K_{AT}}$ refers to the improved QOTP algorithm with assistant CNOT gates in terms of K_{AT}. Before elaborating on the QOTP-CNOT operation, we first describe the QOTP algorithm in the following, where $2n$ random classical bits are required for the encryption of an unknown n-qubit quantum state with the guarantee of informational security [47,48]. Denote $|\phi\rangle$ as the n-qubit message expected to be encrypted with $|\phi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ and K_q as the $2n$-bit key. The encryption process is formulated as

$$|\phi\rangle_C = E_{K_q}(|\phi\rangle) = \bigotimes_{i=1}^{n} (\sigma_x)^{K_q^{2i}} (\sigma_z)^{K_q^{2i-1}} |\phi_i\rangle, \tag{20}$$

where K_q^p is the pth bit of K_q. The corresponding decryption process is

$$|\phi\rangle = D_{K_q}(|\phi\rangle_C) = \bigotimes_{i=1}^{n} (\sigma_z)^{K_q^{2i-1}} (\sigma_x)^{K_q^{2i}} |\phi_i\rangle_C. \tag{21}$$

Then the motivation of the QOTP-CNOT operation includes the following two aspects. The first aspect is from some classical coding schemes, such as the differential encoding, where the encrypted bits correlate with the other bits in order to improve its capacity of resisting disturbance. The second motivation originates from the existing quantum signature schemes, such as chain-based CNOT [49], key-controlled chained CNOT [50], which make the encrypted qubit related to not only the qubit and the key of the current position but also other qubits and keys of other positions. We thus design the improved QOTP encryption algorithm by introducing assistant CNOT gates. In addition, considering the storage space and usage efficiency of the secret key, we circularly use the key to accomplish the encryption task, the length of which is reduced into one third of the key required in the QOTP algorithm. Therefore, in terms of both security and efficiency, we put forward the QOTP-CNOT encryption algorithm, in which we write the required K_{AT} as

$$K_{AT} = \{K_{AT}^1, K_{AT}^2, \ldots, K_{AT}^i, \ldots, K_{AT}^n\}. \tag{22}$$

The length of K_{AT} is assumed to be the same with the length of $|\varphi\rangle_{M''}$, i.e., n. Alice executes the corresponding operation on the qubit $|\varphi_i\rangle_{M''}$ in $|\varphi\rangle_{M''}$ according to the values of $(K_{AT}^i, K_{AT}^{i+1}, K_{AT}^{i+2})$, where K_{AT}^i decides whether σ_x is operated on the corresponding qubit with $(\sigma_x)^{K_{AT}^i}$ and K_{AT}^{i+1} controls the operation of σ_z with $(\sigma_z)^{K_{AT}^{i+1}}$ and K_{AT}^{i+2} determines whether the CNOT operation is applied on $|\varphi_i\rangle_{M''}$ with $|S_A\rangle_{i-1}$ acting as the control qubit. The encryption process can be expressed as follows,

$$|S_A\rangle_i = \begin{cases} |\varphi_i\rangle_{M''} \otimes (\sigma_x)^{K_{AT}^i} \otimes (\sigma_z)^{K_{AT}^{i+1}} \otimes (\sigma_x)^{K_{AT}^{i+2} \cdot |S_A\rangle_{i-1}} & i \neq 1, n-1, n. \\ |\varphi_i\rangle_{M''} \otimes (\sigma_x)^{K_{AT}^i} \otimes (\sigma_z)^{K_{AT}^{i+1}} \otimes (\sigma_x)^{K_{AT}^{i+2} \cdot |\varphi_n\rangle_{M''}} & i = 1. \\ |\varphi_i\rangle_{M''} \otimes (\sigma_x)^{K_{AT}^i} \otimes (\sigma_z)^{K_{AT}^{(i+1) \mod n}} \otimes (\sigma_x)^{|S_A\rangle_{i-1} \cdot K_{AT}^{(i+2) \mod n}} & i = n-1, n. \end{cases} \tag{23}$$

Here let us consider an instance to expound on it. Given $n = 8$, $|\varphi\rangle_{M''} = |01011101\rangle$ and $K_{AT} = 01011001$, in line with Equation (23), the encryption result of $|\varphi\rangle_{M''}$ should be $|00000100\rangle$, where the implementation of $|\varphi_2\rangle_{M''} = |1\rangle$ can be demonstrated as follows. According to the associated key $(K^2_{AT}, K^3_{AT}, K^4_{AT}) = (1, 0, 1)$, we can obtain the qubit $|S_A\rangle_2$ with the form of

$$|S_A\rangle_2 = |\varphi_2\rangle_{M''} \otimes (\sigma_x)^{K^2_{AT}} \otimes (\sigma_z)^{K^3_{AT}} \otimes (\sigma_x)^{K^4_{AT}\cdot|S_A\rangle_1} = |\varphi_2\rangle_{M''} \otimes \sigma_x \otimes (\sigma_x)^{|S_A\rangle_1} = |0\rangle, \tag{24}$$

which coincides with the presented encryption and decryption processes of $|\varphi\rangle_{M''}$ shown in Figures 4 and 5.

Step 4 To verify the validity of the proxy warranty, we apply the model of quantum walks on circles described in Section 2.1 to transmit the random sequence S from the proxy signer Alice to the arbitrator Trent. Assume that the number of the walking steps is t and $P = 2^n$, we denote $|l\rangle \in \{|0\rangle, \ldots, |P-1\rangle\}$ as one vertex state, $|d\rangle \in \{|R\rangle, |L\rangle\}$ as the coin state. Using these parameters, a quantum state can be randomly generated

$$|\varphi\rangle_U = U_k^t|l\rangle|d\rangle = [O \cdot (I_p \otimes R_c)]^t|l\rangle|d\rangle, \tag{25}$$

which is then distributed to Alice and Trent.

Step 5 Alice transforms the random sequence S as a decimal number s (this can be easily done) and obtains the following shift operator

$$T_s = \sum_{i=0}^{P-1} |(i+s) \mod P\rangle\langle i|, \tag{26}$$

which is used to produce

$$|\varphi(s)\rangle = (T_s \otimes I_c)|\varphi\rangle_U, \tag{27}$$

where I_c is the identity operator acting on the coin state and which is transmited to Trent.

Step 6 Trent applies U_k^{-t} to $|\varphi(s)\rangle$ and gains

$$|\varphi\rangle_S = (T_s \otimes I_c)|l\rangle|d\rangle, \tag{28}$$

on which he performs the position measurement

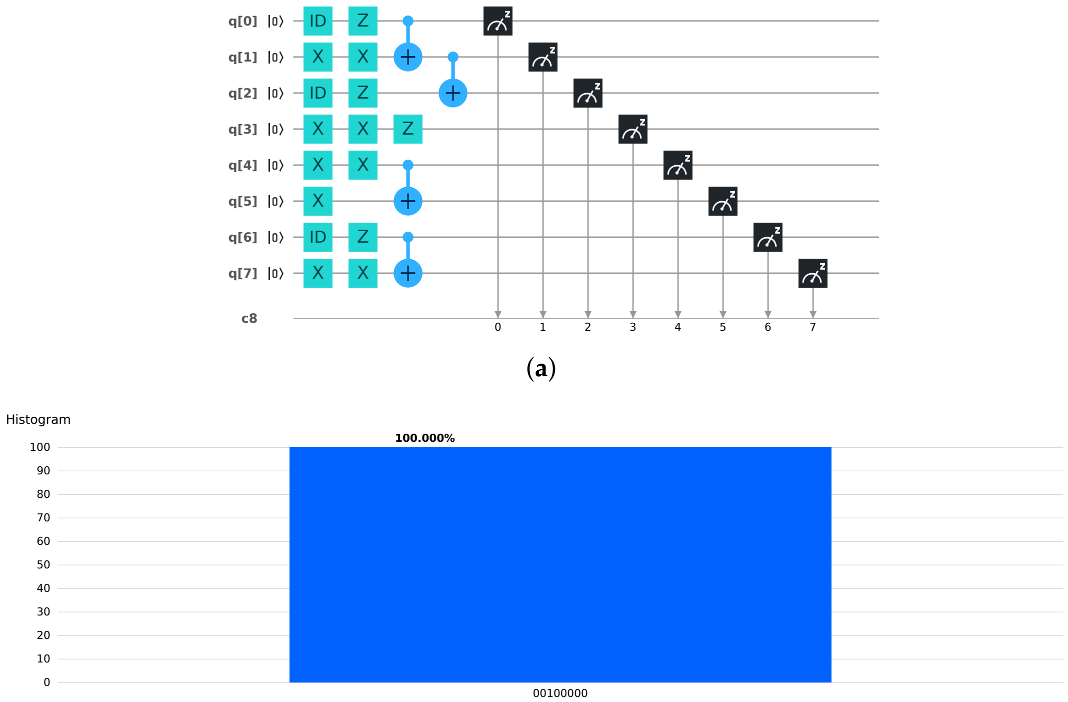
$$K = \sum_{i=0}^{P-1} |i\rangle\langle i| \otimes I_c. \tag{29}$$

Denoting the measurement result as i_s, i.e., $i_s = (l+s) \mod P$, we can obtain

$$s = (i_s - l) \mod P. \tag{30}$$

That is, Trent can easily recover S and obtain $|\varphi\rangle_{M'}$ from $|\varphi\rangle_{M''}$ according to the recovered S.

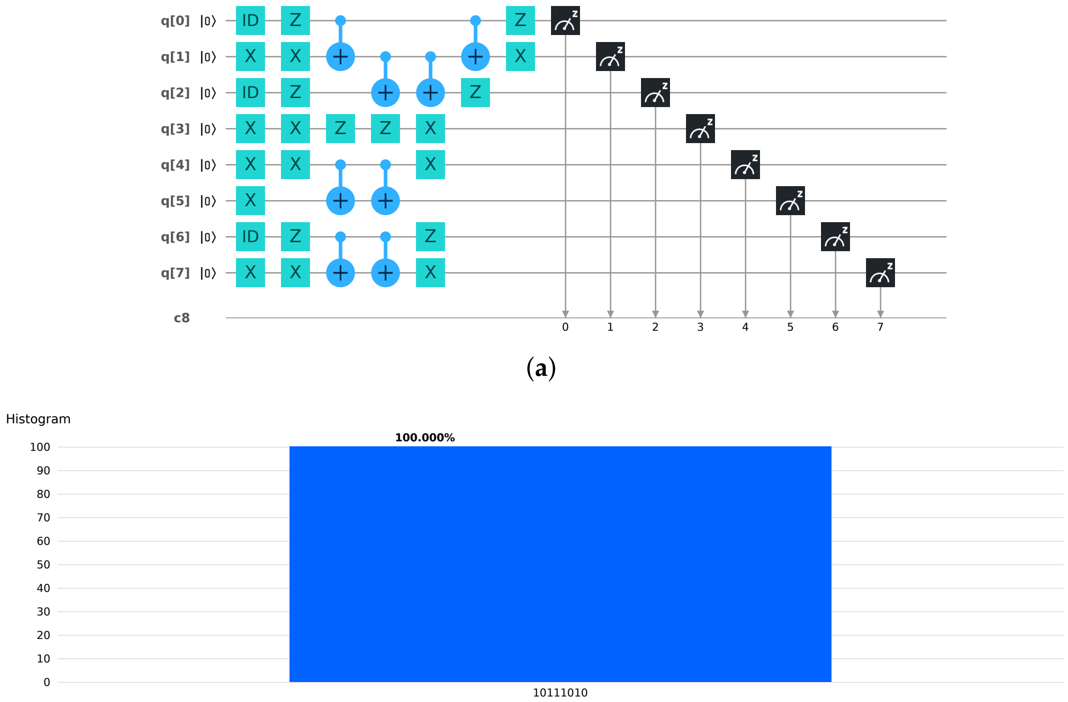
Step 7 After completing the verification of the proxy warranty, Alice produces a quantum state $|\phi_A\rangle = (|S_A\rangle, |\varphi\rangle_{M''})$ and sends it to Bob.



(**a**)

(**b**)

Figure 4. The encryption process of $|\varphi\rangle_{M''}$ based on K_{AT}. (**a**) Quantum circuit for the encryption process of $|\varphi\rangle_{M''}$ with $n = 8$ including X, Z and CNOT gates governed by K_{AT} and ID refers to the identity gate; (**b**) The probability producing the encrypted quantum state $|S_A\rangle$.



(**a**)

(**b**)

Figure 5. The decryption process for recreating $|\varphi\rangle_{M''}$ based on K_{AT}. (**a**) Quantum circuit for the encryption and decryption processes for obtaining $|\varphi\rangle_{M''}$. It can be seen that the gates for encryption and decryption processes are symmetric; (**b**) The probability recovering the quantum state $|\varphi\rangle_{M''}$.

2.3.4. Verifying Phase

In verifying phase, Bob is required to verify the validity of the completed proxy signature and the integrality and authenticity of the conveyed messages based on chosen verifying algorithm with the assistance of Trent, who plays the role of the trusted third party to facilitate the interaction of Alice and Bob.

Step 1 After receiving $|\phi_A\rangle$, Bob encrypts $|S_A\rangle$ and $|\varphi\rangle_{M''}$ using K_{BT} and gets $|\phi_B\rangle$, i.e.,

$$|\phi_B\rangle = E'_{K_{BT}}(|S_A\rangle, |\varphi\rangle_{M''}), \tag{31}$$

which is then transmitted to Trent.

Step 2 Trent decodes $|\phi_B\rangle$ to get $|S_A\rangle$ and $|\varphi\rangle_{M''}$. To begin with, with the acquired random sequence S by Steps 4–6 in the signing phase, Trent can perform the same unitary operators on $|\varphi\rangle_{M''}$ and obtains $|\varphi\rangle_{M'}^{\text{out}}$. He compares it with the obtained $|\varphi\rangle_{M'}$ from Charlie to verify whether the warranty delegated by Charlie to Alice is valid. If the warranty is consilient, Trent implements the associated unitary operations based on S on $|\varphi\rangle_{M'}$ or $|\varphi\rangle_{M'}^{\text{out}}$ to regain $|\varphi\rangle_{M''}$ and achieves $|S_T\rangle$ with K_{AT}. Afterwards, he compares $|S_T\rangle$ with $|S_A\rangle$ by using swap test technique [51], where the independent comparisons of $|S_T\rangle_i$ and $|S_A\rangle_i$ for n times are required. Thus, if the value of n is proper, for any $\varepsilon > 0$, the error probability can be reduced to $[\frac{1}{2}(1+\delta^2)]^n < \varepsilon$. It acts the same when Bob implements the comparison of the quantum states $|\varphi\rangle_{M''}$ and $|\varphi\rangle_{M''}^{\text{out}}$ to verify the completed signature in the later step. If the result τ is negative, the communication is terminated. Otherwise, Trent firstly decrypts $|S_T\rangle$ to gain $|\varphi\rangle_{M''}$ and then encrypts $|S_A\rangle$, $|\varphi\rangle_{M''}$ and $|\tau\rangle$ to generate $|\phi_T\rangle$, i.e.,

$$|\phi_T\rangle = E'_{K_{BT}}(|S_A\rangle, |\varphi\rangle_{M''}, |\tau\rangle), \tag{32}$$

which is delivered to Bob.

Step 3 Bob decrypts the received $|\phi_T\rangle$ and achieves $|S_A\rangle$, $|\varphi\rangle_{M''}$ and $|\tau\rangle$. If $\tau = 0$, it shows that $|S_A\rangle$ is disavowed or forged by some manner. That is, $|S_A\rangle$ is invalid and the protocol will be abandoned. Otherwise, Bob compares $|\varphi\rangle_{M''}$ and $|\varphi\rangle_{M''}^{\text{out}}$, which is obtained from Alice via teleportation protocol based on quantum walks on circles with two coins described in Section 2.2. If $|\varphi\rangle_{M''}^{\text{out}} \neq |\varphi\rangle_{M''}$, the communication fails. If $|\varphi\rangle_{M''}^{\text{out}} = |\varphi\rangle_{M''}$, Bob makes a request for announcing the random sequence S from Alice.

Step 4 Alice publishes S on the public channel.

Step 5 After receiving S, Bob decodes $|\varphi\rangle_{M''}^{\text{out}}$ or $|\varphi\rangle_{M''}$ and obtains the whole original message $|\varphi\rangle_{M'}$, in which the ith qubit $|\varphi_i\rangle_{M'}$ with $m_i = 1$ reveals $M_i = 0$ and $|\varphi_i\rangle_{M'}$ with $m_i = -1$ reveals $M_i = 1$. At this time, Bob can recognize $(|S_A\rangle, S)$ as Alice's completed proxy signature.

3. Results

In terms of secure criterions in quantum signature protocols, the designed signature scheme should satisfy the properties of non-deniability, non-forgeability, and non-repudiation. Based on these criterions, we analyze the security of our presented proxy signature scheme. Then we discuss the potentially practical application of our scheme.

3.1. Impossibility of Denials

In proxy signature scheme, the impossibility of denial refers to that the proxy signer Alice cannot deny her completed signature and that the original signer Charlie cannot deny his delegation.

For one thing, Alice cannot deny her completed signature. In the signing phase, Alice packages or encrypts quantum state $|\varphi\rangle_{M'}$ obtained from Charlie using the random sequence S and gets $|\varphi\rangle_{M''}$. Then Alice creates the proxy signature state $|S_A\rangle$ by encrypting $|\varphi\rangle_{M''}$ with the key K_{AT}, i.e., $|S_A\rangle = E'_{K_{AT}}(|\varphi\rangle_{M''})$, in which K_{AT} is essential for the creation of $|S_A\rangle$ and it is generated by QKD system with perfect security. If Alice disavows the completed signature, the state $|S_A\rangle$ should be forwarded to Trent and then he judges whether K_{AT} is contained in $|S_A\rangle$. If the feedback is positive, then $|S_A\rangle$ must be produced by Alice. If Alice successfully disavows $|S_A\rangle$ resulting in $|S_A\rangle \neq |S_T\rangle$ and the occurrence of disputes, fortunately, this attack can be found by Trent at Step 2 of verifying phase. Therefore, Trent is able to detect Alice's possible disavowals.

For another thing, Charlie cannot deny his delegation. In the authorizing phase, Charlie achieves a quantum state $|\varphi\rangle_{M'}$, which contains the information of his identification and proxy delegation. Then Charlie encrypts $|\varphi\rangle_{M'}$ with K_{CT} to acquire $|\varphi\rangle^2_{M'}$, i.e., $|\varphi\rangle^2_{M'} = K_{CT}(|\varphi\rangle_{M'})$, which is transferred to Trent and in which K_{CT} is also generated via QKD system. Moreover, in the signing phase, Trent receives S from Alice via the model of quantum walks on circles and in the verifying phase Trent obtains $|\varphi\rangle_{M''}$ from Bob included in quantum state $|\phi_B\rangle$. Next Trent can get $|\varphi\rangle_{M'}$ on account of S and the corresponding operations listed in Table 2, which proves that Charlie does authorize Alice to perform the signature behaviour. If Charlie refuses to admit his delegation in the way of delivering fake messages $|\varphi\rangle^{\text{fake}}_{M'} \neq |\varphi\rangle_{M'}$ to Trent before the verifying process, it can be found at Step 2 in the verifying phase. Specifically, Trent compares $|\varphi\rangle^{\text{fake}}_{M'}$ with $|\varphi\rangle^{\text{out}}_{M'}$ derived from S and $|\varphi\rangle_{M''}$, and reaches $|\varphi\rangle^{\text{fake}}_{M'} \neq |\varphi\rangle^{\text{out}}_{M'}$. If Charlie desires to replace $|\varphi\rangle^{\text{out}}_{M'}$ to disturb Trent's verification, he must get hold of both U_k^{-t} and K_{BT} to accomplish the modifications of S and $|\varphi\rangle_{M''}$ without being caught, which is obviously impossible. Consequently, Charlie cannot disavow his delegation successfully.

3.2. Impossibility of Forgeries

In proxy signature scheme, the impossibility of forgery involves that the original signer Charlie and the verifier Bob cannot forge the proxy signer Alice's signature.

In case Charlie is dishonest and he expects to counterfeit Alice's signature based on the original messages $|\varphi\rangle_{M'}$ held in his hand, he needs to obtain the random sequence S to accomplish the package and the key K_{AT} to carry out the signature, where S is randomly chosen by Alice and K_{AT} is produced via QKD system with perfect security. Thus, Charlie has no ability to forge the signature successfully in the manner of obtaining the keys including S. Take a step back, if Charlie produces a random sequence S' with the same n-length of S, the successful possibility is only $\frac{1}{2^n}$ because the probability for each bit is $\frac{1}{2}$, which can be easily simulated via Matlab and shown in Figure 6, where P_n represents the successful probability for creating the same sequence as S. It can be seen that P_n shows an exponential decline and approaches to zero rapidly as n increases. Furthermore, even if Charlie happens to get the correct sequence S (as we know it has very low probability), K_{AT} is still unknown for Charlie, which is the crucial element for the creation of the signature $|S_A\rangle$. Hence Charlie cannot execute a successful forgery of Alice's signature.

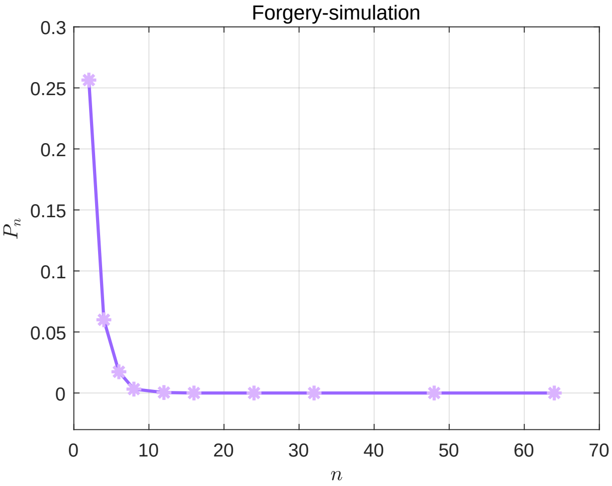


Figure 6. Successful probability P_n for forging the random binary sequence S as a function of the length n of the sequence S.

In case Bob is dishonest and he attempts to counterfeit the signature $|S_A\rangle = E'_{K_{AT}}(|\varphi\rangle_{M''})$, for this purpose, Bob needs to obtain Alice's secret key K_{AT} produced by QKD system. According to the public quantum states including $|S_A\rangle$ and $|\phi_T\rangle$ separately received from Alice and Trent, he cannot acquire any information about K_{AT}. Consequently, Bob cannot forge Alice's signature $|S_A\rangle$ by the method of obtaining K_{AT}. In the QOTP-based quantum signature schemes [35,52], there exists one method for Bob to implement the forgery by the following manner. As the communication receiver, Bob is assumed to hold a valid message-signature pair $(|\varphi\rangle, |S\rangle)$. Then Bob can perform the same unitary operators U_i on each qubit in $|\varphi'\rangle$ and the corresponding qubits in $|S'\rangle$ owing to the encryption manner of qubit by qubit in QOTP algorithm, and he may achieve a new valid message-signature pair without the need for K_{AT}. Based on this, Bob can select his favorable message to perform the forgery attack and claim that it is completed by Alice. In this scenario, when Bob deliberately declares a dispute and lets Trent judge, Trent will stand on the side of Bob. As for this attack strategy, two aspects should be stated. On one hand, Bob cannot choose the preferred message for his own in that the original message $|\varphi\rangle_{M'}$ exists in the form of ciphertext $|\varphi\rangle_{M''}$ via random sequence S. On the other hand, we employ an improved QOTP by introducing assistant CNOT operations to generate the signature, which makes it difficult to find the correct qubit position and modify it due to the correlations among qubits in the signature. In the worse case, we assume that Bob obtains the correct sequence S by some method. If Bob attempts to modify the qubit $|\varphi_j\rangle_{M'}$ at some certain position in $|\varphi\rangle_{M'}$ to forge a valid proxy signature, he can recover $|\varphi\rangle_{M'}$ based on S and determine the position of $|\varphi_j\rangle_{M'}$. Next Bob implements U_{Bob} on $|\varphi_j\rangle_{M'}$ and packages the altered $|\varphi\rangle_{M'}$ with S to get a new $|\varphi'\rangle_{M''}$, in which $|\varphi'_j\rangle_{M''}$ can be expressed as

$$|\varphi'_j\rangle_{M''} = |\varphi_j\rangle_{M'} \otimes U_j \otimes U_{\text{Bob}}. \tag{33}$$

Subsequently Bob implements the same operation U_{Bob} at the corresponding position in $|S_A\rangle$ and acquires

$$|S'_A\rangle_j = |S_A\rangle_j \otimes U_{\text{Bob}} = |\varphi'_j\rangle_{M''} \otimes (\sigma_x)^{K^j_{AT}} \otimes (\sigma_z)^{K^{j+1}_{AT}} \otimes (\sigma_x)^{K^{j+2}_{AT} \cdot |S_A\rangle_{j-1}}. \tag{34}$$

At this moment, a new pair of message-signature $(|\varphi'\rangle_{M''}, |S'_A\rangle)$ is achieved. Meanwhile, the qubit $|S'_A\rangle_{j+1}$ is modified unexpectedly as follows,

$$|S'_A\rangle_{j+1} = |\varphi_{j+1}\rangle_{M''} \otimes (\sigma_x)^{K^{j+1}_{AT}} \otimes (\sigma_z)^{K^{j+2}_{AT}} \otimes (\sigma_x)^{K^{j+3}_{AT} \cdot |S'_A\rangle_j}. \tag{35}$$

Normally $|S'_A\rangle_{j+1}$ should be consistent with $|S_A\rangle_{j+1}$,

$$|S_A\rangle_{j+1} = |\varphi_{j+1}\rangle_{M''} \otimes (\sigma_x)^{K^{j+1}_{AT}} \otimes (\sigma_z)^{K^{j+2}_{AT}} \otimes (\sigma_x)^{K^{j+3}_{AT} \cdot |S_A\rangle_j}. \tag{36}$$

The difference between $|S_A\rangle_{j+1}$ and $|S'_A\rangle_{j+1}$ is attributed to $|S'_A\rangle_j$, which is associated with the next qubit in $|S_A\rangle$ due to the introduction of CNOT gate. Therefore, Bob cannot perform a valid or successful forgery for Alice's signature.

3.3. Impossibility of Repudiations

From a practical point of view, the verifier Bob cannot repudiate his received signature $|S_A\rangle$ from the proxy signer Alice, which can be proved in our presented proxy signature scheme. Normally, in the verifying phase, Bob encodes both $|S_A\rangle$ and $|\varphi\rangle_{M''}$ acquired from Alice with K_{BT} to obtain $|\phi_B\rangle = E'_{K_{BT}}(|S_A\rangle, |\varphi\rangle_{M''})$ and delivers it to Trent, where K_{BT} is guaranteed to be unconditionally safe via QKD protocol and cannot be accessed by others except for Bob and Trent. Then Trent can testify that $|\phi_B\rangle$ contains K_{BT} and get $|S_A\rangle$ and $|\varphi\rangle_{M''}$ to perform the comparison, which implies Bob has obtained $|S_A\rangle$. Actually, the random sequence S is a part of Alice's signature and is announced by public channel which is not obstructed and it is resistant to the modification of messages. As a result, Bob may disavow the integrality of the received signature $(|S_A\rangle, S)$. For example, Bob may claim $|\varphi\rangle_{M''} \neq |\varphi\rangle^{\text{out}}_{M''}$ under the fact of $|\varphi\rangle_{M''} = |\varphi\rangle^{\text{out}}_{M''}$ maliciously and consequently refuses to accept it. Nevertheless, as the communication receiver, Bob's intention is to decode the original message M. If Bob declares $|\varphi\rangle_{M''} \neq |\varphi\rangle^{\text{out}}_{M''}$ under the condition of $|\varphi\rangle_{M''} = |\varphi\rangle^{\text{out}}_{M''}$, he cannot get the random sequence S to yield $|\varphi\rangle_{M'}$, from which the final original message M can be decoded. So this repudiation attack is impossible. In short, Bob cannot disavow the reception and the integrality of Alice's proxy signature $(|S_A\rangle, S)$.

4. Discussions

4.1. Discussion of Complexity

In the above-described quantum proxy signature scheme, the complexity of the scheme attributes to the employed signing and verifying algorithms, which involve two encryption processes including the random sequence-based encryption algorithm and the QOTP-CNOT algorithm. In the former, a randomly produced binary sequence S with n bits is applied to encode the original message $|\varphi\rangle_{M'}$ with the same length into $|\varphi\rangle_{M''}$. Its execution requires n unitary operations U_i (i.e., Pauli operator, I, σ_x, σ_y, σ_z), which can be seen from Figure 3 and Table 2. In terms of key consumption, for encrypting an n-qubit message sequence, an n-length random binary sequence is enough due to the circular use, which differs from the QOTP encryption algorithm with $2n$ bits required [48]. Therefore, our scheme saves the length of the keys and the corresponding storage space. In the language of mathematics and computer, the time complexity and the space complexity of the random sequence-based encryption algorithm both are proportional to n. In the latter, i.e., the QOTP-CNOT algorithm, the secret key K_{AT} with n qubits produced by QKD system is needed and the encryption operations (i.e., σ_x, σ_z and CNOT) are controlled by the key bits in K_{AT}, i.e., $(K^i_{AT}, K^{i+1}_{AT}, K^{i+2}_{AT})$ $(i = 1, 2, \ldots, n)$, as shown in Equation (23). This algorithm is used to encrypt $|\varphi\rangle_{M''}$ derived from the original message $|\varphi\rangle_{M'}$ with the random sequence S and then generate the quantum proxy signature state $|S_A\rangle$. For encrypting an n-qubit message sequence $|\varphi\rangle_{M''}$, the maximum number of the involved unitary operations is $3n$ with the case of full 1 in K_{AT} according to the encryption rules in the QOTP-CNOT operation, which is linear with n. Similarly, the secret key K_{AT} is also used circularly and hence the key length is reduced by three times, which improves the utility efficiency of the key when compared with the QOTP-based signature schemes [31,33]. As a consequence, the time complexity and the space complexity of the proposed scheme are linear with n.

4.2. Discussion of Applications

At present, many researchers have developed various quantum signature protocols designed for special application scenarios, such as electronic payment, electronic voting, electronic commerce, electronic government, and so on [53–57]. Here, we discuss about the possible application of our presented proxy signature scheme in electronic payment as follows. Assume that Charlie is a customer who prefers shopping on the Internet, that Bob is the owner of an online shop, that Alice corresponds to electronic commerce platform and that Trent denotes bank. (i) If Charlie wants to purchase something, which is listed in Bob's store, he will add the merchandise into his fictitious shopping trolley and then submit the order form on the platform (Alice). (ii) Alice will pay for the bill using the credit card which Charlie binds with his account in advance. (iii) Alice handles with the information about Charlie's identification and his order form, and with that she sends the processed Charlie's identification information and the order form to Bob. During the three steps above, the bank Trent plays the role of supervisor, who publishes the credit card used for Charlie's consumption and guarantees the authorities and benefits of every participant. This trade process can be illustrated in Figure 7. Please note that we should consider more potential risks such as untrusted nodes and bounded [58] or more generally noisy-storage model [59] when the involved situations in the cryptography protocols are generalized to realize the network [60] in the future study .

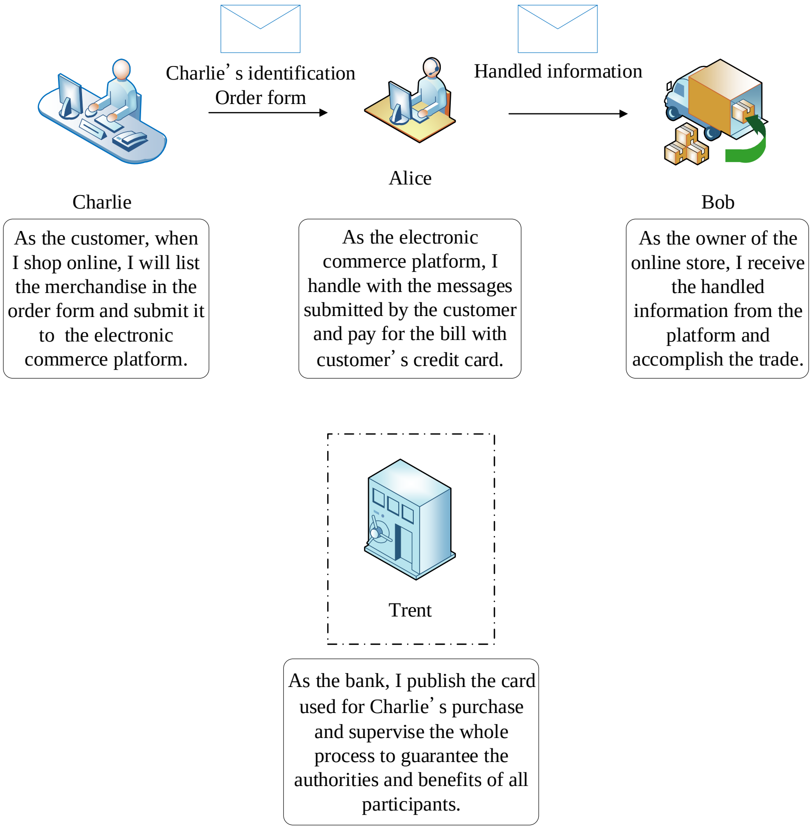

Charlie' s identification
Order form
Handled information
Charlie
Alice
Bob
As the customer, when I shop online, I will list the merchandise in the order form and submit it to the electronic commerce platform.
As the electronic commerce platform, I handle with the messages submitted by the customer and pay for the bill with customer' s credit card.
As the owner of the online store, I receive the handled information from the platform and accomplish the trade.
Trent
As the bank, I publish the card used for Charlie' s purchase and supervise the whole process to guarantee the authorities and benefits of all participants.

Figure 7. Application scene of our presented proxy signature scheme in electronic payment.

5. Conclusions

We presented a quantum proxy signature scheme with QOTP-CNOT operation and quantum walk-based teleportation by making full use of quantum walks on circles. Teleportation based on quantum walks on circles with 4 vertices is employed for the transmission of the encrypted message copy $|\varphi\rangle_{M''}$ from Alice to Bob, which helps Bob to verify the consistency of $|\varphi\rangle_{M''}$. This teleportation can avoid the preparation of the required entanglement resource ahead, which can be produced via quantum walks. Quantum walks on circles are applied to transmit the random sequence S to verify the validity of the proxy warranty. The QOTP-CNOT operation is used to generate the proxy signature and it is designed by introducing the CNOT operation into the QOTP and the CNOT operation breaks the encryption manner of qubit by qubit, which makes multiple qubits interrelated. Security analysis indicates that our proposed scheme has the properties of impossibility of denial, impossibility of forgery and impossibility of repudiation attributing to the deployments of quantum walks on circles, QOTP-CNOT operation, random sequence along with public channel and QKD technologies. Discussion shows that the complexity of the algorithm is linear with the number n of qubits to be encrypted and the possible applications in electronic payment or electronic commerce. In the future, we can explore more applications of realizable quantum computing models such as quantum walks into quantum communication.

Author Contributions: Conceptualization, Y.F. and Q.Z.; methodology, Y.F., Q.Z. and J.S.; software, Q.Z. and S.C.; validation, Y.F., Q.Z. and J.S.; writing—original draft preparation, Y.F. and Q.Z.; writing—review and editing, J.S. and R.S.; supervision, R.S. All authors have read and agreed to the published version of the manuscript.

Funding: The research was funded by [the National Natural Science Foundation of China] grant numbers [61972418], [61872390] and [61871407], [the Natural Science Foundation of Hunan Province] grant number [2020JJ4750] and [the Training Program for Excellent Young Innovators of Changsha] grant number [kq1905058].

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

References

1. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
2. Grover, L.K. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.* **1997**, *79*, 325–328. [CrossRef]
3. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
4. Busch, P.; Heinonen, T.; Lahti, P. Heisenberg's Uncertainty Principle. *Phys. Rep.* **2007**, *452*, 155–176. [CrossRef]
5. Wang, Y.; Shang, Y.; Xue, P. Generalized teleportation by quantum walks. *Quantum Inf. Process.* **2017**, *16*, 221. [CrossRef]
6. Shang, Y.; Wang, Y.; Li, M.; Lu, R.Q. Quantum communication protocols by quantum walks with two coins. *Europhys. Lett.* **2018**, *124*, 60009. [CrossRef]
7. Shang, Y.; Li, M. Experimental realization of state transfer by quantum walks with two coins. *Quantum Sci. Technol.* **2020**, *5*, 015005. [CrossRef]
8. Chatterjee, Y.; Devrari, V.; Behera, B.K.; Panigrahi, P.K. Experimental realization of quantum teleportation using coined quantum walks. *Quantum Inf. Process.* **2020**, *19*, 31. [CrossRef]
9. Li, H.J.; Chen, X.B.; Wang, Y.L.; Hou, Y.Y.; Li, J. A new kind of flexible quantum teleportation of an arbitrary multi-qubit state by multi-walker quantum walks. *Quantum Inf. Process.* **2019**, *18*, 266. [CrossRef]
10. Vlachou, C.; Krawec, W.; Mateus, P.; Paunkovic, N.; Souto, A. Quantum key distribution with quantum walks. *Quantum Inf. Process.* **2018**, *17*, 288. [CrossRef]
11. 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]
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. Feng, Y.; Shi, R.; Shi, J.; Guo, Y. Arbitrated quantum signature scheme based on quantum walks. *Aata Phys. Sin.* **2019**, *68*, 120302. [CrossRef]
14. Feng, Y.; Shi, R.; Shi, J.; Zhao, W.; Lu, Y.; Tang, Y. Arbitrated quantum signature protocol with boson sampling-based random unitary encryption. *J. Phys. A Math. Theor.* **2020**, *53*, 135301. [CrossRef]
15. Li, X.Y.; Chang, Y.; Zhang, S.B.; Dai, J.Q.; Zheng, T. Quantum Blind Signature Scheme Based on Quantum Walk. *Int. J. Theor. Phys.* **2020**, *59*, 2059–2073. [CrossRef]
16. Di, T.; Hillery, M.; Zubairy, M.S. Cavity QED-based quantum walk. *Phys. Rev. A* **2004**, *70*, 032304. [CrossRef]
17. Eckert, K.; Mompart, J.; Birkl, G.; Lewenstein, M. One-and two-dimensional quantum walks in arrays of optical traps. *Phys. Rev. A* **2005**, *72*, 012327. [CrossRef]
18. Zou, X.; Dong, Y.; Guo, G. Optical implementation of one-dimensional quantum random walks using orbital angular momentum of a single photon. *New J. Phys.* **2006**, *8*, 81. [CrossRef]
19. Du, J.; Li, H.; Xu, X.; Shi, M.; Wu, J.; Zhou, X.; Han, R. Experimental implementation of the quantum random-walk algorithm. *Phys. Rev. A* **2003**, *67*, 042316. [CrossRef]
20. Tang, H.; Lin, X.F.; Feng, Z.; Chen, J.Y.; Gao, J.; Sun, K.; Wang, C.Y.; Lai, P.C.; Xu, X.Y.; Wang, Y.; et al. Experimental two-dimensional quantum walk on a photonic chip. *Sci. Adv.* **2018**, *4*, eaat3174. [CrossRef]
21. Bian, Z.H.; Li, J.; Zhan, X.; Twamley, J.; Xue, P. Experimental implementation of a quantum walk on a circle with single photons. *Phys. Rev. A* **2017**, *95*, 052338. [CrossRef]
22. Mambo, M.; Usuda, K.; Okamoto, E. Proxy signatures: Delegation of the power to sign messages. *IEICE Trans. Fund. Electron.* **1996**, *79*, 1338–1354.
23. Gottesman, D.; Chuang, I. Quantum Digital Signatures. *arXiv* **2001**, arXiv:quant-ph/0105032v2.
24. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]
25. Chang, Z.L.; Zhou, J.X.; Zhang, J.; Wen, Q.Y. Quantum proxy signature scheme based on EPR state. *Appl. Res. Comput.* **2010**, *27*, 675–677.
26. Zhou, J.; Zhou, Y.; Niu, X.; Yang, Y. Quantum proxy signature scheme with public verifiability. *Sci. China Phys. Mech.* **2011**, *54*, 1828–1832. [CrossRef]
27. Cao, H.J.; Zhu, Y.Y.; Li, P.F. A Quantum Proxy Weak Blind Signature Scheme. *Int. J. Theor. Phys.* **2014**, *53*, 419–425. [CrossRef]
28. Zhang, K.J.; Jia, H.Y. Cryptanalysis of a Quantum Proxy Weak Blind Signature Scheme. *Int. J. Theor. Phys.* **2015**, *54*, 582–588. [CrossRef]

29. Cao, H.J.; Yu, Y.F.; Song, Q.; Gao, L.X. A Quantum Proxy Weak Blind Signature Scheme Based on Controlled Quantum Teleportation. *Int. J. Theor. Phys.* **2015**, *54*, 1325–1333. [CrossRef]
30. Xu, G.B. Novel Quantum Proxy Signature without Entanglement. *Int. J. Theor. Phys.* **2015**, *54*, 2605–2612. [CrossRef]
31. 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]
32. Qin, H.; Tang, W.K.; Tso, R. Batch quantum multi-proxy signature. *Opt. Quantum Electron.* **2018**, *50*, 450.1–450.8. [CrossRef]
33. Niu, X.F.; Ma, W.P.; Chen, B.Q.; Liu, G.; Wang, Q.Z. A Quantum Proxy Blind Signature Scheme Based on Superdense Coding. *Int. J. Theor. Phys.* **2020**, *59*, 1121–1128. [CrossRef]
34. Zou, X.; Qiu, D. Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A* **2010**, *82*, 042325. [CrossRef]
35. 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]
36. Aharonov, Y.; Davidovich, L.; Zagury, N. Quantum random walks. *Phys. Rev. A* **1993**, *48*, 1687–1690. [CrossRef]
37. Ambainis, A.; Bach, E.; Nayak, A.; Vishwanath, A.; Watrous, J. One-dimensional quantum walks. In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing (STOC01), Hersonissos, Crete, Greece, 6–8 July 2001; pp. 37–49.
38. Aharonov, D.; Ambainis, A.; Kempe, J.; Vazirani, U. Quantum walks on graphs. In Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing (STOC01), Hersonissos, Crete, Greece, 6–8 July 2001; pp. 50–59.
39. Meyer, D.A. From quantum cellular automata to quantum lattice gases. *J. Stat. Phys.* **1996**, *85*, 551–574. [CrossRef]
40. Farhi, E.; Gutmann, S. Quantum computation and decision trees. *Phys. Rev. A* **1998**, *58*, 915. [CrossRef]
41. Jozef, K. Two models of quantum random walk. *Cent. Eur. J. Phys.* **2003**, *1*, 556–573.
42. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **2011**, *84*, 062317. [CrossRef]
43. Zhang, Z.Y.; Shi, R.H.; Guo, Y. Multipartite continuous variable quantum communication with entanglement in the middle. *J. Phys. A Math. Theor.* **2018**, *51*, 295301. [CrossRef]
44. Zhang, Z.; Shi, R.; Zeng, G.; Guo, Y. Coherent attacking continuous-variable quantum key distribution with entanglement in the middle. *Quantum Inf. Process.* **2018**, *17*, 133. [CrossRef]
45. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
46. Inamori, H.; Lutkenhaus, N.; Mayers, D. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D* **2007**, *41*, 599–627. [CrossRef]
47. Leung, D.W. Quantum Vernam Cipher. *Quantum Inf. Comput.* **2001**, *2*, 14.
48. Boykin, P.O.; Roychowdhury, V. Optimal encryption of quantum bits. *Phys. Rev. A* **2003**, *67*, 042317. [CrossRef]
49. 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]
50. Zhang, L.; Sun, H.W.; Zhang, K.J.; Jia, H.Y. An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. *Quantum Inf. Process.* **2017**, *16*, 70. [CrossRef]
51. Buhrman, H.; Cleve, R.; Watrous, J.; De Wolf, R. Quantum fingerprinting. *Phys. Rev. Lett.* **2001**, *87*, 167902. [CrossRef]
52. 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]
53. Wen, X.J.; Nie, Z. An E-payment system based on quantum blind and group signature. *Phys. Scr.* **2010**, *82*, 5468–5478.
54. Wen, X.J.; Chen, Y.Z.; Fang, J.B. An inter-bank E-payment protocol based on quantum proxy blind signature. *Quantum. Inf. Process.* **2013**, *12*, 549–558. [CrossRef]
55. Tian, J.H.; Zhang, J.Z.; Li, Y.P. A voting protocol based on the controlled quantum operation teleportation. *Int. J. Theor. Phys.* **2016**, *55*, 2303–2310. [CrossRef]

56. Cao, H.J.; Ding, L.Y.; Yu, Y.F.; Li, P.F. A Electronic Voting Scheme Achieved by Using Quantum Proxy Signature. *Int. J. Theor. Phys.* **2016**, *55*, 4081–4088. [CrossRef]
57. Shao, A.X.; Zhang, J.Z.; Xie, S.C. An E-payment Protocol Based on Quantum Multi-proxy Blind Signature. *Int. J. Theor. Phys.* **2017**, *56*, 1241–1248. [CrossRef]
58. Damgård, I.B.; Fehr, S.; Salvail, L.; Schaffner, C. Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.* **2008**, *37*, 1865–1890. [CrossRef]
59. Wehner, S.; Schaffner, C.; Terhal, B.M. Cryptography from noisy storage. *Phys. Rev. Lett.* **2008**, *100*, 220502. [CrossRef]
60. Wehner, S.; Elkouss, D.; Hanson, R. Quantum internet: A vision for the road ahead. *Science* **2018**, *362*, eaam9288. [CrossRef]