entropy

MDPI

Article

A Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation

Dianjun Lu [1,2], Zhihui Li [1,*], Jing Yu [1] and Zhaowei Han [1]

[1] School of Mathematics and Statistics, Shaanxi Normal University, Xi'an 710119, China; ldj@qhnu.edu.cn (D.L.); 2008011@qhnu.edu.cn (J.Y.); hanzw888@snnu.edu.cn (Z.H.)
[2] School of Mathematics and Statistics, Qinghai Normal University, Xining 810008, China
* Correspondence: lizhihui@snnu.edu.cn

Abstract: In this paper, we present a verifiable arbitrated quantum signature scheme based on controlled quantum teleportation. The five-qubit entangled state functions as a quantum channel. The proposed scheme uses mutually unbiased bases particles as decoy particles and performs unitary operations on these decoy particles, applying the functional values of symmetric bivariate polynomial. As such, eavesdropping detection and identity authentication can both be executed. The security analysis shows that our scheme can neither be disavowed by the signatory nor denied by the verifier, and it cannot be forged by any malicious attacker.

Keywords: arbitrated quantum signature; controlled quantum teleportation; von Neumann measurement; Bell measurement; verifiability

Citation: Lu, D.; Li, Z.; Yu, J.; Han, Z. A Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation. *Entropy* **2022**, *24*, 111. https://doi.org/10.3390/e24010111

Academic Editors: Leong Chuan Kwek, Xiang-Bin Wang and Cong Jiang

Received: 16 December 2021
Accepted: 9 January 2022
Published: 11 January 2022

1. Introduction

Since Bennett and Brassard [1] proposed the quantum key distribution (QKD) protocol in 1984, quantum cryptography has attracted extensive attention. Its security is guaranteed by the principles of quantum mechanics such as the Heisenberg uncertainty principle and the quantum no-cloning theorem. Quantum cryptography can provide the advantage of unconditional security, making the research of quantum cryptography increasingly important. Many important quantum cryptography branches have been developed, such as quantum key distribution [2,3], quantum signature (QS) [4–6], quantum teleportation (QT) [7], quantum authentication [8], and deterministic secure quantum communication [9].

Quantum signatures can be applied to verify the identity of the sender and the integrity of the information. The arbitrated quantum signature (AQS), providing many merits, has attracted much attention. In 2002, Zeng et al. [10] proposed the first arbitrated quantum signature scheme using the Green–Horne–Zeilinger (GHZ) state and the quantum one-time pad (QOTP). Based on the design of the classical arbitrated digital signature, the scheme provides a re-verification service for signatory and receiver using the online signature provided by a trusted third party arbitrator. In 2008, Curty and Lutkenhaus [11] investigated the scheme [10], and they claimed that it was not clearly described and that the safety analysis was incorrect. In response to the controversy of Curty et al., Zeng et al. [12] proved the scheme [10] in more detail. In 2009, to reduce the complexity and improve the efficiency of the protocol [10], Li et al. [13] proposed an AQS scheme based on the Bell states rather than the GHZ states and proved its advantages in terms of transmission efficiency and low complexity. Unfortunately, in 2010, Zou and Qiu [14] argued that Li's AQS scheme can be disavowed by the receiver, and they proposed an AQS protocol that uses bulletin boards and other security schemes that do not use entangled state. Their scheme further simplified the protocol of Li et al., and an improved AQS scheme was designed using single particles that can resist the denunciation of the receiver, thus reducing the difficulty of the physical implementation of AQS. However, in 2011, Gao et al. [15] conducted the first comprehensive cryptanalysis of previous AQS schemes in terms of forgery and disavowal.

They found that the existing AQS schemes based on QOTP encryption [13,14] all have some security problems. In other words, the receiver Bob can realize the existence of the forgery of a signature under the known message attack, while the sender Alice can successfully disavow any signature of hers through a simple attack. Choi et al. [16] found that most AQS protocols can be cracked through a specific existential forgery attack due to the careless taking advantage of the optimal quantum one-time pad based on Pauli operators. To overcome this weakness, they proposed a simple method to ensure the security of the signature. As Choi et al.proved, Bob could not simultaneously forge both the information and the signature to be verified by an arbitrator in the event of a dispute. In the same year, Yang et al. [17] demonstrated how to construct an arbitrated quantum signature protocol for classical messages using untrusted arbitrators. In order to solve the security problems experienced with the AQS protocol, Zhang et al. [18] analyzed the existing security problems [15,16] in 2013 and suggested some corresponding improvement strategies to counter forgery attacks. In order to solve the problem proposed by Gao et al. [15], Liu et al. [19] designed a new QOTP algorithm in 2014, which mainly relies on inserting decoy states into fixed positions, and constructed an unconditionally secure AQS scheme with fast signing and verifying using only a single particle state. In 2015, Li [20] used chained CNOT operation for encryption, instead of quantum one-time pad, to ensure the security of the protocol. To improve the efficiency of quantum bit to 100%, Yang [21] proposed an AQS scheme with the cluster state in 2016. In 2017, in order to resist forgery attacks and disavowal attacks, Zhang et al. [22] proposed a new quantum encryption based on the key-controlled chained CNOT operations (KCCC encryption), and through KCCC encryption, constructed an improved arbitrated quantum signature protocol. In 2016, Yang et al. [23] also proposed a theoretically extensible quantum digital signature with a star-like cluster state. In 2018, Shi et al. [24] proposed an arbitrated quantum signature scheme with the Hamiltonian algorithm based on blind quantum computation. Due to the application of blind quantum computation, it is not necessary to recover the original message during verification, which can improve the simplicity and operability of AQS. In the same year, Feng et al. [25] constructed an AQS scheme based on continuous variable squeezed vacuum states rather than coherent states to further improve coding efficiency and performance. In 2019, Feng et al. [26] proposed an AQS scheme with quantum walk-based teleportation, which does not require the preparation of entangled particles in advance, making the AQS protocol more flexible and practical. In 2020, Chen et al. [27] proposed an offline arbitrated semi-quantum signature scheme based on four-particle cluster states, in which the classical parties can sign with the assistance of a quantum arbitrator. Different from the typical arbitrated quantum signature schemes, the arbitrator in this protocol acts as a relay station of signature transmission and no longer interferes with the direct authentication of the signature, so that the signature receiver has completed authentication rights. There is no additional direct communication between the signatory and the receiver, which reduces the complexity of transmission. However, the above AQS scheme does not consider authentication between signatory, arbitrator, and verifier.

Quantum teleportation is a technology that uses the entangled state or cluster state to transmit information between two sides of communication. The first scheme of quantum teleportation was proposed by Bennett et al. [28] in 1993. It is a scheme of teleportation through classical channel and an EPR entangled channel. In 1998, Karlsson and Bourennane [29] proposed controlled quantum teleportation. Its basic idea is that the receiver reconstructs the unknown quantum state with the help of the controller. Until now, quantum teleportation has been studied using the GHZ states [30], W. states [31,32], cluster states [33], and other entangled states as quantum channels. In recent years, many quantum signature schemes have used entangled states as quantum channels, and methods were proposed to transmit unknown quantum states of a single particle [34] or double particles [35]. In 2005, Brown et al. [36] developed a computationally feasible entanglement measurement method based on negative bias transposition criterion, and found highly entangled four-qubit states and five-qubit states by searching. In 2008, Muralidharan and Panigrahi [37] investigated the

usefulness of the five-qubit state introduced by Brown et al. [36] for quantum information applications such as quantum teleportation. The results show that this state can be used for perfect teleportation of arbitrary single- and two-qubit systems.

In this paper, we construct an arbitrated quantum signature scheme that can verify the identity of participants using five-qubit entangled states as quantum channels and controlled quantum teleportation. The security analysis result shows that our AQS scheme ensures that the signatory Alice cannot disavow, the verifier Bob cannot repudiate, and any illegal attacker can not forge. The proposed scheme uses mutually unbiased bases particles as decoy particles. It applies a pair of function values of symmetric binary polynomials to perform a unitary operation on decoy particles so that eavesdropping detection and identity verification between participants can be performed. In addition, the scheme only needs von Neumann measurement, Bell measurement, and a unitary operation to recover the single-particle qubit state. It replicates message from the signatory Alice to the verifier Bob, which is an attractive advantage for realizing an actual quantum communication network.

The scheme has the following advantages:

(1) The mutually unbiased bases particles are used as decoy particles to prevent external adversaries from eavesdropping during transmission;
(2) The receiver only needs to ask about the position of the decoy particles without asking what the measurement bases are in the process of eavesdropping detection;
(3) The scheme provides the function of identity authentication among participants. It uses a pair of function values of symmetric binary polynomials as parameters of the unitary operation, which is used to act on the decoy particles to verify the identity of participants.

The rest of this article are organized as follows. In Section 2, the concepts of the arbitrated quantum signature, mutually unbiased bases and controlled quantum teleportation are introduced. In Section 3, the detailed process of the proposed protocol is described. In Sections 4 and 5, the verifiability analysis and safety analysis are conducted, respectively. Finally, a brief conclusion is provided in Section 6.

2. Preliminaries

In this section, we first briefly review some notions concerning the arbitrated quantum signature scheme and the definition of mutually unbiased bases, which is presented in [38]. Then, we introduce controlled quantum teleportation, which is used in constructing the arbitrated quantum signature scheme. Finally, an example of controlled quantum teleportation is given.

2.1. Some Notions Concerning the Arbitrated Quantum Signature

A digital signature scheme is a cryptographic primitive that provides the receiver of a message with assurance about the integrity of the data, and the identity of the sender/signatory. Furthermore, it offers unforgeable and undeniable property. Similarly, the arbitrated signature scheme is a digital signature scheme finished with the help of an arbitrator, who is a disinterested third party trusted to complete a protocol. Here "trusted" means that all people involved in the protocol accept what he says as true and what he does as correct, as well as that he will complete his part of the protocol [14]. The quantum signature is a quantum version of the classical digital signature.

2.2. Mutually Unbiased Bases

Definition 1 ([38]). *We suppose that* $A_1 = \{|\varphi_i\rangle\}^q{}_{i=1}$ *and* $A_2 = \{|\psi_i\rangle\}^q{}_{i=1}$ *are two sets of standard orthogonal bases, which are defined over a q-dimensional complex space* C^q*. We state that* A_1 *and* A_2 *are mutually unbiased if the following relationship is satisfied:* $|\langle\varphi_i|\psi_j\rangle| = \frac{1}{\sqrt{q}}$.

If any two sets of standard orthogonal bases $A_1, A_2, \cdots, A_m$ in space C^q is unbiased, then this set is called an unbiased bases set. Additionally, one can find at most $q+1$

mutually unbiased bases if q is an odd prime number. In particular, the computation basis is expressed as $\{|k\rangle|k \in D\}$, where $D = \{0, 1, ..., q-1\}$. In addition to the computation basis, the remaining q groups of unbiased bases can be expressed as $|\varphi_l^{(j)}\rangle = \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} \omega^{k(l+jk)} |k\rangle$, where $\omega = e^{\frac{2\pi i}{q}}$ and $j \in D$ represent the number of the mutually unbiased bases and $l \in D$ list the number of vectors for the given bases. For $j \neq j'$ these mutually unbiased bases satisfy the following conditions: $|\langle \varphi_l{}^{(j)} | \varphi_l{}^{(j')} \rangle| = \frac{1}{\sqrt{q}}$.

Letting $X_q = \sum_{n=0}^{q-1} \omega^n |n\rangle\langle n|$, we have following operations:

$$X_q{}^x |\varphi_l{}^{(j)}\rangle = X_q{}^x \tfrac{1}{\sqrt{q}} \textstyle\sum_{k=0}^{q-1} \omega^{k(l+jk)} |k\rangle$$

$$= \tfrac{1}{\sqrt{q}} \left(\textstyle\sum_{n=0}^{q-1} \omega^{xn} |n\rangle\langle n| \right) \left(\textstyle\sum_{k=0}^{q-1} \omega^{k(l+jk)} |k\rangle \right) = \tfrac{1}{\sqrt{q}} \left(\textstyle\sum_{k=0}^{q-1} \omega^{k(l+x)+jk} |k\rangle \right) = |\varphi_{l+x}{}^{(j)}\rangle.$$

For the convenience of expression, $X_q{}^x$ is denoted as U_x which is a unitary operator, that is, $U_x |\varphi_l{}^{(j)}\rangle = |\varphi_{l+x}{}^{(j)}\rangle$. Especially, we have $U_l |\varphi_0{}^{(0)}\rangle = |\varphi_l{}^{(0)}\rangle$.

2.3. Controlled Quantum Teleportation

Our arbitrated quantum signature scheme is based on controlled quantum teleportation. The five-qubit entangled state can be used to perfect the teleportation of arbitrary single- and two-qubit systems [37], which are suitable for maximum contact teleportation and satisfy the biggest task-oriented definition of entangled state [36]. Due to the above advantages, in this section, we use the five-qubit entangled state as the quantum channel to execute controlled quantum teleportation. The design form is as follows:

$$|\xi\rangle_{12345} = \frac{1}{2} \left(|001\rangle|\phi^-\rangle + |010\rangle|\psi^-\rangle + |100\rangle|\phi^+\rangle + |111\rangle|\psi^+\rangle \right)_{12345}.$$

In the form above, $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ represent the four Bell states of two particles, respectively, $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. These states exhibit true multipartite entanglement from both negative bias measurements and von Neumann measurements. Even after tracking one or two qubits from this state, entanglement is maintained in the resulting subsystem, which is therefore highly robust.

In the quantum teleportation process, the participants are Alice, Trent, and Bob. Alice owns particles (M, 2, 3), Trent owns particles (1, 4), and Bob owns the particle (5).

The model of controlled quantum teleportation is shown in Figure 1.

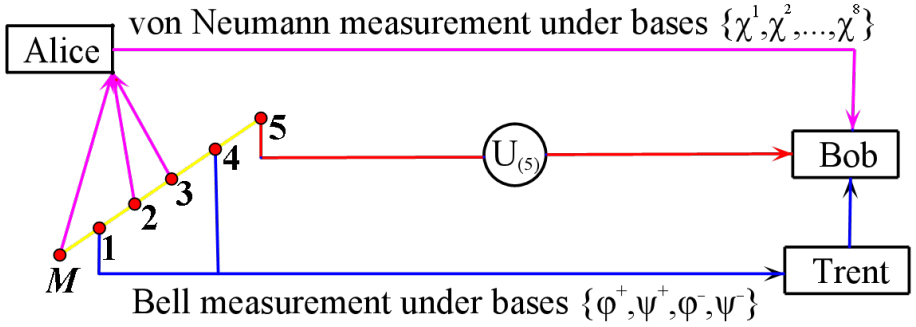

Figure 1. The model of controlled quantum teleportation.

The working process of the controlled quantum teleportation is described below:

Step 1: Alice performs three-particle von Neumann measurements of the particles (M, 2, 3) in her possession. The three-particle von Neumann measurement basis is $\{|\chi^i\rangle\}$ $(i = 1, 2, \cdots, 8)$, as shown in Table 1.

Table 1. The three-particle von Neumann measurement basis.

$\chi^1 = \frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$\chi^2 = \frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$
$\chi^3 = \frac{1}{\sqrt{2}}(\|001\rangle + \|110\rangle)$	$\chi^4 = \frac{1}{\sqrt{2}}(\|001\rangle - \|110\rangle)$
$\chi^5 = \frac{1}{\sqrt{2}}(\|010\rangle + \|101\rangle)$	$\chi^6 = \frac{1}{\sqrt{2}}(\|010\rangle - \|101\rangle)$
$\chi^7 = \frac{1}{\sqrt{2}}(\|100\rangle + \|011\rangle)$	$\chi^8 = \frac{1}{\sqrt{2}}(\|100\rangle - \|011\rangle)$

Suppose Alice carries the information of the quantum state of particle M as $|\gamma\rangle_M = (\alpha|0\rangle + \beta|1\rangle)_M$, where the coefficients α and β are unknown and satisfy $|\alpha|^2 + |\beta|^2 = 1$. The combined state of the entire system $|\Psi\rangle_{M12345}$ consisting of particles M and $(1,2,3,4,5)$ is given by the formula below.

$$\begin{aligned}
|\Psi\rangle_{M12345} &= |\gamma\rangle_M \otimes |\xi\rangle_{12345} = (\alpha|0\rangle + \beta|1\rangle)_M \otimes |\xi\rangle_{12345} \\
&= (\alpha|0\rangle + \beta|1\rangle)_M \otimes \frac{1}{2}\big(|001\rangle|\phi^-\rangle + |010\rangle|\psi^-\rangle + |100\rangle|\phi^+\rangle + |111\rangle|\psi^+\rangle\big)_{12345} \\
&= (\alpha|0\rangle + \beta|1\rangle)_M \otimes \frac{1}{2\sqrt{2}}(|00100\rangle \\
&- |00111\rangle + |01001\rangle - |01010\rangle + |10000\rangle + |10011\rangle + |11101\rangle + |11110\rangle)_{12345} \\
&= \frac{1}{2\sqrt{2}}[\alpha|000100\rangle - \alpha|000111\rangle + \alpha|001001\rangle \\
&- \alpha|001010\rangle + \alpha|010000\rangle + \alpha|010011\rangle + \alpha|011101\rangle + \alpha|011110\rangle \\
&+ \beta|100100\rangle - \beta|100111\rangle + \beta|101001\rangle - \beta|101010\rangle \\
&+ \beta|110000\rangle + \beta|110011\rangle + \beta|111101\rangle + \beta|111110\rangle]_{12345}.
\end{aligned}$$

Step 2: Alice conveys her measurement outcomes to Bob through the classical channel. If Alice uses measurement basis $\{|\chi^i\rangle\}$ $(i = 1, 2, \cdots, 8)$ to measure $|\Psi\rangle_{M12345}$, then $|\Psi\rangle_{M12345}$ will collapse into the corresponding states shown in Table 2.

Table 2. The outcomes of Alice's measuring $|\Psi\rangle_{M12345}$ with measurement basis $\left\{|\chi^i\rangle\right\}$.

$\langle\chi^1_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|100\rangle + \alpha\|111\rangle + \beta\|101\rangle + \beta\|110\rangle)$	$\langle\chi^2_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|100\rangle + \alpha\|111\rangle - \beta\|101\rangle - \beta\|110\rangle)$
$\langle\chi^3_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|000\rangle - \alpha\|011\rangle + \beta\|001\rangle - \beta\|010\rangle)$	$\langle\chi^4_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|000\rangle - \alpha\|011\rangle - \beta\|001\rangle + \beta\|010\rangle)$
$\langle\chi^5_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|001\rangle - \alpha\|010\rangle + \beta\|000\rangle - \beta\|011\rangle)$	$\langle\chi^6_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|001\rangle - \alpha\|010\rangle - \beta\|000\rangle + \beta\|011\rangle)$
$\langle\chi^7_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(\alpha\|101\rangle + \alpha\|110\rangle + \beta\|100\rangle + \beta\|111\rangle)$	$\langle\chi^8_{M23}|\Psi\rangle_{M12345} = \frac{1}{4}(-\alpha\|101\rangle - \alpha\|110\rangle + \beta\|100\rangle + \beta\|111\rangle)$

Step 3: Trent uses Bell measurement basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ to perform two-particle measurements on particles (1,4). After Trent measures $\langle\chi^i_{M23}|\Psi\rangle_{M12345}$ with Bell measurement basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, $\langle\chi^i_{M23}|\Psi\rangle_{M12345}$ collapses to the corresponding state shown in Table 3.

Step 4: Trent sends his measurement results to Bob through the classical channel.

Step 5: Following Trent and Alice's measurements, Bob performs an appropriate unitary operation $U_{(5)}$ and successfully reconstructs the original unknown quantum state $|\gamma\rangle_M$ on the particle (5).

Table 3. Outcomes of Trent's measuring $\langle\chi^i_{M23}|\Psi\rangle_{M12345}$ with Bell measurement basis.

	$\|\phi^+_{14}\rangle$	$\|\phi^-_{14}\rangle$	$\|\psi^+_{14}\rangle$	$\|\psi^-_{14}\rangle$
$\langle\chi^1_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$
$\langle\chi^2_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$
$\langle\chi^3_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$
$\langle\chi^4_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$
$\langle\chi^5_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$
$\langle\chi^6_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$
$\langle\chi^7_{M23}\|\Psi\rangle_{M12345}$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$
$\langle\chi^8_{M23}\|\Psi\rangle_{M12345}$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$

The participants' measurement outcomes and the unitary operation $U_{(5)}$ are shown in Table 4, in which MO represents the measurement outcomes and all the Pauli matrices are shown below.

$$I=\begin{bmatrix}1&0\\0&1\end{bmatrix},\quad \sigma_x=\begin{bmatrix}0&1\\1&0\end{bmatrix},\quad \sigma_y=\begin{bmatrix}0&-i\\i&0\end{bmatrix},\quad \sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix}.$$

Table 4. The relationship between Alice's, Trent's measurement outcomes, and Bob's unitary operation.

Alice' MO	Trent' MO	Bob's State	$U_{(5)}$	Trent' MO	Bob's State	$U_{(5)}$
$\chi^1=\frac{1}{\sqrt{2}}(\|000\rangle+\|111\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\sigma_x)_5$	$\|\psi^+_{14}\rangle$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	I_5
	$\|\phi^-_{14}\rangle$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\sigma_x)_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$-I_5$
$\chi^2=\frac{1}{\sqrt{2}}(\|000\rangle-\|111\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(i\sigma_y)_5$	$\|\psi^+_{14}\rangle$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\sigma_z)_5$
	$\|\phi^-_{14}\rangle$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-i\sigma_y)_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\sigma_z)_5$
$\chi^3=\frac{1}{\sqrt{2}}(\|001\rangle+\|110\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	I_5	$\|\psi^+_{14}\rangle$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\sigma_x)_5$
	$\|\phi^-_{14}\rangle$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	I_5	$\|\psi^-_{14}\rangle$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\sigma_x)_5$
$\chi^4=\frac{1}{\sqrt{2}}(\|001\rangle-\|110\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\sigma_z)_5$	$\|\psi^+_{14}\rangle$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-i\sigma_y)_5$
	$\|\phi^-_{14}\rangle$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\sigma_z)_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-i\sigma_y)_5$
$\chi^5=\frac{1}{\sqrt{2}}(\|010\rangle+\|101\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\sigma_x)_5$	$\|\psi^+_{14}\rangle$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$-I_5$
	$\|\phi^-_{14}\rangle$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\sigma_x)_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$-I_5$
$\chi^6=\frac{1}{\sqrt{2}}(\|010\rangle-\|101\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(i\sigma_y)_5$	$\|\psi^+_{14}\rangle$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\sigma_z)_5$
	$\|\phi^-_{14}\rangle$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(i\sigma_y)_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\sigma_z)_5$
$\chi^7=\frac{1}{\sqrt{2}}(\|100\rangle+\|011\rangle)$	$\|\phi^+_{14}\rangle$	$(\alpha\|0\rangle+\beta\|1\rangle)_5$	I_5	$\|\psi^+_{14}\rangle$	$(\alpha\|1\rangle+\beta\|0\rangle)_5$	$(\sigma_x)_5$
	$\|\phi^-_{14}\rangle$	$(-\alpha\|0\rangle-\beta\|1\rangle)_5$	$-I_5$	$\|\psi^-_{14}\rangle$	$(-\alpha\|1\rangle-\beta\|0\rangle)_5$	$(-\sigma_x)_5$
$\chi^8=\frac{1}{\sqrt{2}}(\|100\rangle-\|011\rangle)$	$\|\phi^+_{14}\rangle$	$(-\alpha\|0\rangle+\beta\|1\rangle)_5$	$(-\sigma_z)_5$	$\|\psi^+_{14}\rangle$	$(-\alpha\|1\rangle+\beta\|0\rangle)_5$	$(-i\sigma_y)_5$
	$\|\phi^-_{14}\rangle$	$(\alpha\|0\rangle-\beta\|1\rangle)_5$	$(\sigma_z)_5$	$\|\psi^-_{14}\rangle$	$(\alpha\|1\rangle-\beta\|0\rangle)_5$	$(i\sigma_y)_5$

Based on Alice and Trent's measurement outcomes, Bod performs the corresponding unitary operation $U_{(5)}$ on particle (5) and his result is $\alpha|0\rangle+\beta|1\rangle$. This is the original information particle state. That is, Alice successfully transmits the unknown quantum state to Bob under Trent's control.

Example 1. *Suppose that the information particle states are* $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\rangle,|0\rangle,|-\rangle,|1\rangle,|1\rangle,|0\rangle\}$. *Alice combines each information particle state and five-particle entangled state into a six-particle state sequence:* $\{|0\rangle\otimes|\xi\rangle_{12345},|1\rangle\otimes|\xi\rangle_{12345},|+\rangle\otimes|\xi\rangle_{12345},|-\rangle\otimes|\xi\rangle_{12345},|+\rangle\otimes|\xi\rangle_{12345},|0\rangle\otimes|\xi\rangle_{12345},|-\rangle\otimes|\xi\rangle_{12345},|1\rangle\otimes|\xi\rangle_{12345},|1\rangle\otimes|\xi\rangle_{12345},|0\rangle\otimes|\xi\rangle_{12345}\}$. *Alice performs von Neumann measurement of the particles (M,2,3) in the sequence. Suppose that von Neumann measurement outcomes are* $\{\chi^1,\chi^5,\chi^7,\chi^2,\chi^8,\chi^3,\chi^4,\chi^4,\chi^8,\chi^6\}$, *and Trent's measurement outcomes of the particles (1,4) in the sequence are* $\{|\phi^+_{14}\rangle,|\phi^-_{14}\rangle,|\psi^+_{14}\rangle,|\psi^-_{14}\rangle,|\phi^+_{14}\rangle,|\psi^+_{14}\rangle,|\psi^-_{14}\rangle,|\phi^-_{14}\rangle,|\psi^+_{14}\rangle,|\psi^-_{14}\rangle\}$. *At this time, the states of all particles (5) should be* $(\alpha|1\rangle+\beta|0\rangle)_5$, $(\alpha|1\rangle+\beta|0\rangle)_5$, $(\alpha|1\rangle+\beta|0\rangle)_5$, $(-\alpha|0\rangle+\beta|1\rangle)_5$, $(-\alpha|0\rangle+\beta|1\rangle)_5$, $(-\alpha|1\rangle-\beta|0\rangle)_5$, $(-\alpha|1\rangle+\beta|0\rangle)_5$, $(\alpha|0\rangle-\beta|1\rangle)_5$, $(-\alpha|1\rangle+\beta|0\rangle)_5$, $(-\alpha|0\rangle+\beta|1\rangle)_5$. *After Bob performs the following unitary operation:* $\{\sigma_x,\sigma_x,\sigma_x,-\sigma_z,-\sigma_z,-\sigma_x,-i\sigma_y,\sigma_z,-i\sigma_y,-\sigma_z\}$, *the states of the information particles are* $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle,|+\rangle,|0\rangle,|-\rangle,|1\rangle,|1\rangle,|0\rangle\}$.

3. The Proposed Verifiable Arbitrated Quantum Signature Scheme

In our scheme, Alice the signatory, Bob the verifier, and Trent the arbitrator are defined as the three participants. The arbitrator Trent should be trusted by both Alice and Bob. The detailed procedures of our scheme can be described as follows.

3.1. Initializing Phase

Step I1: Alice and Trent share secret key K_A and Bob and Trent share secret key K_B. The secret key distribution task can be performed using the QKD protocol, which has been proven to provide unconditional security [39,40].

Step I2: Trent selects a $k-1$-order symmetric binary polynomial: $F(x,y) = a_{00} + a_{10}x + a_{01}y + a_{11}xy + a_{20}x^2 + a_{02}y^2 + a_{12}xy^2 + a_{21}x^2y + a_{22}x^2y^2 + \cdots + a_{k-1,k-1}x^{k-1}y^{k-1} \bmod q$, where q is a prime number, $F(x,y) \in GF(q)[x,y]$, $a_{ij} \in F_q$, $i,j \in \{0,1,\cdots,k-1\}$, $a_{ij} = a_{ji}$, F_q is a finite field. Suppose that the public identity information for the participants Alice, Bob, and Trent is x_A, x_B, x_T. Trent computes two share polynomials $f_A(y) = F(x_A,y)$ and $f_B(y) = F(x_B,y)$. The share polynomial $f_A(y)$ is encrypted as $f_A^{'}(y) = E_{K_A}(f_A(y))$ and $f_A^{'}(y)$ is sent to Alice. The share polynomial $f_B(y)$ is encrypted as $f_B^{'}(y) = E_{K_B}(f_B(y))$ and $f_B^{'}(y)$ is sent to Bob.

Step I3: Alice receives $f_A^{'}(y)$ and decrypts it with secret key K_A to obtain $f_A(y) = F(x_A,y)$. Alice calculates $f_A(x_B) = F(x_A,x_B)$ and $f_A(x_T) = F(x_A,x_T)$ based on Bob's and Trent's public identity information x_B and x_T. Similarly, Bob can calculate $f_B(x_A) = F(x_B,x_A)$ and $f_B(x_T) = F(x_B,x_T)$ based on Alice's and Trent's public identity information x_A and x_T. Due to the symmetry of the binary polynomial, $f_A(x_B) = f_B(x_A)$, $f_A(x_T) = f_T(x_A)$, $f_B(x_T) = f_T(x_B)$.

Step I4: According to the value of $F(x_A,x_B)$ and $F(x_A,x_T)$, Alice executes the unitary operations $U_{F(x_A,x_B)}$ and $U_{F(x_A,x_T)}$ on $|\mu\rangle = |\varphi_0^{(0)}\rangle = \frac{1}{\sqrt{q}}\sum_{i=0}^{q-1}|i\rangle$ to produce enough decoy particles: $|\mu\rangle_{A,B} = U_{F(x_A,x_B)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_B)}^{(0)}\rangle$ and $|\mu\rangle_{A,T} = U_{F(x_A,x_T)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_T)}^{(0)}\rangle$.

The parameter formation process of the initializing phase is shown in Figure 2.

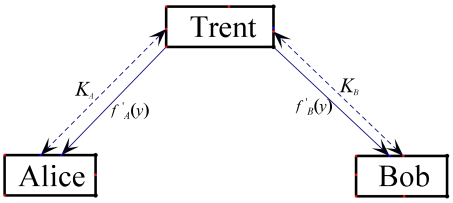

Figure 2. Initializing phase schematic diagram.

3.2. Signing Phase

Step S1: Alice obtains a qubit string $|\Gamma\rangle$ based on the signature information m. Suppose there are n qubits in the information qubit string $|\Gamma\rangle = \{|\gamma_1\rangle, |\gamma_2\rangle, \cdots, |\gamma_n\rangle\}$, where the symbol $\{\cdots\}$ represents the collection and $|\gamma_i\rangle$ represents a single qubit in $|\Gamma\rangle$. Any qubit $|\gamma_i\rangle$ $(i = 1,2,\cdots,n)$ in $|\Gamma\rangle$ can be represented as a superposition of two eigenstates $|0\rangle$ and $|1\rangle$, namely, $|\gamma_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$, where α_i, β_i are complex numbers that satisfy $|\alpha_i|^2 + |\beta_i|^2 = 1$. Thus, the signed quantum information string of Alice can be represented as $|\Gamma\rangle = \{\alpha_1|0\rangle + \beta_1|1\rangle, \alpha_2|0\rangle + \beta_2|1\rangle, \cdots, \alpha_n|0\rangle + \beta_n|1\rangle\}$. Note that if the signature quantum state is known, any copies of $|\Gamma\rangle$ can be prepared in advance. If the signature quantum state is unknown, at least three copies of $|\Gamma\rangle$ are necessary, among which one is combined with 5-particle entangled state, one produces a secret qubit string $|R_A\rangle$, and the other is sent to Bob.

Step S2: Alice transforms the information qubit string $|\Gamma\rangle$ into a secret qubit string $|R_A\rangle = M_{K_A}(|\Gamma\rangle)$ in terms of the secret key K_A. This transform method can be seen in [14].

Step S3: Alice prepares 5-particle entangled states. Alice combines each information qubit with 5-particle entangled state into the same long 6-particle qubit string. Each

combinatorial state includes one information particle and five entangled particle. This 6-particle combination state can be described as follows:

$$\begin{aligned}|\Psi^i\rangle_{M12345} &= |\gamma_i\rangle_M \otimes |\xi\rangle_{12345} = (\alpha_i|0\rangle + \beta_i|1\rangle)_M \otimes |\xi\rangle_{12345} \\ &= \frac{1}{2\sqrt{2}}[\alpha_i|000100\rangle - \alpha_i|000111\rangle + \alpha_i|001001\rangle - \alpha_i|001010\rangle + \alpha_i|010000\rangle \\ &+ \alpha_i|010011\rangle + \alpha_i|011101\rangle + \alpha_i|011110\rangle + \beta_i|100100\rangle - \beta_i|100111\rangle \\ &+ \beta_i|101001\rangle - \beta_i|101010\rangle + \beta_i|110000\rangle + \beta_i|110011\rangle + \beta_i|111101\rangle \\ &+ \beta_i|111110\rangle]_{M12345}\end{aligned}$$

Step S4: Alice uses Ω_A to represent the sequence of n (M, 2, 3) particles, where M represents the information particle to be signed. Ω_T represents the sequence of n (1, 4) particles, and Ω_B represents the sequence of n (5) particles. The decoy particles $|\mu\rangle_{A,T} = U_{F(x_A,x_T)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_T)}^{(0)}\rangle$ and $|\mu\rangle_{A,B} = U_{F(x_A,x_B)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_B)}^{(0)}\rangle$ are randomly inserted in Ω_T and Ω_B to form $\Omega_T^{'}$ and Ω'_B, respectively. Alice sends $\Omega_T^{'}$ to Trent and Ω'_B to Bob.

Step S5: Alice performs von Neumann measurement on the particle sequence Ω_A that she has mastered. Suppose the n-group von Neumann measurement results are $\delta(\Omega_A) = \{\delta(\Omega_{A,1}), \delta(\Omega_{A,2}), \cdots, \delta(\Omega_{A,n})\}$, where $\Omega_{A,i} \in \{\chi^1, \chi^2, \cdots, \chi^8\}$. Alice encrypts $|R_A\rangle$ and $\delta(\Omega_A)$ to form the signature $|S\rangle = E_{K_A}(|R_A\rangle, \delta(\Omega_A))$ by using quantum one-time pad algorithm [41]. Note that $\delta(\Omega_A)$, even if sometimes described as classical bits, can be converted to qubits from the measurement basis $\{\chi^1, \chi^2, \cdots, \chi^8\}$. Alice sends the signature $|S\rangle$ and 2 information qubit strings $|\Gamma\rangle$ to Bob.

3.3. Verification Phase

Step V1: After confirming that Bob received Ω'_B, Alice tells Bob the position of the decoy particles and Bob executes the unitary operation $U_{-F(x_B,x_A)}$ on the decoy particle $|\mu\rangle_{A,B}$, that is, $|\mu\rangle_{B,A} = U_{-F(x_B,x_A)}|\mu\rangle_{A,B}$. Then, Bob measures the decoy particles using measurement basis $\{|\varphi_l^{(0)}\rangle \; | l \in q\}$. If $|\mu\rangle_{B,A} \neq |\varphi_0^{(0)}\rangle$, it implies that the identity authentication between Alice and Bob cannot be passed or the decoy particle have been eavesdropped. Finally, Bob calculates the error rate based on measurement outcomes of the decoy particles. If the error rate is less than the previously given value, they perform the next step. Otherwise, the execution of the protocol is aborted. After Bob passes the eavesdropping detection and identity authentication of Ω'_B, the decoy particles are removed and Ω_B is restored. Similarly, after confirming that Trent received Ω'_T, Alice tells Trent the position of the decoy particles and then Trent executes the unitary operations $U_{-F(x_T,x_A)}$ on the decoy particle $|\mu\rangle_{A,T}$, that is, $|\mu\rangle_{T,A} = U_{-F(x_T,x_A)}|\mu\rangle_{A,T}$. Then Trent measures the decoy particles using the measurement basis $\{|\varphi_l^{(0)}\rangle | l \in q\}$. If $|\mu\rangle_{T,A} \neq |\varphi_0^{(0)}\rangle$, it indicates that the identity authentication between Alice and Trent cannot be passed or that the particles are eavesdropped. Finally, Trent calculates the error rate based on measurement outcomes of the decoy particles. If the error rate is less than the previously given value, they perform the next step; otherwise, they abandon the agreement. After Trent performs the eavesdropping detection and identity authentication on Ω'_T, the decoy particles are removed and Ω_T is restored.

Step V2: After Bob receives $|S\rangle$ which was sent by Alice, he encrypts $|S\rangle$ and $|\Gamma\rangle$ with the secret key K_B to obtain $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$. Bob sends Y_B to Trent via a quantum channel.

Step V3: After receiving $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$, Trent decrypts it using secret key K_B to obtain $|S\rangle$ and $|\Gamma\rangle$, and decrypts $|S\rangle$ using secret key K_A to obtain $|R_A\rangle$ and $\delta(\Omega_A)$. In the meantime, Trent measures Ω_T with measurement basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ to obtain the measurement outcome $\delta(\Omega_T)$. Trent uses the secret key K_A to transform the information qubit string $|\Gamma\rangle$ into $|R_A^{'}\rangle$ and compare $|R_A\rangle$ with $|R_A^{'}\rangle$. If $|R_A\rangle = |R_A^{'}\rangle$, Trent sets the initial check parameter $\theta = 1$; otherwise, he sets $\theta = 0$. Note that this step and the subsequent

comparison of the quantum states can be found in [14,42]. To ensure the integrity of the signature, Trent selects an appropriate hash function $H(.)$ and calculates $H(|S\rangle)$.

Step V4: Trent encryptions $|S\rangle$, $H(|S\rangle)$, $\delta(\Omega_A)$, $\delta(\Omega_T)$, θ with secret key K_B and sends $Y_{TB} = E_{K_B}(|S\rangle, H(|S\rangle), \delta(\Omega_A), \delta(\Omega_T), \theta)$ to Bob.

Step V5: Bob decrypts Y_{TB} to obtain $|S\rangle$, $H(|S\rangle)$, $\delta(\Omega_A)$, $\delta(\Omega_T)$ and θ. If $\theta = 0$, Bob can assume that the signature was forged, he rejects the signature and exits the verification process; otherwise, Bob continues with the next verification process.

Step V6: According to the values of $\delta(\Omega_A)$ and $\delta(\Omega_T)$, Bob chooses the corresponding unitary operator $U_{(5)}$ in Table 4. Bob performs unitary operation $U_{(5)}$ on the particles in sequence Ω_B and measures them to obtain the quantum state $|\Gamma^{'}\rangle$. Notice that $|\Gamma^{'}\rangle$ is the result of executing controlled quantum teleportation. Then, he compares whether it is equal to $|\Gamma\rangle$. If $|\Gamma\rangle \neq |\Gamma^{'}\rangle$, Bob considers the signature invalid and rejects it. If $|\Gamma\rangle = |\Gamma^{'}\rangle$, Bob calculates $H^{'}(|S\rangle)$ with the same hash function and compares $H^{'}(|S\rangle)$ with $H(|S\rangle)$. If $H^{'}(|S\rangle) = H(|S\rangle)$, Bob accepts $|S\rangle$ as the signature of $|\Gamma\rangle$ from Alice; otherwise, the signature is rejected.

The schematic diagram of the main steps of the arbitrated quantum signature scheme is shown in Figure 3.

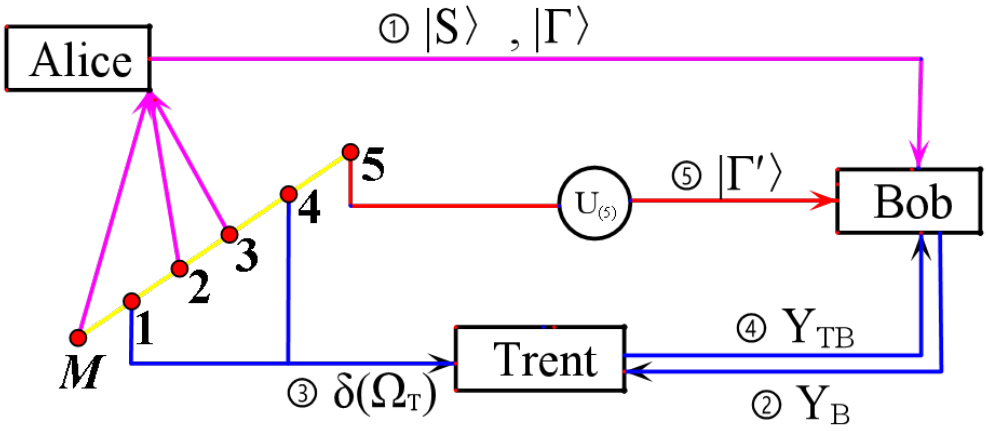

Figure 3. Schematic diagram of the main steps of the arbitrated quantum signature scheme.

4. Verifiability Analysis

We can prove that, in this scheme, identity authentication and eavesdropping detection can be conducted between Alice and Bob as well as between Alice and Trent according to the measurement outcomes of the decoy particles. An example for the proposed verifiable arbitrated quantum signature scheme can be seen in Appendix A.

In steps I3 and I4, according to Alice's share polynomial $F(x_A, y)$ and Bob's publicly identified information x_B, Alice calculates $F(x_A, x_B)$ and creates decoy particles $|\mu\rangle_{A,B} = U_{F(x_A,x_B)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_B)}^{(0)}\rangle$. According to Bob's share polynomial $F(x_B, y)$ and Alice's publicly identified information x_A, Bob calculates $F(x_B, x_A)$. In step V1, after Bob receives $|\mu\rangle_{A,B}$, he performs the unitary operation $U_{-F(x_B,x_A)}$ on $|\mu\rangle_{A,B}$, that is $|\mu\rangle_{B,A} = U_{-F(x_B,x_A)}|\mu\rangle_{A,B}$. According to the properties of symmetric binary polynomials, we have $F(x_B, x_A) = F(x_A, x_B)$ and $|\mu\rangle_{B,A} = U_{-F(x_B,x_A)}U_{F(x_A,x_B)}|\varphi_0^{(0)}\rangle = |\varphi_0^{(0)}\rangle$. Without external eavesdropping and cheating on either side, Bob's measurement outcomes of the decoy particles should be $|\varphi_0^{(0)}\rangle$; otherwise, it can be determined that either identity cheating on both sides or external eavesdropping are occurring. Therefore, Alice and Bob can verify whether identity cheating is occurring according to the measurement outcomes of the decoy particles. Similarly, identity verification and eavesdropping detection can also be conducted between Alice and Trent according to the measurement outcomes of the decoy particles.

5. Safety Analysis

A secure quantum signature scheme should be of an unforgeable and undeniable property. In other words, it should meet the following requirements: (1) The signature cannot be forged by an attacker (including external adversary Eve and malicious receiver Bob). (2) The signatory Alice cannot disavow the message and signature she sent, and the receiver Bob cannot disavow that he received the signature. (3) That can be arbitrated if the receiver Bob admits the fact of receiving the signature but disavows the integrity of the signature.

5.1. Impossibility of Forgery

If the external attacker Eve tries to forge Alice's signature $|S\rangle$ for her own benefit, she should know the key K_A. However, due to the unconditional security of quantum key distribution [39,40], this is not possible. In addition, the quantum one-time pad protocol [41] is used to improve the security. Therefore, Eve's forgery is impossible.

If the malicious receiver Bob tries to forge Alice's signature $|S\rangle = E_{K_A}(|R_A\rangle, \delta(\Omega_A))$ for his own benefit, he must also know Alice's secret key K_A. However, for the same reason, he cannot obtain any information about the key K_A. Thus, Bob cannot obtain the correct $|R_A\rangle$. Subsequently, the initial check parameter θ used in the verifying phase will not be right, so the arbitrator Trent will discover this forgery. In a worse case, even if key K_A is exposed to Eve, she still cannot forge the signature because she cannot create the appropriate $|R_A\rangle$ and $\delta(\Omega_A)$ to associate with the new message. Bob uses the correlation of the Bell state to find this kind of forged file; further verification of $|R_A\rangle = |R'_A\rangle$ cannot be established without the correct $|R_A\rangle$. However, if Bob knew the secret key K_A, forgery would be inevitable.

We can prove that Eve, an external attacker, cannot entangle a decoy particle or an information particle with an auxiliary particle to steal secret information and forge a signature. See Appendix B for details.

5.2. Impossibility of Disavowal by the Signatory and the Verifier

A secure quantum signature scheme should have undeniable property. In other words, once the quantum signature is verified as a valid signature, the signatory cannot disavow the fact that the quantum signature is generated by them. The receiver of the signature cannot disavow the fact that he has received the quantum signature.

5.2.1. Impossibility of Disavowal by the Signatory Alice

Suppose Alice tries to disavow the signature $|S\rangle$ that she has signed. As shown in Figure 4, after receiving the signature $|S\rangle$, Bob cannot decrypt it without the key K_A. He can only encrypt $|S\rangle$ and $|\Gamma\rangle$ to obtain Y_B and sends Y_B to Trent. After receiving Y_B, the arbitrator Trent decrypts $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$ and $|S\rangle = E_{K_A}(|R_A\rangle, \delta(\Omega_A))$ with K_A and K_B. As the signature $|S\rangle = E_{K_A}(|R_A\rangle, \delta(\Omega_A))$ contains the key K_A shared only by Alice and Trent, Trent can accurately confirm that the signature $|S\rangle$ was signed by Alice. Whether $|S\rangle$ is the signature of the message $|\Gamma\rangle$ is determined by the initial check parameter θ calculated by the arbitrator Trent. Because $|R_A\rangle = M_{K_A}(|\Gamma\rangle)$, $|R'_A\rangle = M_{K_A}(|\Gamma'\rangle)$, if $|R_A\rangle = |R'_A\rangle$, namely $\theta = 1$, then the signature $|S\rangle$ was signed by Alice for the message $|\Gamma\rangle$.

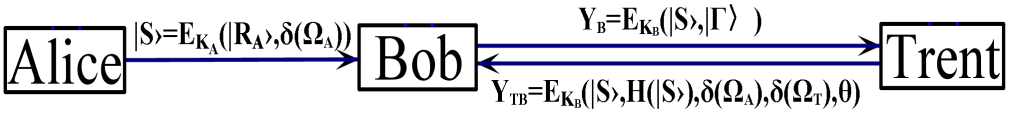

Figure 4. Diagram of transferring signature information.

5.2.2. Impossibility of Disavowal by the Verifier Bob

Similarly, as long as Trent receives the Y_B sent from Bob, because $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$ contains the key K_B shared only by Bob and Trent, Trent can confirm that Bob received

the signature and cannot change it, that is, Bob cannot disavow the fact that he received the signature. If Alice changes signature $|S\rangle$ to $|S'\rangle$, her behavior will be found when Bob calculates hash value $H'(|S\rangle)$ and compares it with $H(|S\rangle)$. If Bob admits to receiving the signature, but disavows the integrity of the signature, it can be arbitrated according to the hash value $H(|S\rangle)$ of $|S\rangle$.

In this scheme, the eavesdropping detection also functions as identity authentication, which can strengthen the undeniable property of Alice and Bob. In conclusion, our verifiable arbitrated quantum signature scheme has undeniable security.

6. Conclusions

In this paper, we proposed a verifiable arbitrated quantum signature scheme based on five-qubit entangled state. The proposed scheme uses mutually unbiased bases particles as decoy particles, and performs unitary operations on these decoy particles using the function values of symmetric binary polynomials, which can carry out not only eavesdropping detection, but also identity authentication among participants.

Due to the unconditional security of quantum key distribution and the quantum one-time pad, the external attacker Eve cannot know Alice's key K_A; she cannot forge Alice's signature $|S\rangle$ for her own benefit. For the same reason, Bob cannot forge Alice's signature $|S\rangle$, either. In order to avoid Alice's disavowal, we set that when Trent receives Alice's signature $|S\rangle$, the hash function value $H(|S\rangle)$ of the signature is calculated to ensure the integrity of the signature. After Trent receives Y_B and decrypts Y_B and $|S\rangle = E_{K_A}(|R_A\rangle, \delta(\Omega_A))$, the initial check parameter θ confirms that $|S\rangle$ is jointly generated by $|\Gamma\rangle$ and K_A, which proves that Alice did not cheat. At this time, since Trent had no information on parameter Ω_B, he could not forge a new signature. After Bob receives $Y_{TB} = E_{K_B}(|S\rangle, H(|S\rangle), \delta(\Omega_A), \delta(\Omega_T), \theta)$ and decrypts it, as the information of $\delta(\Omega_A), \delta(\Omega_T)$ and Ω_B are in his grasp at this time, he can use the function of quantum teleportation to reconstruct the information qubit $|\Gamma\rangle$ to judge whether to accept the quantum signature $|S\rangle$ signed by Alice.

Different from the signature scheme in classical cryptography, the security of our scheme is guaranteed by the quantum one-time pad [41] and quantum key distribution [39,40]. Therefore, it is unconditionally secure. The five-qubit entangled state plays a key role in quantum information processing tasks and it is the threshold number of qubits required for quantum error correction [43]. The principle of five-photon entanglement and open teleportation was reported in [44] and proved that von Neumann measurement, Bell measurement, and single-particle measurement are all feasible under the current technical and experimental conditions, so the scheme has good application value. Compared with the existing arbitrated quantum signature scheme [10,13,14,17,27], our scheme has high stability and can avoid being disavowed for the integrality of signature $|S\rangle$. But due to the large number of qubits used in the scheme, it also experiences the problem of low quantum efficiency.

Author Contributions: Data curation, Z.H.; Methodology, J.Y.; Project administration, Z.L.; Writing—original draft, D.L.; Writing—review & editing, D.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, grant number 11671244; 12071271 and The Applied Basic Research Project of Qinghai Province, grant number 2019-ZJ-7099.

Acknowledgments: We would like to thank the anonymous reviewers for their valuable comments. This work was supported by the National Natural Science Foundation of China under grant 11671244 and Grant 12071271. It was also financially supported by the Applied Basic Research Project of Qinghai Province (2019-ZJ-7099).

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

Appendix A. An Example for the Proposed Scheme

Suppose that Alice wants to sign the information particles $|\Gamma\rangle = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+\rangle, |0\rangle, |-\rangle, |1\rangle, |1\rangle, |0\rangle\}$, The following procedure needs to be performed.

Appendix A.1. Initializing Phase

Step I1: Alice and Trent share secret key $K_A = 00101101100110101011$. Bob and Trent share secret key $K_B = 10101001000100101011$.

Step I2: Trent selects a 4-order symmetric binary polynomial $F(x,y) = 11 + 7x + 4x^2 + 21x^3 + 18x^4 + 7y + 9xy + 5x^2y + 10x^3y + 13x^4y + 4y^2 + 5xy^2 + 6x^2y^2 + 14x^3y^2 + 19x^4y^2 + 21y^3 + 10xy^3 + 14x^2y^3 + 22x^3y^3 + 2x^4y^3 + 18y^4 + 13xy^4 + 19x^2y^4 + 2x^3y^4 + 19x^4y^4 mod 23$. Suppose that Alice's identity information is $x_A = 7$, Bob's identity information is $x_B = 3$, and Trent's identity information is $x_T = 13$. Trent calculates three share polynomials $f_T(y) = F(13,y) = 15y^4 + 11y^3 + 6y^2 + 12y + 20$, $f_A(y) = F(7,y) = 11y^4 + 15y^3 + 16y^2 + 21y + 8$ and $f_B(y) = F(3,y) = 4y^4 + 13y^3 + 12y^2 + 22y$. Trent encrypts $f_A(y)$ and sends $f'_A(y) = E_{K_A}(f_A(y))$ to Alice, and encrypts $f_B(y)$ and sends $f'_B(y) = E_{K_B}(f_B(y))$ to Bob.

Step I3: After Alice and Bob receive $f'_A(y)$ and $f'_B(y)$, respectively, Alice decrypts $f'_A(y)$ by using keys K_A to get $f_A(y) = F(7,y)$ and Bob decrypts $f'_B(y)$ by using keys K_B to get $f_B(y) = F(3,y)$. Alice calculates $f_A(x_B) = F(7,3) = 16$ and $f_A(x_T) = F(7,13) = 5$ based on Bob's and Trent's public identity information $x_B = 3$ and $x_T = 13$. Similarly, Bob calculates $f_B(x_A) = F(3,7) = 16$ and $f_B(x_T) = F(3,13) = 12$ based on Alice's and Trent's public identity information $x_A = 7$ and $x_T = 13$.

Step I4: Alice executes the unitary operations $U_{F(x_A,x_B)} = U_{16}$ and $U_{F(x_A,x_T)} = U_5$ on $|\mu\rangle = |\varphi_0^{(0)}\rangle = \frac{1}{\sqrt{q}}\sum_{i=0}^{q-1}|i\rangle$ to produce enough decoy particles: $|\mu\rangle_{A,B} = U_{16}|\varphi_0^{(0)}\rangle = |\varphi_{16}^{(0)}\rangle$ and $|\mu\rangle_{A,T} = U_5|\varphi_0^{(0)}\rangle = |\varphi_5^{(0)}\rangle$.

Appendix A.2. Signing Phase

Step S1: Suppose that the information qubit string $|\Gamma\rangle$ obtained by Alice is $|\Gamma\rangle = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+\rangle, |0\rangle, |-\rangle, |1\rangle, |1\rangle, |0\rangle\}$.

Step S2: Using secret key $K_A = 00101101100110101011$, Alice transforms the information qubit string $|\Gamma\rangle = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+\rangle, |0\rangle, |-\rangle, |1\rangle, |1\rangle, |0\rangle\}$ into $|R_A\rangle = M_{K_A}(|\Gamma\rangle) = \sigma_x^0\sigma_z^{0+1}|0\rangle \otimes \sigma_x^0\sigma_z^{0+1}|1\rangle \otimes \sigma_x^1\sigma_z^{1+1}|+\rangle \otimes \sigma_x^0\sigma_z^{0+1}|-\rangle \otimes \sigma_x^1\sigma_z^{1+1}|+\rangle \otimes \sigma_x^1\sigma_z^{1+1}|0\rangle \otimes \sigma_x^0\sigma_z^{0+1}|-\rangle \otimes \sigma_x^1\sigma_z^{1+1}|1\rangle \otimes \sigma_x^1\sigma_z^{1+1}|1\rangle \otimes \sigma_x^0\sigma_z^{0+1}|0\rangle = \sigma_z|0\rangle \otimes \sigma_z|1\rangle \otimes \sigma_x|+\rangle \otimes \sigma_z|-\rangle \otimes \sigma_x|+\rangle \otimes \sigma_x|0\rangle \otimes \sigma_z|-\rangle \otimes \sigma_x|1\rangle \otimes \sigma_x|1\rangle \otimes \sigma_z|0\rangle = |0\rangle(-|1\rangle)|+\rangle|+\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|0\rangle$.

Step S3: Alice prepares 5-particle entangled states: $|\xi\rangle_{12345} = \frac{1}{2}(|001\rangle|\phi^-\rangle + |010\rangle|\psi^-\rangle + |100\rangle|\phi^+\rangle + |111\rangle|\psi^+\rangle)_{12345}$. Alice combines each information qubit state with 5-particle entangled state into the same long 6-particle qubit string. The 6-particle qubit string is shown in Table A1.

Table A1. The 6-particle qubit string composed of information states and 5-particle entangled states.

$\|\Psi^1\rangle_{M12345} = \|\gamma_1\rangle_M \otimes \|\xi\rangle_{12345} = \|0\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^2\rangle_{M12345} = \|\gamma_2\rangle_M \otimes \|\xi\rangle_{12345} = \|1\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^3\rangle_{M12345} = \|\gamma_3\rangle_M \otimes \|\xi\rangle_{12345} = \|+\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2\sqrt{2}}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$ $+\frac{1}{2\sqrt{2}}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^4\rangle_{M12345} = \|\gamma_4\rangle_M \otimes \|\xi\rangle_{12345} = \|-\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2\sqrt{2}}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$ $-\frac{1}{2\sqrt{2}}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^5\rangle_{M12345} = \|\gamma_5\rangle_M \otimes \|\xi\rangle_{12345} = \|+\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2\sqrt{2}}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$ $+\frac{1}{2\sqrt{2}}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^6\rangle_{M12345} = \|\gamma_6\rangle_M \otimes \|\xi\rangle_{12345} = \|0\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^7\rangle_{M12345} = \|\gamma_7\rangle_M \otimes \|\xi\rangle_{12345} = \|-\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2\sqrt{2}}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$ $-\frac{1}{2\sqrt{2}}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^8\rangle_{M12345} = \|\gamma_8\rangle_M \otimes \|\xi\rangle_{12345} = \|1\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^9\rangle_{M12345} = \|\gamma_9\rangle_M \otimes \|\xi\rangle_{12345} = \|1\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|1001\rangle\|\phi^-\rangle + \|1010\rangle\|\psi^-\rangle + \|1100\rangle\|\phi^+\rangle + \|1111\rangle\|\psi^+\rangle)_{M12345}$
$\|\Psi^{10}\rangle_{M12345} = \|\gamma_{10}\rangle_M \otimes \|\xi\rangle_{12345} = \|0\rangle_M \otimes \|\xi\rangle_{12345} = \frac{1}{2}(\|0001\rangle\|\phi^-\rangle + \|0010\rangle\|\psi^-\rangle + \|0100\rangle\|\phi^+\rangle + \|0111\rangle\|\psi^+\rangle)_{M12345}$

Step S4: Alice inserts decoy particles $|\mu\rangle_{A,T} = U_{F(x_A,x_T)}|\varphi_0^{(0)}\rangle = U_{F(7,13)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_T)}^{(0)}\rangle = |\varphi_5^{(0)}\rangle$ and $|\mu\rangle_{A,B} = U_{F(x_A,x_B)}|\varphi_0^{(0)}\rangle = U_{F(7,3)}|\varphi_0^{(0)}\rangle = |\varphi_{F(x_A,x_B)}^{(0)}\rangle = |\varphi_{16}^{(0)}\rangle$ into sequence Ω_T and Ω_B to form $\Omega_T^{'}$ and $\Omega_B^{'}$, respectively. Alice sends $\Omega_T^{'}$ to Trent and $\Omega_B^{'}$ to Bob.

Step S5: Alice performs von Neumann measurement on the particles sequence Ω_A that she has mastered. Suppose that 10-group von Neumann measurement outcomes are $\delta(\Omega_A) = \{\chi^1, \chi^4, \chi^2, \chi^7, \chi^3, \chi^6, \chi^8, \chi^5, \chi^1, \chi^7\}$. Alice encrypts R_A and $\delta(\Omega_A)$ to form the signature:

$$|S\rangle = E_{K_A}(\{|0\rangle(-|1\rangle)|+\rangle|+\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|0\rangle\}, \{\chi^1, \chi^4, \chi^2, \chi^7, \chi^3, \chi^6, \chi^8, \chi^5, \chi^1, \chi^7\}).$$

Then, Alice sends the signature $|S\rangle$ and 2 information qubit strings $|\Gamma\rangle$ to Bob.

Appendix A.3. Verifytion Phase

Step V1: After confirming that Bob received $\Omega_B^{'}$, Alice tells Bob the position of the decoy particles, and then Bob executes the unitary operation $U_{-F(x_B,x_A)} = U_{-16}$ on the decoy particle $|\mu\rangle_{A,B}$. That is, $|\mu\rangle_{B,A} = U_{-F(x_B,x_A)}|\mu\rangle_{A,B} = U_{-F(3,7)}|\mu\rangle_{A,B} = U_{-16}|\varphi_{16}^{(0)}\rangle = |\varphi_0^{(0)}\rangle$. Bob uses measurement basis $\{|\varphi_l^{(0)}\rangle|l \in q\}$ to measure the decoy particles. If $|\mu\rangle_{B,A} \neq |\varphi_0^{(0)}\rangle$, it implies that the identity authentication between Alice and Bob cannot be passed or the particles have been eavesdropped. Finally, Bob calculates the error rate based on measurement outcomes of the decoy particles. If the error rate is less than the previously given value, they perform the next step; otherwise, the execution of the protocol is aborted. After Bob passes the eavesdropping detection and identity authentication on $\Omega_B^{'}$, the decoy particles are removed and Ω_B is recovered. Similarly, after confirming that Trent received $\Omega_T^{'}$, Alice tells Trent the position of the decoy particles, and then Trent executes the unitary operation $U_{-F(x_T,x_A)} = U_{-5}$ on the decoy particle $|\mu\rangle_{A,T}$. That is, $|\mu\rangle_{T,A} = U_{-F(x_T,x_A)}|\mu_{A,T} = U_{-5}|\mu\rangle_{A,T} = U_{-5}|\varphi_5^{(0)}\rangle = |\varphi_0^{(0)}\rangle$. Then Trent measures the decoy particles using the measurement basis $\{|\varphi_l^{(0)}\rangle|l \in q\}$. If $|\mu\rangle_{T,A} \neq |\varphi_0^{(0)}\rangle$, it implies that the identity authentication between Alice and Trent cannot be passed or that the particles are eavesdropped. Finally, Trent calculates the error rate based on measurement outcomes of the decoy particles. If the error rate is less than the previously given value, they perform the next step; otherwise, they abandon the agreement. After Trent performs the eavesdropping detection and identity authentication on $\Omega_T^{'}$, the decoy particles are removed and Ω_T is restored.

Step V2: After Bob receives the $|S\rangle$ which is sent by Alice, he encrypts $|S\rangle$ and $|\Gamma\rangle$ with secret key K_B to obtain $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$, where $Y_B = E_{K_B}(E_{K_A}(\{|0\rangle(-|1\rangle)|+\rangle|+\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|0\rangle\}, \{\chi^1, \chi^4, \chi^2, \chi^7, \chi^3, \chi^6, \chi^8, \chi^5, \chi^1, \chi^7\}), \{|0\rangle|1\rangle|+\rangle|-\rangle|+\rangle|0\rangle|-\rangle|1\rangle|1\rangle|0\rangle\})$. Bob sends Y_B to Trent via a quantum channel.

Step V3: After receiving $Y_B = E_{K_B}(|S\rangle, |\Gamma\rangle)$, Trent decrypts it using secret key K_B to obtain $|S\rangle$ and $|\Gamma\rangle$, and decrypts $|S\rangle$ using secret key K_A to obtain $|R_A\rangle$ and $\delta(\Omega_A)$. Where $|\Gamma\rangle = \{|0\rangle|1\rangle|+\rangle|-\rangle|+\rangle|0\rangle|-\rangle|1\rangle|1\rangle|0\rangle\}$, $|R_A\rangle = M_{K_A}(|\Gamma\rangle) = |0\rangle(-|1\rangle)|+\rangle|+\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|0\rangle$, $\delta(\Omega_A) = \{\chi^1, \chi^4, \chi^2, \chi^7, \chi^3, \chi^6, \chi^8, \chi^5, \chi^1, \chi^7\}$. In the meantime, Trent measures Ω_T with measurement basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ to obtain the measurement outcome $\delta(\Omega_T)$. We suppose that $\delta(\Omega_T) = \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle, |\phi^-\rangle, |\psi^+\rangle, |\phi^-\rangle, |\phi^+\rangle, |\phi^+\rangle, |\phi^-\rangle\}$. Using the secret key K_A, Trent transforms the information qubit string $|\Gamma\rangle$ into $|R_A^{'}\rangle$ and compares $|R_A\rangle$ with $|R_A^{'}\rangle$. If $|R_A\rangle = |R_A^{'}\rangle$, Trent sets the initial check parameter $\theta = 1$, otherwise he sets $\theta = 0$.

Step V4: Trent encrypts $|S\rangle, H(|S\rangle), \delta(\Omega_A), \delta(\Omega_T), \theta$ with secret key K_B to obtain $Y_{TB} = E_{K_B}(E_{K_A}(\{|0\rangle(-|1\rangle)|+\rangle|+\rangle|+\rangle|1\rangle|+\rangle|0\rangle|0\rangle|0\rangle\}, \{\chi^1, \chi^4, \chi^2, \chi^7, \chi^3, \chi^6, \chi^8, \chi^5, \chi^1, \chi^7\}), H(|S\rangle), \delta(\Omega_A), \delta(\Omega_T), \theta)$ and sends it to Bob.

Step V5: Bob decrypts Y_{TB} to obtain $|S\rangle$, $H(|S\rangle)$, $\delta(\Omega_A)$, $\delta(\Omega_T)$ and θ. If $\theta = 0$, Bob can assume that the signature was forged, he rejects the signature and exits the verification process. Otherwise, Bob continues to carry out the next verification process.

Step V6: According to the values of $\delta(\Omega_A)$ and $\delta(\Omega_T)$, Bob chooses the corresponding unitary operator $U_{(5)} = \{(\sigma_x)_5, (\sigma_z)_5, (\sigma_z)_5, -(\sigma_x)_5, I_5, (-\sigma_z)_5, (\sigma_z)_5, (\sigma_x)_5, (\sigma_x)_5, (-I_5)\}$. Bob performs unitary operation $U_{(5)}$ on the particles in sequence Ω_B and measures them to obtain the quantum state $|\Gamma^{'}\rangle$, and then he compares whether it is equal to $|\Gamma\rangle = \{|0\rangle|1\rangle|+\rangle|-\rangle|+\rangle|0\rangle|-\rangle|1\rangle\ |1\rangle|0\rangle\}$. If $|\Gamma\rangle \neq |\Gamma^{'}\rangle$, Bob considers the signature invalid and rejects it. If $|\Gamma\rangle = |\Gamma^{'}\rangle$, Bob computes $H^{'}(|S\rangle)$ and compares $H^{'}(|S\rangle)$ with $H(|S\rangle)$. If $H^{'}(|S\rangle) = H(|S\rangle)$, Bob accepts $|S\rangle$ as the signature of $|\Gamma\rangle$ sent by Alice. Otherwise, the signature is rejected.

Appendix B. Unforgeable Property of Eve'S Entangle-Measure Attack

Appendix B.1. Eve Cannot Entangle a Decoy Particle to Forge a Signature

We can prove that the external attacker Eve cannot entangle a decoy particle with an auxiliary particle to steal secret information and forge a signature.

Lemma A1. *For the measurement basis* $|\varphi_g^{(0)}\rangle = \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kg}|k\rangle$, $\omega = e^{\frac{2\pi i}{q}}$, *we have* $\sum_{m=0}^{q-1}|m\rangle = \frac{1}{\sqrt{q}}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle$.

Proof.

$$\frac{1}{\sqrt{q}}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}\rangle$$
$$= \frac{1}{\sqrt{q}}[|\varphi_0^{(0)}\rangle + \omega^{-m}|\varphi_1^{(0)}\rangle + \omega^{-2m}|\varphi_2^{(0)}\rangle + \cdots + \omega^{-m(q-1)}|\varphi_{q-1}^{(0)}\rangle]$$
$$= \frac{1}{\sqrt{q}}[\sum_{k=0}^{q-1}|k\rangle + \omega^{-m}\sum_{k=0}^{q-1}\omega^{k}|k\rangle + \omega^{-2m}\sum_{k=0}^{q-1}\omega^{2k}|k\rangle + \cdots + \omega^{-m(q-1)}\sum_{k=0}^{q-1}\omega^{(q-1)k}|k\rangle]$$
$$= \frac{1}{\sqrt{q}}[\sum_{k=0}^{q-1}\omega^{-mg}|0\rangle + \sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle + \sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle + \cdots + \sum_{g=0}^{q-1}\omega^{g(q-1-m)}|q-1\rangle]$$
$$\frac{1}{\sqrt{q}}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_g^{(0)}$$
$$= \frac{1}{q}[\sum_{m=0}^{q-1}(\sum_{k=0}^{q-1}\omega^{-mg}|0\rangle + \sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle + \sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle + \cdots + \sum_{g=0}^{q-1}\omega^{g(q-1-m)}|q-1\rangle)]$$
$$= \frac{1}{q}[\sum_{m=0}^{q-1}\sum_{k=0}^{q-1}\omega^{-mg}|0\rangle + \sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(1-m)}|1\rangle + \sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(2-m)}|2\rangle + \cdots$$
$$+ \sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{g(q-1-m)}|q-1\rangle]$$

$= \frac{1}{q}[q|0\rangle + q|1\rangle + \cdots q|q-1\rangle] = \sum_{m=0}^{q-1}|m\rangle$. □

Suppose that Eve prepares an auxiliary quantum state $|E\rangle$, and she executes unitary operation U_E, which can entangle the auxiliary quantum states onto the transmitted particles to steal secret information by measuring the auxiliary particles. Consider the corresponding measurement basis $|\varphi_l^{(0)}\rangle = \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}|k\rangle$, which is in the attack of decoy

particles. According to Lemma 1, the following expression can be obtained by executing unitary operation U_E.

$$U_E|k\rangle|E\rangle = \sum_{m=0}^{q-1} a_{km}|m\rangle|\varepsilon_{km}\rangle \tag{A1}$$

$$\begin{aligned} U_E|\varphi_l^{(0)}\rangle|E\rangle &= U_E\left(\frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}|k\rangle\right)|E\rangle \\ &= \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\omega^{kl}\left(\sum_{m=0}^{q-1}a_{km}|m\rangle|\varepsilon_{km}\rangle\right) \\ &= \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\sum_{m=0}^{q-1}\omega^{kl}a_{km}\left(\frac{1}{\sqrt{q}}\sum_{g=0}^{q-1}\omega^{-mg}|\varphi_l^{(0)}\rangle\right)|\varepsilon_{km}\rangle \\ &= \frac{1}{\sqrt{q}}\sum_{k=0}^{q-1}\sum_{m=0}^{q-1}\sum_{g=0}^{q-1}\omega^{kl-mg}a_{km}|\varphi_l^{(0)}\rangle|\varepsilon_{km}\rangle. \end{aligned} \tag{A2}$$

where $\omega = e^{\frac{2\pi i}{q}}$ and $|E\rangle$ express the initial auxiliary quantum state; $|\varepsilon_{km}\rangle$ $(k, m = 0, 1, \cdots, q-1)$ denotes the only pure state obtained by executing unitary operation U_E.

Therefore, their coefficients satisfy condition $\sum_{m=0}^{q-1}|a_{km}|^2 = 1(k = 0, 1, \cdots, q-1)$. The unitary operation U_E must satisfy the following conditions if there is no error introduced by Eve:

$$a_{km} = \begin{cases} 0 & k \neq m \\ 1 & k = m \end{cases}$$

$k, m \in 0, 1, \cdots, q-1$.

Consequently, $(A1)$ and $(A2)$ can be simplified as: $U_E|k\rangle|E\rangle = a_{kk}|k\rangle|\varepsilon_{kk}\rangle$, $U_E|\varphi_l^{(0)}\rangle|E\rangle = \frac{1}{q}\sum_{k=0}^{q-1}\sum_{g=0}^{q-1}\omega^{k(l-g)}a_{kk}|\varphi_l^{(0)}|\varepsilon_{kk}\rangle$.

Similarly, Eve can obtain the equations: $\sum_{k=0}^{q-1}\omega^{k(l-g)}a_{kk}|\varepsilon_{kk}\rangle = 0$, where $g \neq l$, $g \in \{0, 1, \cdots q-1\}$. For any $l \in \{0, 1, \cdots q-1\}$, we can obtain q equations. According to these equations, the following formula can be calculated:

$$a_{00}|\varepsilon_{00}\rangle = a_{11}|\varepsilon_{11}\rangle = \cdots = a_{q-1,q-1}|\varepsilon_{q-1,q-1}\rangle.$$

This means that, no matter what quantum states are adopted, Eve can only obtain the same information from the auxiliary particles. Therefore, Eve fails to obtain any signature messages by conducting this kind of attack.

Appendix B.2. Eve Cannot Entangle an Information Particle to Forge a Signature

We can also prove that Eve cannot entangle an information particle with an auxiliary particle to steal secret information and forge a signature. Since Eve does not have the keys K_A and K_T, there is only one opportunity for him to attack Bob's information particle, i.e., during the transmission of the particle (5) from Alice to Bob in Step V6 of the verification phase. We can describe the effect of Eve's eavesdropping on qubit (5) using the following equations:

$$\tilde{U}_E|0\rangle|E\rangle = |0\rangle|\varepsilon_{00}\rangle + |1\rangle|\varepsilon_{01}\rangle, \tilde{U}_E|1\rangle|E\rangle = |0\rangle|\varepsilon_{10}\rangle + |1\rangle|\varepsilon_{11}\rangle,$$

$$\tilde{U}_E|+\rangle|E\rangle = \frac{1}{2}[|+\rangle(|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle) + |-\rangle(|\varepsilon_{00}\rangle - |\varepsilon_{01}\rangle + |\varepsilon_{10}\rangle - |\varepsilon_{11}\rangle)],$$

$$\tilde{U}_E|-\rangle|E\rangle = \frac{1}{2}[|+\rangle(|\varepsilon_{00}\rangle + |\varepsilon_{01}\rangle - |\varepsilon_{10}\rangle - |\varepsilon_{11}\rangle) + |-\rangle(|\varepsilon_{00}\rangle - |\varepsilon_{01}\rangle - |\varepsilon_{10}\rangle + |\varepsilon_{11}\rangle)],$$

where $|E\rangle$ is Eve's auxiliary state. $\{|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle\}$ are the pure auxiliary states determined uniquely by the unitary operation U_E. Therefore, $\{|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle\}$ must satisfy the relationship $\tilde{U}_E\tilde{U}_E^+ = I$, i.e., $\langle\varepsilon_{00}|\varepsilon_{00}\rangle + \langle\varepsilon_{01}|\varepsilon_{01}\rangle = 1$, $\langle\varepsilon_{10}|\varepsilon_{10}\rangle + \langle\varepsilon_{11}|\varepsilon_{11}\rangle = 1$, $\langle\varepsilon_{10}|\varepsilon_{00}\rangle + \langle\varepsilon_{11}|\varepsilon_{01}\rangle = 0$, $\langle\varepsilon_{00}|\varepsilon_{01}\rangle + \langle\varepsilon_{10}|\varepsilon_{11}\rangle = 0$. If no errors are introduced in Bob's detection, we can get $|\varepsilon_{01}\rangle = |\varepsilon_{01}\rangle = 0$. This implies that if Eve wants to attack without introducing any error, his auxiliary state and Alice's particle (5) will be in a tensor product state. Therefore, if Eve tries to take an attack strategy on the particle (5), he will be detected during the comparison between $|\Gamma\rangle$ and $|\Gamma'\rangle$ in Step V6 of the verification phase.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–19 December 1984; pp. 175–179.
2. Wang, X.B.; Yu, Z.W.; Hu, X.L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **2018**, *98*, 062323. [CrossRef]
3. Zhou, Y.H.; Yu, Z.W.; Li, A.; Hu, X.L.; Wang, X.B. Measurement-device-independent quantum key distribution via quantum blockade. *Sci. Rep.* **2018**, *8*, 4155. [CrossRef]
4. Ryan, A.; Erika, A. Unconditionally secure quantum signatures. *Entropy* **2015**, *17*, 5635–5659.
5. Chen, F.L.; Wang, Z.H.; Hu, Y.M. A new quantum blind signature scheme with bb84-state. *Entropy* **2019**, *21*, 336. [CrossRef]
6. Yadav, P.; Mateus, P.; Paunković N.; Souto, A. Quantum contract signing with entangled pairs. *Entropy* **2017**, *21*, 821. [CrossRef]
7. Martini, F.; Sciarrino, F. Twenty years of quantum state teleportation at the sapienza university in rome. *Entropy* **2019**, *21*, 768. [CrossRef] [PubMed]
8. González-Guillén C.; Vasco, M.; Johnson, F.; Pozo, N. An attack on zawadzki's quantum authentication scheme. *Entropy* **2021**, *23*, 389. [CrossRef] [PubMed]
9. Jeong, Y.C.; Ji, S.W.; Hong, C.; Park, H.S.; Jang, J. Deterministic secure quantum communication on the bb84 system. *Entropy* **2020**, *22*, 1268. [CrossRef] [PubMed]
10. Zeng, G.H.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]
11. Curty, M.; Lütkenhaus, N. Comment on Arbitrated quantum-signature scheme. *Phys. Rev. A* **2008**, *77*, 046301. [CrossRef]
12. Zeng, G. Reply to Comment on arbitrated quantum-signature scheme. *Phys. Rev. A* **2008**, *78*, 016301. [CrossRef]
13. Li, Q.; Chan, W.H.; Long, D.Y. Arbitrated quantum signature scheme using Bell states. *Phys. Rev. A* **2009**, *79*, 054307. [CrossRef]
14. Zou, X.; Qiu, D. Security analysis and improvements of arbitrated quantum signature schemes. *Phys. Rev. A* **2010**, *82*, 042325. [CrossRef]
15. 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]
16. Choi, J.W.; Chang, K.Y.; Hong, D. Security problem on arbitrated quantum signature schemes. *Phys. Rev. A* **2011**, *84*, 062330. [CrossRef]
17. Yang, Y.G.; Zhou, Z.; Teng, Y.W.; Wen, Q.Y. Arbitrated quantum signature with an untrusted arbitrator. *Eur. Phys. J. D* **2011**, *61*, 773–778. [CrossRef]
18. 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]
19. Liu, F.; Qin, S.J.; Su, Q. An arbitrated quantum signature scheme with fast signing and verifying. *Quantum Inf. Process.* **2014**, *13*, 491–502. [CrossRef]
20. 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]
21. 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]
22. 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]
23. Yang, Y.G.; Liu, Z.C.; Li, J.; Chen, X.B.; Zuo, H.J.; Zhou, Y H.; Shi, W.M. Theoretically extensible quantum digital signature with starlike cluster states. *Quantum Inf. Process.* **2017**, *16*, 12. [CrossRef]
24. Shi, R.H.; Ding, W.T.; Shi, J.J. Arbitrated quantum signature with Hamiltonian algorithm based on blind quantum computation. *Int. J. Theor. Phys.* **2018**, *57*, 1961–1973. [CrossRef]
25. Feng, Y.; Shi, R.; Guo, Y. Arbitrated quantum signature scheme with continuous-variable squeezed vacuum states. *Chin. Phys. B* **2018**, *27*, 020302. [CrossRef]
26. Feng, Y.; Shi, R.H.; Shi, J.J.; Zhou, J.; Guo, Y. Arbitrated quantum signature scheme with quantum walk-based teleportation. *Quantum Inf. Process.* **2019**, *18*, 254. [CrossRef]
27. Chen, L.Y.; Liao, Q.; Tan, R.C.; Gong, L.H.; Chen, H.Y. Offline arbitrated semi-quantum signature scheme with four-particle cluster state. *Int. J. Theor. Phys.* **2020**, *59*, 3685–3695. [CrossRef]

28. Bennett, C.H.; Brassard, G.; Crepeau, C.; Jozsa, R.; Peres, A.; William, K. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.* **1993**, *70*, 1895–1899. [CrossRef] [PubMed]
29. Karlsson, A.; Bourennane, M. Quantum teleportation using three-particle entanglement. *Phys. Rev. A* **1998**, *58*, 99. [CrossRef]
30. Deng, F.G.; Li, C.Y.; Li, Y.S.; Zhou, H.Y.; Wang, Y. Symmetric multiparty-controlled teleportation of an arbitrary two particle entanglement. *Phys. Rev. A* **2005**, *72*, 656–665. [CrossRef]
31. Nie, Y.Y.; Liu, J.C.; Sang, M.H. Perfect teleportation of an arbitrary three-qubit state by using w-class states. *Int. J. Theor. Phys.* **2011**, *50*, 3225–3229. [CrossRef]
32. Agrawal, P.; Pati, A. Perfect teleportation and superdense coding with w-states. *Phys. Rev. A* **2006**, *74*, 154. [CrossRef]
33. Nie, Y.Y.; Li, Y.H.; Liu, J.C.; Sang, M.H. Quantum information splitting of an arbitrary three-qubit state by using two four-qubit cluster states. *Quantum Inf. Process.* **2011**, *10*, 297–305. [CrossRef]
34. Nie, Y.Y.; Hong, Z.H.; Huang, Y.B.; Yi, X.J.; Li, S.S. Non-maximally entangled controlled teleportation using four particles cluster states. *Int. J. Theor. Phys.* **2009**, *48*, 1485–1490. [CrossRef]
35. Zhang, B.; Liu, Y. Economic and deterministic quantum teleportation of arbitrary bipartite pure and mixed state with shared cluster entanglement. *Int. J. Theor. Phys.* **2009**, *48*, 2644–2651. [CrossRef]
36. Brown, I.D.K.; Stepney, S.; Sudbery, A.; Braunstein, S.L. Searching for highly entangled multi-qubit states. *J. Phys. A Math. Gen.* **2005**, *38*, 1119–1131. [CrossRef]
37. Muralidharan, S.; Panigrahi, P.K. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. *Phys. Rev. A* **2006**, *77*, 032321. [CrossRef]
38. Wootters, W.K.; Fields, B.D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **1989**, *191*, 363–381. [CrossRef]
39. Lo, H.; Chau, H. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]
40. Shor, P.W.; Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
41. Boykin, P.O.; Roychowdhury, V. Optimal encryption of quantum bits. *Phys. Rev. A* **2003**, *67*, 042317. [CrossRef]
42. Buhrman, H.; Cleve, R.; Watrous, J.; Wolf, R.D. Quantum fingerprinting. *Phys. Rev. Lett.* **2001**, *87*, 167902. [CrossRef] [PubMed]
43. Bennett, C.H.; DiVincenzo, D.P.; Smolin, J.A.; Wootters, W.K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **1996**, *54*, 3824. [CrossRef] [PubMed]
44. Zhao, Z.; Chen, Y.A.; Zhang, A.N.; Yang, T.; Briegel, H.J.; Pan, J.W. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **2004**, *430*, 54–58. [CrossRef]