Quantum Information Processing (2022) 21:390
https://doi.org/10.1007/s11128-022-03730-3

Provably secure arbitrated-quantum signature

Xiangjun Xin[1] · Li Ding[1] · Tianyuan Zhang[1] · Qinglan Yang[2] · Chaoyang Li[1]

Received: 1 May 2022 / Accepted: 3 November 2022 / Published online: 22 November 2022

Abstract

Although the researchers have proposed many arbitrator quantum signature (AQS) for various applications in practice, the security proof of most AQSs was not strictly presented. Many results have shown that the AQS schemes without strict security proof may be broken by various measurement and forgery attacks. Therefore, a secure AQS should strictly put its security on the quantum theorems and principles. Based on the non-orthogonal entangled-triple sequence, an AQS with provable security is proposed. First, the theoretical security proof of our AQS is presented. Second, we prove the non-cloning theorem for the entangled-triple sequence. Third, by using the non-cloning property of the entangled-triple particle, we prove the new AQS signature cannot be forged. At last, the non-repudiation of the proposed AQS is analyzed. We showed that if an adversary can break the signature, his/her actions will violate some quantum principles. The security proof of the proposed signature scheme also shows the idea of provable security for a quantum signature. On the other hand, in the proposed scheme, the partners need not perform the probabilistic quantum state comparison test. It has better qubit efficiency. Therefore, compared with the other similar schemes, ours has the better merits in security and efficiency.

Keywords Quantum signature · Provable security · Unforgeability · Non-repudiation

1 Introduction

Now, the world is a digital word. Every day, many digital messages are exchanged by the internet. And most often, the transmitted messages have to be authenticated by the message receivers. That is, the receivers need to check where the messages come from, and whether they have been eavesdropped or disturbed by an adversary before

✉ Xiangjun Xin
xin_xiang_jun@126.com

[1] College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China

[2] Library, Zhengzhou University of Light Industry, Zhengzhou 450002, China

receiving them. To address the need of authenticating digital messages, Diffie et al. [1] proposed the idea of digital signature. Generally, in a digital signature system, the signatory creates his/her signature by encrypting the message with some secret key, and the signature receiver can verifies its validity with the public key of the signer. By the digital signature technologies, one can efficiently authenticate the received digital messages.

Since the introduction of the digital signature, the researchers proposed many different classical signature schemes for the applications in different environments [2–6]. However, the security of all these classical digital signatures is heavily dependent on the mathematic computation problems [7, 8], which may be efficiently solved with the help of the modern quantum computer [9–12].

To make the digital signature be secure against the quantum computer, Gottesman and Chuang [13] introduced the concept of quantum digital signature, whose security was found on some physical theorems and quantum properties of the particles instead of the unproved mathematical assumptions. Therefore, the quantum signature has the good merit of physical security. Based on the work in [13], many novel quantum signature schemes were proposed [14–47]. In the schemes [13, 40–42], the signers' signing keys and public keys can only be used one time. To make the quantum signature more secure and practical, Zeng and Christoph developed the AQS [14], in which the signing key can be reused. In the AQS, an arbitrator, which is a party trusted by all participants, is introduced. The arbitrator takes part in the key generation phase so that the participants can share some private keys, which are used to sign and verify a message. During the signature verification phase, the arbitrator can securely help the signature verifier verify the quantum signature. What is more, the arbitrator is very helpful in solving the disputations between the signer and the verifier. Therefore, compared with the quantum signature in [13, 40–42], Zeng and Christoph's AQS was more efficient and practicable. Based on the Zeng et al.'s idea, many AQSs schemes [15–21, 23–39, 43–51] were proposed. For example, Yang et al. presented the weak arbitrator-based AQSs [15, 16, 44, 45] so as to improve the security of the AQS scheme. Jiang's AQS [17] was based on the product states with local indistinguishability so that the AQS could be more practicable. Although there were lots of AQSs, their security was not strictly proved. That is, there was not strictly proof to support the security of the proposed AQS schemes. In fact, many AQS schemes have been proven to be insecure against various attacks duo to two main reasons as follows.

First, according to Kerckhofs's principle, the security of the modern cryptography systems should depend on the secrecy of the users' private keys rather than the cryptography algorithm. Especially, in a signing system, if the signer's private key is broken, anyone can produce the forgery of the quantum signature by using the broken key. Generally, in an AQS scheme, the signer's private key is created by performing the unconditionally secure quantum key distribution protocol (e.g., BB84 Protocol [52]) such that the private key cannot be broken during the key generation phase of the scheme. However, it should be noted that in a quantum signature scheme, the signature is generated by performing the quantum encryption with the signer's private key. Therefore, the quantum signature also includes the information of the private key. To guarantee the security of the private key, the quantum signature ciphertext should be information-theoretically secure [53–55]. That is, the quantum signature should be theoretically indistinguishable such that the adversary cannot derive any useful information about the private key from the quantum signature. However, the information-theoretical security of most existing quantum signature schemes cannot be strictly proved. This means that for these schemes, the adversaries may get some information about the private keys by performing some measurement attacks or other unknown attacks to the quantum signatures. For example, in 2019, Chen et al. [56] proved the private keys of the quantum signature systems based on quantum one-time pad (QOTP) [57] could be broken by performing the controlled SWAP attack. This means the adversary can get some information about the private keys of the signers in the QOTP-based quantum signature systems (e.g., [14, 25–28, 36, 39, 43]) by the controlled SWAP attack. Therefore, the quantum signature ciphertext should be theoretically indistinguishable and the quantum signature scheme should be information-theoretically secure.

Second, can a quantum signature with unconditionally secure signing key (private key) be secure against forgery? The answer is no due to much strong proof. For example, under the man-in-the-middle attack, Luo's AQS [16] can be forged [22]. Although Jiang presented some security analysis in [17], his AQS can still be forged by a quantum adversary [23]. In [29], Zhou et al. showed that the quantum signature in [30] could be forged by adaptively performing some Hadamard gates on the signed message without knowing the private key of the signer. Similarly, Ding et al. [31] demonstrated that the quantum signature in [32] was not secure, because the signature receiver could generate a forgery by adaptively performing NOT gate to the received signature without knowing the signer's private key as well. He et al. [33] proved that in [34], the adversary could create a forgery by performing the NOT and Hadamard operators on the received signature, because he/she knew the structure of the original message. Gao et al.'s research results showed that some AQS schemes using Pauli operators were insecure against the participant's forgery [24]. Some other results [35–38] also showed various forgery attacks to the quantum signatures [36, 48–51] without knowing the signers' private keys. Why many quantum signatures can be forged? In fact, in these quantum signature schemes, there are two common features. First, in these schemes, the authors analyzed that their quantum signatures were secure against forgery because the forger could not master the private keys. Then, this kind of security analysis is not comprehensive, because many quantum signatures with unconditionally secure private keys can still be forged. On the other hand, their security against forgery cannot be proved with strict formal mathematical proof. No formal proof can sufficiently support that the unforgeability of these quantum signatures strictly depends on the basic principles of the quantum mechanics such as the non-cloning theorem and the theoretical indistinguishability of the quantum states. How can we guarantee the security of a quantum signature such that its unforgeability is strictly dependent on the basic principles of the quantum mechanics? A general idea is that the unforgeability of the quantum signature should be proved with the strict proof based on the principles of the quantum mechanics. That is, we should mathematically prove that if an adversary can generate a forgery for the quantum signature, his/her actions will violate some quantum principles. This is the idea of provable security for a quantum signature.

In this paper, the main contribution is that we propose the first provably secure AQS with strictly security proof. Different from most of the AQSs, the proposed scheme can be proved to be information-theoretically secure, and its security against forgery can be proved under the basic principle of quantum mechanics as well. In this ASQ, the signature is produced with the controlled particles such that the signed particles have the same states, which can be used to prove the theoretical indistinguishability of the proposed AQS. Thus, the secrecy of the signatory's private key can be proved. On the other hand, we prove that the unforgeability of the proposed AQS with the non-cloning principle. That is, for the proposed scheme, if an adversary can produce a forgery of the signature, his/her actions will violate the non-cloning principle. This means it is impossible for the adversary to generate a forgery for our signature under the basic principle of quantum mechanics. On the other hand, compared with the similar schemes, our AQS has the better merits in security and efficiency as well.

The following contents of our paper include: AQS scheme in Sect. 2, AQS security proof, security and efficiency comparisons in Sect. 3, and paper conclusion in Sect. 4. On the other hand, in appendix A and appendix B, a simple simulation of our scheme is presented.

2 The proposed AQS

In the proposed AQS scheme, the operators $H = (|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)/\sqrt{2}$ and $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ are used. We define the operator $H^0 = X^0 = I$, in which I is the identity map. Assume that $f : \{0, 1\}^* \to \{0, 1\}^n$ is a public one-way hash function, which has the uniform output. On the other hand, we assume Alice is the message signatory. Bob acts as the receiver. On the other hand, Trent is employed as the arbitrator, who is trusted by all of the other parties.

Our AQS includes the following three phases: initialization, signature generation phase and message verification phase.

2.1 Initializing phase

In this phase, the partners share the private key and entangled particle sequence. The following are the initializing steps.

IS-1: By performing Bennett and Brassard's quantum key distribution protocol (BB84 Protocol) [52], Trent and Alice share a random n-bit private key $k = (k_1, k_2, ..., k_n)$.

IS-2: In this step, the private key k is used. Trent prepares n entangled-triple particles ϕ_1, ϕ_2,..., ϕ_n. The state of each particle ϕ_i is $|\phi_i\rangle = \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^A\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^A\right\rangle\right)$, where $i = 1, 2, \ldots, n$. According to the private key $k = (k_1, k_2, \ldots, k_n)$, for each ϕ_i, if $k_i = 0$, Trent performs the operator $I \otimes I \otimes I$ on the particle ϕ_i, or he performs the operator $H \otimes H \otimes H$ on the particle ϕ_i. Thus, the state of each entangled $\phi_i (i = 1, 2, \ldots, n)$ is changed into.

$$|\phi_i\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^{A}\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^{A}\right\rangle\right), & \text{if } k_i = 0 \\ \frac{1}{\sqrt{2}}\left(\left|+_i^{(T1)}+_i^{(T2)}+_i^{A}\right\rangle + \left|-_i^{(T1)}-_i^{(T2)}-_i^{A}\right\rangle\right), & \text{if } k_i = 1 \end{cases}, \tag{1}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. According to the entangled particles $\phi_1, \phi_2, \ldots, \phi_n$, Trent composes three particle sequences $G_{T1} = \{t_1^{(T1)}, t_2^{(T1)}, \ldots, t_n^{(T1)}\}$, $G_{T2} = \{t_1^{(T2)}, t_2^{(T2)}, \ldots, t_n^{(T2)}\}$ and $G_A = \{a_1, a_2,\ldots, a_n\}$, in which $t_i^{(T1)}$,$t_i^{(T2)}$, and a_i $(i = 1, 2, \ldots, n)$ represent the first, the second and the third particle of ϕ_i, respectively.

IS-3: Trent randomly produces sufficient decoy particles whose states come from the non-orthogonal set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Then, Trent mixes them with G_A at random and gets the new non-orthogonal sequence G'_A. After that, Trent transmits the sequence G'_A to Alice.

IS-4: After Alice receives G'_A, Trent publishes the information of the decoy particles including their positions and correct states. Then, Alice measures all the decoy particles in G'_A and checks whether the measurement results are the same as those published by Trent. Once the error rate is above the established standards set by the system, the partners restart the protocol. Or Alice gets G_A from the sequence G'_A by deleting the decoy particles. G_A is kept by Alice as her private sequence.

2.2 Signing phase

Suppose that Alice will sign a classical message $c \in \{0, 1\}^*$. Alice generates the signature by the steps as follows.

SS-1: Alice computes the message digest $f(k\|c) = m = (m_1, m_2,\ldots, m_n)$ with her key k and the hash function f, where the symbol "||" denotes the connection of the bit strings. After that, Alice prepares a particle sequence $S = \{s_1, s_2,\ldots, s_n\}$, and the state of the i-th particle s_i of the sequence S is $|s_i\rangle = |m_i\rangle$.

SS-2: According to the private key k, the private sequence $G_A = \{a_1, a_2,\ldots, a_n\}$ and the sequence $S = \{s_1, s_2,\ldots, s_n\}$, Alice performs n controlled unitary operations as follows.

For the ith operation $(i = 1, 2, \ldots, n)$, if $k_i = 0$, Alice executes the controlled NOT operator on a_i and s_i, where a_i is operated as the controlled particle, while s_i as the target particle. Thus, the particles $t_i^{(T1)}$, $t_i^{(T2)}$, a_i and s_i are entangled together with the state

$$\left|\chi_{t_i^{(T1)},t_i^{(T2)},a_i,s_i}\right\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^{A}0_i^{S}\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^{A}1_i^{S}\right\rangle\right), & \text{if } m_i = 0 \\ \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^{A}1_i^{S}\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^{A}0_i^{S}\right\rangle\right), & \text{if } m_i = 1 \end{cases}. \tag{2}$$

For the ith operation ($i = 1, 2, \ldots, n$), if $k_i = 1$, Alice executes the operator H on a_i. Then, she performs the controlled NOT operation on a_i and s_i, where a_i is operated as the controlled particle, while s_i the target particle. Next, Alice performs the H operations on the particles a_i and s_i, respectively. Thus, the entangled state of $t_i^{(T1)}$, $t_i^{(T2)}$, a_i and s_i is changed into

$$\left|\chi_{t_i^{(T1)},t_i^{(T2)},a_i,s_i}\right\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(\left|+_i^{(T1)}+_i^{(T2)}+_i^{A}+_i^{S}\right\rangle + \left|-_i^{(T1)}-_i^{(T2)}-_i^{A}-_i^{S}\right\rangle\right), & \text{if } m_i = 0 \\ \frac{1}{\sqrt{2}}\left(\left|+_i^{(T1)}+_i^{(T2)}+_i^{A}-_i^{S}\right\rangle + \left|-_i^{(T1)}-_i^{(T2)}-_i^{A}+_i^{S}\right\rangle\right), & \text{if } m_i = 1 \end{cases}. \quad (3)$$

After that, Alice sends c and S to Bob. Bob keeps the particle sequence S as the quantum signature on c.

The simple schematic diagram of the signing process is shown in Fig. 1.

2.3 Verifying phase

In our scheme, Alice is the signer. In this phase, the quantum signature S signed by Alice is verified. This phase includes three verification steps:

VS-1: Bob publishes c. Then, by the decoy particles and the methods in steps IS-3 and IS-4, Bob sends Trent the sequence S.

VS-2: According to k, the private sequence $G_{T1} = \{t_1^{(T1)}, t_2^{(T1)}, \ldots, t_n^{(T1)}\}$ and the sequence $S = \{s_1, s_2, \ldots, s_n\}$, Trent performs n controlled unitary operations as follows.

For the ith operation ($i = 1, 2, \ldots, n$), if $k_i = 0$, Trent executes the controlled NOT operator on the controlled $t_i^{(T1)}$ and the target particle s_i. Then, the entangled state of $t_i^{(T1)}$, $t_i^{(T2)}$, a_i and s_i evolves into

$$\left|\chi_{t_i^{(T1)},t_i^{(T2)},a_i,s_i}\right\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^{A}\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^{A}\right\rangle\right)\left|0_i^{S}\right\rangle, & \text{if } m_i = 0 \\ \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^{A}\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^{A}\right\rangle\right)\left|1_i^{S}\right\rangle, & \text{if } m_i = 1 \end{cases}. \quad (4)$$

For the ith operation ($i = 1, 2, \ldots, n$), if $k_i = 1$, Trent performs the H operations on the particles $t_i^{(T1)}$ and s_i, respectively. Then, he performs the controlled NOT operator on $t_i^{(T1)}$ and s_i so that $t_i^{(T1)}$ is operated as the controlled particle, while s_i the target particle. At last, he applies operator H to $t_i^{(T1)}$. Then, the entangled state of $t_i^{(T1)}$, $t_i^{(T2)}$,

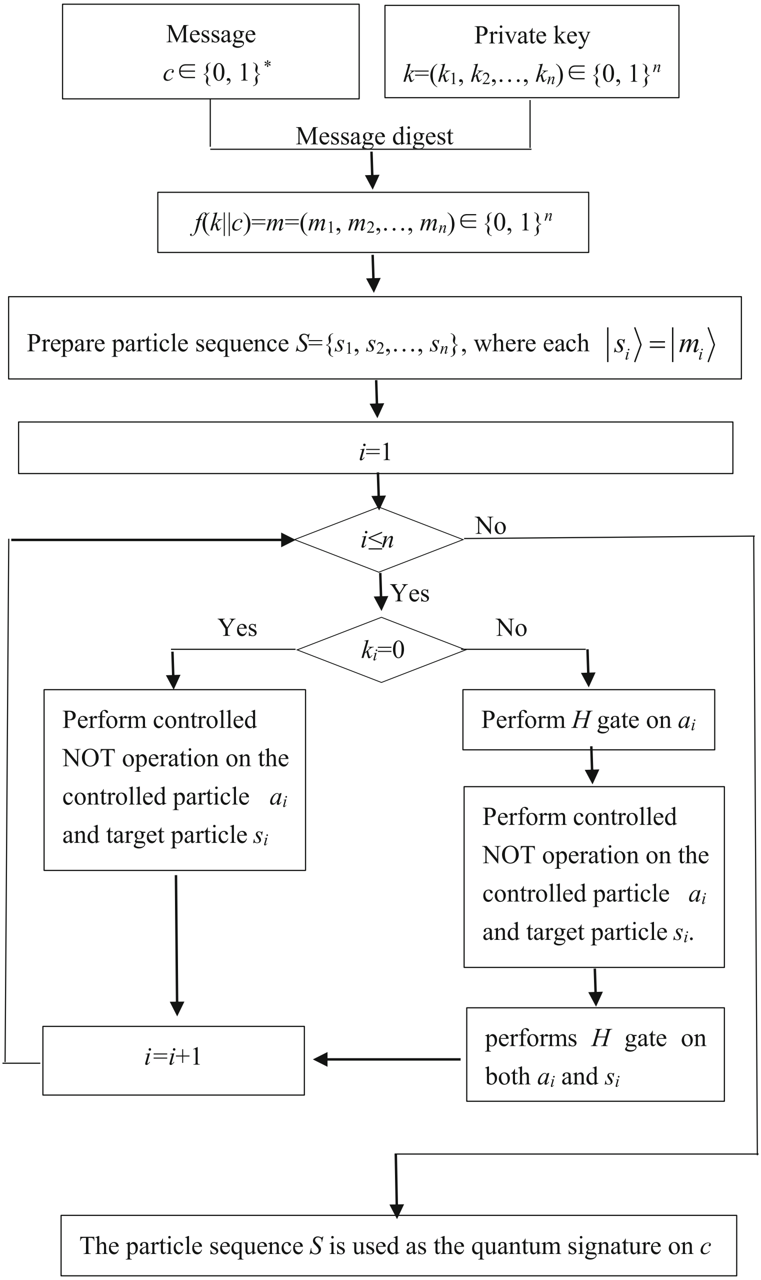
Message
$c \in \{0, 1\}^*$
Private key
$k=(k_1, k_2,\dots, k_n) \in \{0, 1\}^n$
Message digest
$f(k\|c)=m=(m_1, m_2,\dots, m_n) \in \{0, 1\}^n$
Prepare particle sequence $S=\{s_1, s_2,\dots, s_n\}$, where each $|s_i\rangle = |m_i\rangle$
$i=1$
$i \le n$
No
Yes
Yes
$k_i=0$
No
Perform controlled NOT operation on the controlled particle a_i and target particle s_i
Perform H gate on a_i
Perform controlled NOT operation on the controlled particle a_i and target particle s_i.
performs H gate on both a_i and s_i
$i=i+1$
The particle sequence S is used as the quantum signature on c

Fig. 1 Schematic diagram of the signing process

a_i and s_i evolves into

$$\left|\chi_{t_i^{(T1)},t_i^{(T2)},s_i}\right\rangle = \begin{cases} \frac{1}{\sqrt{2}}\left(\left|+_i^{(T1)}+_i^{(T2)}+_i^{A}\right\rangle + \left|-_i^{(T1)}-_i^{(T2)}-_i^{A}\right\rangle\right)\left|0_i^S\right\rangle, & \text{if } m_i = 0 \\ \frac{1}{\sqrt{2}}\left(\left|+_i^{(T1)}+_i^{(T2)}+_i^{A}\right\rangle + \left|-_i^{(T1)}-_i^{(T2)}-_i^{A}\right\rangle\right)\left|1_i^S\right\rangle, & \text{if } m_i = 1 \end{cases}. \tag{5}$$

VS-3: Trent measures each particle s_i ($i = 1, 2,\ldots, n$) with z-basis $\{|0\rangle, |1\rangle\}$. By the measurement result of s_i, Trent sets

$$m_i' = \begin{cases} 0, & \text{if } |s_i\rangle = |0\rangle \\ 1, & \text{if } |s_i\rangle = |1\rangle \end{cases}, \quad i = 1, 2, \ldots, n. \tag{6}$$

Thus, Trent gets $m' = \left(m_1', m_2', \ldots, m_n'\right)$. Then, by the shared k and the message c published by Bob, Trent computes the message digest $m = f(k\|c)$. Next, he checks whether $m = m'$. If $m = m'$($m \neq m'$), Trent publishes "Yes" ("No"), and Bob accepts (denies) the validity of the quantum signature. If the signature is valid, Trent also keeps (c, m, Bob) as the "proof" of the quantum signature so as to solve the disputation that may occur between Alice and Bob in the future.

3 Analysis of the security

The correctness of the AQS can be easily verified. This section first showed the theoretical security proof for the proposed AQS. Then, the unforgeability of the quantum signature is proved. At last, the no-repudiation of the signature is analyzed.

3.1 Information-theoretical security

In this section, first, by analyzing the density operator of the quantum signature, it is found that all the quantum signatures have the same state. What is more, any unitary operator attack to the quantum signature cannot change its density operator. This means that the adversary cannot get useful information about the private key by performing the unitary operator attack. Second, we analyze information-theoretical security of the proposed scheme. In [55], Yang et al. proved that for a quantum signature scheme, its information-theoretical security relies on the trace distance of the different quantum signatures. Then, by analyzing the trace distance of different quantum signatures, we prove that the trace distance of different quantum signatures is zero. Then, the proposed AQS can be proved to be information-theoretically secure.

Theorem 1. The quantum signatures on all the messages have the same density operator.

Proof. Note that any c and its signature S satisfies Eqs. (2) and (3). Hence, the density operator of s_i is.

$$\rho_{s_i} = \begin{cases} \frac{1}{2}\left(\left|0_i^S\right\rangle\left\langle 0_i^S\right| + \left|1_i^S\right\rangle\left\langle 1_i^S\right|\right) = \frac{I}{2}, & \text{if } m_i = 0,\ k_i = 0 \\ \frac{1}{2}\left(\left|1_i^S\right\rangle\left\langle 1_i^S\right| + \left|0_i^S\right\rangle\left\langle 0_i^S\right|\right) = \frac{I}{2}, & \text{if } m_i = 1,\ k_i = 0 \\ \frac{1}{2}\left(\left|+_i^S\right\rangle\left\langle +_i^S\right| + \left|-_i^S\right\rangle\left\langle -_i^S\right|\right) = \frac{I}{2}, & \text{if } m_i = 0,\ k_i = 1 \\ \frac{1}{2}\left(\left|-_i^S\right\rangle\left\langle -_i^S\right| + \left|+_i^S\right\rangle\left\langle +_i^S\right|\right) = \frac{I}{2}, & \text{if } m_i = 1,\ k_i = 1 \end{cases}. \tag{7}$$

Therefore, for any message c, the corresponding density operator of signature S is always $\rho_s = \frac{\otimes_{i=1}^n I}{2^n}$. Therefore, the quantum signatures on all the messages have the same density operator. □

Suppose that an adversary Eve attempts to get some information on the signer's secret k by performing some unitary operator $U = \otimes_{i=1}^n U_i$ on the signature S. However, we can prove that the operation U cannot change the density operator of the state of the signatures S.

Theorem 2. If an adversary Eve performs some unitary operator $U = \otimes_{i=1}^n U_i$ on the signature S, the density operator of the signature will not have any change. That is, for each message-signature pair (c, S), after the unitary operator attack $U = \otimes_{i=1}^n U_i$ on S, the density operator of the state of the disturbed quantum signature S is always $\rho_s = \frac{\otimes_{i=1}^n I}{2^n}$.

Proof. Note the signature S and the message c satisfy Eqs. (2) and (3). If an adversary Eve applies some unitary operator $U = \otimes_{i=1}^n U_i$ to S, the density operator of s_i can be computed as follows.

$$\rho_{s_i} = \begin{cases} \frac{1}{2}U_i\left(\left|0_i^S\right\rangle\left\langle 0_i^S\right| + \left|1_i^S\right\rangle\left\langle 1_i^S\right|\right)U_i^+ = \frac{I}{2}, & \text{if } m_i = 0,\ k_i = 0 \\ \frac{1}{2}U_i\left(\left|1_i^S\right\rangle\left\langle 1_i^S\right| + \left|0_i^S\right\rangle\left\langle 0_i^S\right|\right)U_i^+ = \frac{I}{2}, & \text{if } m_i = 1,\ k_i = 0 \\ \frac{1}{2}U_i\left(\left|+_i^S\right\rangle\left\langle +_i^S\right| + \left|-_i^S\right\rangle\left\langle -_i^S\right|\right)U_i^+ = \frac{I}{2}, & \text{if } m_i = 0,\ k_i = 1 \\ \frac{1}{2}U_i\left(\left|-_i^S\right\rangle\left\langle -_i^S\right| + \left|+_i^S\right\rangle\left\langle +_i^S\right|\right)U_i^+ = \frac{I}{2}, & \text{if } m_i = 1,\ k_i = 1 \end{cases}. \tag{8}$$

Therefore, if an adversary Eve applies some unitary operator $U = \otimes_{i=1}^n U_i$ to S, the density operator of the state of the disturbed quantum signatures S is $\rho_s = \frac{\otimes_{i=1}^n I}{2^n}$. Therefore, for any unitary operator attack, the signature density operator will not have any change. □

The following theorem shows that the AQS's information-theoretical security can also be proved. This means that the adversary can get no information about the secret key of the signatory from the published quantum signature by the unitary operation attack.

Theorem 3. For any message c and unitary operator attack $U = \otimes_{i=1}^{n} U_i$ on the signature S, the mutual information between private key space K and the probabilistic polynomial-time quantum adversary Eve is zero. That is,

$$I(K;\mathrm{Eve}|c,\ S,\ U) = 0. \tag{9}$$

Proof. Note that the mutual information.

$$I(K;\mathrm{Eve}|c,\ S,\ U) = H(K|c,\ S,\ U) - H(K|c,\ S,\ U,\mathrm{Eve}). \tag{10}$$

Because $H(K|c,\ S,\ U) \leq H(K)$, we can get

$$I(K;\mathrm{Eve}|c,\ S,\ U) \leq H(K) - H(K|c,\ S,\ U,\mathrm{Eve}). \tag{11}$$

Because the private k is randomly generated by performing the unconditional secure quantum protocol on key sharing [52], the private key space K has a uniform distribution. Therefore, the entropy of K is

$$H(K) = n. \tag{12}$$

Now, we consider the probability of Eve's successfully guessing the private key k under the unitary operator attack with the public message c and the quantum signature S. By Theorem 2 and Eq. (8), we can get that for any c, k and unitary operator attack U, the signature S has the same density operator. Therefore, According to Theorem 2 and Eq. (8), Eve can guess the private key k from c, S and the unitary operation attack U with a probability

$$\Pr(k|c,\ S,\ U,\ Eve) = \frac{1}{2^n}. \tag{13}$$

Hence, the conditional entropy

$$\begin{aligned} H(K|c,\ S,\ U,\mathrm{Eve}) &= -\sum_k \Pr(k|c,\ S,\ U,\mathrm{Eve}) \log \Pr(k|c,\ S,\ U,\mathrm{Eve}) \\ &= -\sum_k \left(\frac{1}{2^n} \log \frac{1}{2^n}\right) \\ &= n. \end{aligned} \tag{14}$$

Therefore, by Eqs. (11, 12, 14), we can get $I(K;\mathrm{Eve}|c,\ S,\ U) = 0$. □

Theorem 3 shows that if an adversary Eve tries to perform some unitary operator attack, he will get nothing about the signatory's secret key from the published information.

Now, for the proposed scheme, we prove that there exists no polynomial algorithm C_n such that the signatures on different messages can be efficiently distinguished.

It should be noted that the quantum signature is generated by encrypting the message c. Then, our scheme can be viewed as one quantum encryption scheme. In [53–55], for the quantum signature, its information-theoretical security is defined as follows.

Definition 1. We call a quantum signature is information-theoretically secure, if there exists no polynomial distinguishing algorithm D_n such that it can distinguish the quantum signatures S and S^* with a non-negligible probability, where S and S^* are the quantum signatures on any two different messages c and c^* in the message space $\{0, 1\}^n$, respectively. That is, for any positive polynomial $p(\cdot)$ and sufficient large n, a quantum signature scheme with information-theoretical security should satisfy

$$\left|\Pr\left[D_n\left(S^*\right) = 1\right] - \Pr[D_n(S) = 1]\right| < 1/p(n). \tag{15}$$

The results in [55] show that for a quantum signature scheme, its information-theoretical security relies on the trace distance of the different quantum signatures.

Theorem 4 [55] **.** A quantum signature has information-theoretical security only if, for each polynomial p and different messages c and c^*, the trace distance.

$$D(\rho_c, \rho_{c*}) < 1/p(n), \tag{16}$$

where $\rho_c(\rho_{c^*})$ denotes the density operator of the signature S (S^*) on $c(c^*)$.

Theorem 5. Our new AQS has the information-theoretical security.

Proof. Let c and c^* be any two different messages. Let S and S^* be the quantum signatures on the messages c and c^*, respectively. We use ρ_c and ρ_{c^*} which denote the density operators of the states of the quantum signatures S and S^*, respectively. According to Theorem 1, it follows that

$$\rho_c = \rho_{c^*} = \frac{\otimes_{i=1}^n I}{2^n}. \tag{17}$$

According to Eq. (17), we can get

$$D(\rho_c, \rho_{c*}) = 0. \tag{18}$$

It is clear that Eq. (18) satisfies the result of Theorem 4. Therefore, our scheme can be of information-theoretical security. □

The result of Theorem 5 means that no distinguishing algorithm D_n can distinguish the signatures S and S^* efficiently. This means that for our quantum signature scheme, no efficient distinguishing algorithm D_n can break the signer's key. Otherwise, given any two quantum signatures S and S^* on different messages c and c^*, respectively, the quantum adversary can use the private key to accurately generate the corresponding quantum signatures on c and c^* such that S and S^* can be distinguished by performing the quantum swap test algorithm [58], which contradicts the theoretical security of our AQS that proved in Theorem 5. Therefore, there is no efficient distinguishing algorithm that can break the signatory's private key. The proposed AQS can guarantee the secrecy of signatory's private key.

3.2 Unforgeability

In this section, we prove that it is infeasible to generate a forgery for the proposed quantum signature without knowing the private of the signer. First, based on the non-orthogonality of $\left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}$, the non-cloning theorem for the non-orthogonal entangled-triple sequence $\Pi = \{\pi_1, \pi_2, \ldots, \pi_k\}$ is proved, in which each $\pi_i \in \left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}$. Then, we prove that if an adversary can forge the quantum signature, his forgery action will violate the non-cloning theorem for the non-orthogonal entangled-triple sequence Π. This means it is infeasible for the adversary to forge the quantum signature of the signer.

Theorem 6. Given an entangled-triple sequence $\Pi = \{\pi_1, \pi_2, \ldots, \pi_k\}$, in which each entangled π_i $(1 \leq i \leq k)$ is randomly selected in the set $\left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}$, there is not any unitary operator W so that the sub-system of each π_i can be cloned. That is, there is not any unitary operator W so that.

$$W\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)|\varepsilon\rangle\right) = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle) \tag{19}$$

and

$$W\left(\frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)|\varepsilon\rangle\right) = \frac{1}{\sqrt{2}}(|++++\rangle + |----\rangle). \tag{20}$$

where ε is an auxiliary particle.

Proof. Let $\Pi = \{\pi_1, \pi_2, \ldots, \pi_k\}$ be an entangled-triple sequence, in which each entangled π_i $(1 \leq i \leq k)$ is randomly selected in the set $\left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}$. Note that the states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)$ are non-orthogonal. Therefore, the entangled-triple sequence Π is a non-orthogonal sequence, which cannot be accurately distinguished. Suppose there is some unitary operator W so that Eqs. (19, 20) hold. From Eqs. (19, 20), we can get.

$$(\langle 000| + \langle 111|)(|+++\rangle + |---\rangle) = (\langle 0000| + \langle 1111|)(|++++\rangle + |----\rangle), \tag{21}$$

from which we can get a conflict equation $1 = \sqrt{2}$. Therefore, there is not any unitary operator W so that the sub-system of each π_i can be cloned.

Theorem 7. Without the knowledge of the signer's private key, it is not feasible for the adversary Eve to produce a forged quantum signature.

Proof. Suppose Eve is a quantum adversary, who plays the role of the forger. Note that Sect. 3.1 has proved the information-theoretical security for the proposed AQS, which can ensure the secrecy of signatory's key. For our scheme, to forge the quantum signature, Eve has to query the oracle f for its output. Suppose that Eve can successfully forge a signature S on some message c without knowing the signatory's key k. And the answer for the output of the query on the oracle f about the message c is $m = (m_1, m_2,\ldots, m_n) \in \{0, 1\}^n$. Note that the quantum signature S satisfies Eqs. (2, 3). This means that the state sequence of entangled particle sequence including the forged quantum signature S is.

$$\chi_{T1,T2,A,S} = \left\{\left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle, \left|\chi_{t_2^{(T1)},t_2^{(T2)},a_2,s_2}\right\rangle, \ldots, \left|\chi_{t_n^{(T1)},t_n^{(T2)},a_n,s_n}\right\rangle\right\}, \tag{22}$$

in which each

$$\begin{aligned}&\left|\chi_{t_i^{(T1)},t_i^{(T2)},a_i,s_i}\right\rangle\\ &\in \left\{\begin{array}{l}\frac{1}{\sqrt{2}}\left(|0000\rangle + |1111\rangle\right), \frac{1}{\sqrt{2}}\left(|0001\rangle + |1110\rangle\right),\\ \frac{1}{\sqrt{2}}\left(|++++\rangle + |----\rangle\right), \frac{1}{\sqrt{2}}\left(|+++-\rangle + |---+\rangle\right)\end{array}\right\} \quad (i = 1, 2, \ldots, n).\end{aligned} \tag{23}$$

According to $m = (m_1, m_2,\ldots, m_n)$ and the forged quantum signature S, Eve composes a new particle sequence $S|_{m_{i_j}=0}$. That is, for each particle s_i $(1 \le i \le n)$ of the particle sequence S, if $m_i = 0$, Eve puts the particle s_i into the set $S|_{m_{i_j}=0}$. Assume that

$$S|_{m_{i_j}=0}= \left\{s_{i_1}, s_{i_2}, \ldots, s_{i_l}\right\}, \tag{24}$$

where $i_1, i_2,\ldots,i_l \in \{1, 2,\ldots, n\}$ and the corresponding $m_{i_1} = m_{i_2} = \cdots = m_{i_l} = 0$. According to Eq. (1), it follows that

$$\Phi|_{m_{i_j}=0} = \left\{\left|\phi_{i_1}\right\rangle, \left|\phi_{i_2}\right\rangle, \ldots, \left|\phi_{i_l}\right\rangle\right\} \in \left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}^l, \tag{25}$$

which is corresponding to Eq. (24). After the successful forgery, Eve queries about the private particles indexed by $i_1, i_2,\ldots,i_l$, the signing system outputs the particle sequence $\Phi|_{m_{i_j}=0}$ for Eve. Because $\Phi|_{m_{i_j}=0}$ is a non-orthogonal particle sequence, the particles in $\Phi|_{m_{i_j}=0}$ cannot be accurately distinguished from each other. Therefore, for Eve, $\Phi|_{m_{i_j}=0}$ is an unknown quantum sequence.

On the other hand, according to Eq. (22) and i_1, i_2,…,i_l, the signing system outputs a sequence

$$\chi_{T1,T2,A,S}|_{m_{i_j}=0}= \left\{ \left|\chi_{t_{i_1}^{(T1)},t_{i_1}^{(T2)},a_{i_1},s_{i_1}}\right\rangle, \left|\chi_{t_{i_2}^{(T1)},t_{i_2}^{(T2)},a_{i_2},s_{i_2}}\right\rangle, \ldots, \left|\chi_{t_{i_l}^{(T1)},t_{i_l}^{(T2)},a_{i_l},s_{i_l}}\right\rangle \right\}. \tag{26}$$

Now, we compare the form of each particle of the particle sequence $\Phi|_{m_{i_j}=0}$ with that of the particle sequence $\chi_{T1,T2,A,S}|_{m_{i_j}=0}$. According to Eqs. (2, 3, 24–26), it follows that if $k_{i_j} = 0$ ($j = 1, 2,\ldots, l$)

$$\begin{cases} \left|\phi_{i_j}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_{i_j}^{(T1)}0_{i_j}^{(T2)}0_{i_j}^{A}\right\rangle + \left|1_{i_j}^{(T1)}1_{i_j}^{(T2)}1_{i_j}^{A}\right\rangle\right) \\ \left|\chi_{t_{i_j}^{(T1)},t_{i_j}^{(T2)},a_{i_j},s_{i_j}}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_{i_j}^{(T1)}0_{i_j}^{(T2)}0_{i_j}^{A}0_{i_j}^{S}\right\rangle + \left|1_{i_j}^{(T1)}1_{i_j}^{(T2)}1_{i_j}^{A}1_{i_j}^{S}\right\rangle\right) \end{cases}. \tag{27}$$

If $k_{i_j} = 1$ ($j = 1, 2,\ldots, l$)

$$\begin{cases} \left|\phi_{i_j}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_{i_j}^{(T1)}+_{i_j}^{(T2)}+_{i_j}^{A}\right\rangle + \left|-_{i_j}^{(T1)}-_{i_j}^{(T2)}-_{i_j}^{A}\right\rangle\right) \\ \left|\chi_{t_{i_j}^{(T1)},t_{i_j}^{(T2)},a_{i_j},s_{i_j}}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_{i_j}^{(T1)}+_{i_j}^{(T2)}+_{i_j}^{A}+_{i_j}^{S}\right\rangle + \left|-_{i_j}^{(T1)}-_{i_j}^{(T2)}-_{i_j}^{A}-_{i_j}^{S}\right\rangle\right) \end{cases}. \tag{28}$$

According to Eqs. (24, 25, 27, 28), we can get that if Eve can produce a valid forged signature S, he can clone a particle sequence $S|_{m_{i_j}=0}= \left\{s_{i_1}, s_{i_2}, \ldots, s_{i_l}\right\}$ from the unknown entangled-triple sequence $\Phi|_{m_{i_j}=0} = \left\{\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_l}\right\}$, which is conflict to the non-cloning theorem (proved in Theorem 6) for the sub-system of each entangled ϕ_{i_j}. Therefore, it will be infeasible for Eve to forge the quantum signature of the signer.

3.3 Non-repudiation

In Sect. 3.2, for the proposed AQS, we have proved its unforgeability. Therefore, once the verification shows the validity of the signature, both the signer and the signature receiver cannot refuse its validity due to the unforgeability of the quantum signature.

For the signature, when the partners finish checking its validity, either the signatory or the signature receiver will lose the state of signature, because it has been changed after the signature verification. The signatory may deny her signature generation for the signature receiver. And the signature receiver may refuse his participation of the signature verification. In this case, Trent can solve the disputation between the signer and the signature receiver. Note that in the proposed scheme, the message digest of c is computed by $m = f(k\|c)$. That is, to compute the digest m, the private key k has to be used as the input of the one-way function f. Therefore, without k, it is not feasible for the adversary to compute the digest m. At the same time, without the input k of f, the adversary can guess the message digest m by the negligible probability $\frac{1}{2^n}$ because of the uniform distribution of f. This means that only the signatory can generate m by her key k. Note that in the new AQS, when verifying a signature, Trent keeps the triple (c, m, Bob) as the "proof" of the quantum signature. If the signatory denies her signature generation for the signature receiver, Trent can recover the proof (c, m, Bob) to prove that signer has ever produced the valid signature S, because only the signer can produce the message digest $m = f(k||c)$ with the private key k. On the other hand, it is infeasible for Bob to deny the truth of the signature verification due to the verification proof (c, m, Bob), in which c was announced by Bob.

According to the analysis above, it follows that both the signature receiver and the signer cannot refuse a valid signature. At the same time, the signer cannot deny her signature generation for the signature receiver, and the signature receiver cannot refuse his participation of the signature verification. Therefore, we can get the non-repudiation of the proposed AQS.

3.4 Security and efficiency comparisons

In this section, the security and efficiency of the similar schemes are compared. Here, we ignore the AQSs which have been proved to be insecure against forgery attacks and disavowal attacks.

First, although the private keys of most quantum signature systems were created with the unconditionally secure quantum key distribution protocol (e.g., BB84 Protocol), they still could be broken by some novel attacks or some unknown unitary operator attacks to the quantum signatures, which include the information of the private keys. For example, Chen et al. [56] found that the private keys of the QOTP [57]-based quantum signature schemes could be broken by performing the controlled SWAP attacks to the quantum signatures. This means the QOTP-based signatures in [14, 25–28, 36, 39, 43] is not immune to the controlled SWAP attacks. Therefore, to guarantee the security of private keys of the quantum signing systems, the quantum signature ciphertexts should be information-theoretically secure such that there is not any unitary operator attack or polynomial distinguishing algorithm which can distinguish the quantum signature ciphertexts with a non-negligible probability. In Sect. 3.1, we have proved the information-theoretical security of the proposed AQS scheme. However, in the similar schemes, the information-theoretical security of the quantum signatures was not proved.

Second, to our knowledge, in most of the quantum signature schemes including the schemes in [18, 23, 36, 44–47], the unforgeability of the signature was analyzed by emphasizing the secrecy of the private keys of the signers. However, according to the review of the quantum signature in Sect. 1, we know that many quantum signatures can be forged by various forgery attacks without knowing the private keys of the signers. No sufficient formal proof can mathematically prove that the unforgeability of these schemes relies on the basic the quantum theories. In this paper, we prove that the unforgeability of the proposed scheme depends on the non-cloning theorem.

Table 1 Security and efficiency comparisons

Schemes	Information-theoretical security	Provable security proof for unforgeability	Need quantum state comparison	Qubit efficiency (%)
[18]	No	No	Yes	50
[23]	No	No	No	60
[36]	No	No	No	33
[43]	No	No	Yes	5
[44]	No	No	No	50
[45]	No	No	Yes	14
[46]	No	No	Yes	14
[47]	No	No	Yes	20
Ours	Yes	Yes	No	50

That is, if the adversary can forge the signature, his/her actions will violate the non-cloning theorem. This means that it is infeasible for the adversary to forge the quantum signature. However, in the similar schemes, no sufficient formal security proof can mathematically prove that the unforgeability of these schemes is strictly dependent on the basic principles of the quantum mechanics.

Third, we compare the qubit efficiency of the similar AQSs. In [59], the qubit efficiency is defined as $\eta{=}\delta_1/\delta_2$, where $\delta_1(\delta_2)$ denotes the number of transmitted bits (qubits) in the quantum protocol. In our AQS, $2n$ qubits are transmitted during the signature generation and verification phases, while n bits classical message bits are authenticated. Therefore, the qubit efficiency of the proposed AQS is about 50%(the decoy particles which are used to check the quantum channel are ignored). In Table 1, the qubit efficiency of the other similar schemes is computed as well.

Fourth, in the schemes of [18, 43, 45–47], the arbitrators or the signature receivers had to perform the quantum state comparison algorithm [58] so as to verify the signature. Note that the quantum state comparison test may fail with probability $\left(1+\theta^2\right)/2$, where $\theta = |\langle\alpha \mid \beta\rangle| \in (0, 1)$ dependents on the compared states. Then, the signature can be successfully verified by the quantum state comparison algorithm with probability $p = 1 - \left(\frac{1+\theta^2}{2}\right)^t$, where t denotes the count of performing the quantum state comparison. Therefore, in [18, 43, 45–47], to make the comparison result be reliable, the verifiers should perform the state comparison many times so that $p = 1 - \left(\frac{1+\theta^2}{2}\right)^t \rightarrow 1(t \rightarrow +\infty)$. What is more, the signers should produce many copies of the quantum signature and transmit them to the receivers for the use of quantum state comparison. All of these will greatly decrease the computation efficiency and the qubit efficiency of the AQSs. In our AQS, the quantum signature is verified without performing any quantum state comparison algorithm. Therefore, compared with the similar AQSs [18, 43, 45–47], our scheme has the better computation efficiency.

4 Conclusions

First, in most of the existing AQSs, the signers' private keys were created with the unconditionally secure quantum key distribution protocol so that the private keys cannot be broken during the key generation phase. However, the adversary may break the private keys by performing some novel attacks (e.g., the controlled SWAP attacks) or some unknown attacks to the quantum signatures, which include the information of the private keys. Therefore, the quantum signature ciphertext should be theoretically indistinguishable and the quantum signature scheme should be information-theoretically secure such that the adversary can get no useful information about the private key of the signer from the quantum signatures.

Second, in most of the quantum signature schemes, the unforgeability of the signatures was analyzed by emphasizing the secrecy of the private keys of the signers. This kind of security analysis is not comprehensive. According to the review of the quantum signature schemes, we found many quantum signatures could still be forged, even if the private keys of the signers were unconditionally secure. Therefore, the unforgeablity of an AQS should be provably secure. The unforgeability of the quantum signature should be proved with the strict proof based on the principles of the quantum mechanics. We can prove that if an adversary can generate a forgery for the quantum signature, his/her actions will violate some quantum principles.

Third, we proposed such an AQS with provable security. The proposed AQS was different from the other existing AQS schemes. Its security can be supported by the information-theoretical indistinguishability of the non-orthogonal quantum states and the non-cloning theorem. In the proposed scheme, we proved the non-cloning theorem for the sub-system of the entangled-triple particles with non-orthogonal states. The unforgeability of the proposed scheme was proved as well. Theorem 7 shows that the unforgeability of the proposed AQS was put on the quantum mechanics. That is, the adversary forgery will lead to some conflict actions on the quantum principles. The security proof of our AQS also showed the idea of provable security for a quantum signature.

On the other hand, in the proposed AQS, the participants need not perform the probabilistic quantum state comparison test. The proposed scheme has better qubit efficiency.

Therefore, compared with the other similar schemes, ours has the better security and efficiency.

Acknowledgements This work is supported by the Key Scientific Research Project of Colleges and Universities in Henan Province (CN) (No.22A413010).

Data availability My manuscript has no associated data.

Appendix A: A simple simulation of the proposed scheme

To simplify the example, we suppose the parameter $n = 4$. Assume that $f : \{0, 1\}^* \rightarrow \{0, 1\}^4$ is a public one-way hash function, and it has the uniform output.

Appendix A.1: Initializing phase

IS-1: By performing Bennett and Brassard's BB84 Protocol, Trent and Alice share a random private key k. Assume $k = (1001)$. Thus, $k_1 = k_4 = 1$, $k_2 = k_3 = 0$.

IS-2: Trent prepares four entangled-triple particles ϕ_1, ϕ_2, ϕ_3 and ϕ_4. The state of each particle ϕ_i $(i = 1, 2, 3, 4)$ is $|\phi_i\rangle = \frac{1}{\sqrt{2}}\left(\left|0_i^{(T1)}0_i^{(T2)}0_i^A\right\rangle + \left|1_i^{(T1)}1_i^{(T2)}1_i^A\right\rangle\right)$. According to k, for each $\phi_i(i = 1, 2, 3, 4)$, if $k_i = 0$, Trent performs the operator $I \otimes I \otimes I$ on ϕ_i, or he performs the operator $H \otimes H \otimes H$ on ϕ_i. Thus, the states of ϕ_1, ϕ_2, ϕ_3 and ϕ_4 are changed into

$$\begin{cases} |\phi_1\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^A\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^A\right\rangle\right) \\ |\phi_2\rangle = \frac{1}{\sqrt{2}}\left(\left|0_2^{(T1)}0_2^{(T2)}0_2^A\right\rangle + \left|1_2^{(T1)}1_2^{(T2)}1_2^A\right\rangle\right) \\ |\phi_3\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^A\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^A\right\rangle\right) \\ |\phi_4\rangle = \frac{1}{\sqrt{2}}\left(\left|+_4^{(T1)}+_4^{(T2)}+_4^A\right\rangle + \left|-_4^{(T1)}-_4^{(T2)}-_4^A\right\rangle\right) \end{cases}, \tag{A1}$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. According to ϕ_1, ϕ_2, ϕ_3 and ϕ_4, Trent composes three particle sequences $G_{T1} = \{t_1^{(T1)}, t_2^{(T1)}, t_3^{(T1)}, t_4^{(T1)}\}$, $G_{T2} = \{t_1^{(T2)}, t_2^{(T2)}, t_3^{(T2)}, t_4^{(T2)}\}$ and $G_A = \{a_1, a_2, a_3, a_4\}$, in which $t_i^{(T1)}$,$t_i^{(T2)}$, and a_i represent the 1st, the 2nd and the 3rd particle of ϕ_i, respectively, where $i = 1, 2, 3, 4$.

IS-3: Trent randomly produces sufficient decoy particles whose states come from the non-orthogonal set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$**.** Then, Trent mixes them with G_A at random and gets the new non-orthogonal sequence G'_A. After that, Trent transmits the sequence G'_A to Alice.

IS-4: After Alice receives G'_A, Trent publishes the information of the decoy particles including their positions and correct states. Then, Alice measures all the decoy particles in G'_A and checks whether the measurement results are the same as those published by Trent. Once the error rate is above the established standards set by the system, the partners restart the protocol. Or Alice gets G_A from the sequence G'_A by deleting the decoy particles. G_A is kept by Alice as her private sequence.

Appendix A.2: Signing phase

Suppose that Alice will sign a classical message $c = (0100101)$.

SS-1: Alice computes the message digest $f(k\|c) = m$ with her key k and the hash function f. Suppose $m = (1100)$. Then $m_1 = m_2 = 1$ and $m_3 = m_4 = 0$. After that, Alice prepares a particle sequence where the symbol "||" denotes the connection of the bit strings. After that, Alice prepares a particle sequence $S = \{s_1, s_2, s_3, s_4\}$, and the state of the i-th particle s_i of the sequence S is $|s_i\rangle = |m_i\rangle$. That is,

$$|s_1\rangle = |s_2\rangle = |1\rangle \text{ and } |s_3\rangle = |s_4\rangle = |0\rangle.$$

SS-2: For the ith($i = 1, 2, 3, 4$) operation, if $k_i = 0$, Alice executes the controlled NOT operator on a_i and s_i, where a_i is operated as the controlled particle, while s_i as the target particle.

For the ith($i = 1, 2, 3, 4$) operation, if $k_i = 1$, Alice executes the operator H on a_i. Then, she performs the controlled NOT operation on a_i and s_i, where a_i is operated as the controlled particle, while s_i the target particle. Next, Alice performs the H operations on the particles a_i and s_i, respectively.

After that, the particles $t_i^{(T1)}$, $t_i^{(T2)}$, a_i and s_i are entangled together with the state as follows:

$$\begin{cases} \left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}-_1^{S}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}+_1^{S}\right\rangle\right) \\ \left|\chi_{t_2^{(T1)},t_2^{(T2)},a_2,s_2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_2^{(T1)}0_2^{(T2)}0_2^{A}1_2^{S}\right\rangle + \left|1_2^{(T1)}1_2^{(T2)}1_2^{A}0_2^{S}\right\rangle\right) \\ \left|\chi_{t_3^{(T1)},t_3^{(T2)},a_3,s_3}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}0_3^{S}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}1_3^{S}\right\rangle\right) \\ \left|\chi_{t_4^{(T1)},t_4^{(T2)},a_4,s_4}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_4^{(T1)}+_4^{(T2)}+_4^{A}+_4^{S}\right\rangle + \left|-_4^{(T1)}-_4^{(T2)}-_4^{A}-_4^{S}\right\rangle\right) \end{cases}, \tag{A2}$$

After that, Alice sends c and the particle sequence S to Bob. Bob keeps the particle sequence S as the quantum signature on c.

Appendix A.3: Verifying phase

VS-1: Bob publishes $c = (0100101)$. Then, by the decoy particles and the methods in steps IS-3 and IS-4, Bob sends Trent the sequence S.

VS-2: According to the shared key $k = (k_1, k_2, k_3, k_4) = (1001)$, the particle sequences $G_{T1} = \{t_1^{(T1)}, t_2^{(T1)}, t_3^{(T1)}, t_4^{(T1)}\}$ and $S = \{s_1, s_2, s_3, s_4\}$, Trent performs four controlled unitary operations as follows.

For the ith($i = 1, 2, 3, 4$) operation, if $k_i = 0$, Trent executes the controlled NOT operator on the controlled $t_i^{(T1)}$ and the target particle s_i.

For the ith ($i = 1, 2, 3, 4$) operation, if $k_i = 1$, Trent performs the H operations on the particles $t_i^{(T1)}$ and s_i, respectively. Then, he performs the controlled NOT operator on $t_i^{(T1)}$ and s_i so that $t_i^{(T1)}$ is operated as the controlled particle while s_i the target particle. At last, he applies operator H to $t_i^{(T1)}$.

After that, the entangled state of $t_i^{(T1)}$, $t_i^{(T2)}$, a_i and s_i ($i = 1, 2, 3, 4$) evolves into

$$\begin{cases} \left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}\right\rangle\right)\left|1_1^{S}\right\rangle \\ \left|\chi_{t_2^{(T1)},t_2^{(T2)},a_2,s_2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_2^{(T1)}0_2^{(T2)}0_2^{A}\right\rangle + \left|1_2^{(T1)}1_2^{(T2)}1_2^{A}\right\rangle\right)\left|1_2^{S}\right\rangle \\ \left|\chi_{t_3^{(T1)},t_3^{(T2)},a_3,s_3}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}\right\rangle\right)\left|0_3^{S}\right\rangle \\ \left|\chi_{t_4^{(T1)},t_4^{(T2)},a_4,s_4}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_4^{(T1)}+_4^{(T2)}+_4^{A}\right\rangle + \left|-_4^{(T1)}-_4^{(T2)}-_4^{A}\right\rangle\right)\left|0_4^{S}\right\rangle \end{cases}. \tag{A3}$$

VS-3: Trent measures each particle s_i ($i = 1, 2, 3, 4$) with z-basis $\{|0\rangle, |1\rangle\}$. By the measurement result of s_i, Trent sets $m' = \left(m'_1, m'_2, m'_3, m'_4\right)$, where.

$$m'_i = \begin{cases} 0, & \text{if } |s_i\rangle = |0\rangle \\ 1, & \text{if } |s_i\rangle = |1\rangle \end{cases}. \tag{A4}$$

According to Eq. (A3), it is clear that $|s_1\rangle = |s_2\rangle = |1\rangle$ and $|s_3\rangle = |s_4\rangle = |0\rangle$. Therefore, Trent gets $m' = (1, 1, 0, 0)$. Then, by the shared k and the message c published by Bob, Trent can compute the message digest $f(k\|c) = m = (1100)$. Next, he checks whether $m = m'$. If $m = m'$ ($m \neq m'$) Trent publishes "Yes"("No"), and Bob accepts (denies) the validity of the quantum signature. If the signature is valid, Trent also keeps (c, m, Bob) as the "proof" of the quantum signature so as to solve the disputation that may occur between Alice and Bob in the future.

For this example, it is obvious that $m = m'$. Then, the signature is valid. Thus, Trent keeps (c, m, Bob) as the "proof" of the quantum signature so as to solve the disputation that may occur between Alice and Bob in the future.

Appendix B: Analysis of the security

In this section, the example in Appendix A is used.

Appendix B.1: Information-theoretical security

Theorem 1. The quantum signatures on all the messages have the same density operator.

According to the proposed scheme in Appendix A, we know that the quantum signature S on message c satisfies Eq. (A2). By Eq. (A2), we can get

$$\begin{cases} \rho_{s_1} = \dfrac{1}{2}\left(\left|-_1^S\right\rangle\left\langle -_1^S\right| + \left|+_1^S\right\rangle\left\langle +_1^S\right|\right) = \dfrac{I}{2} \\ \rho_{s_2} = \dfrac{1}{2}\left(\left|1_2^S\right\rangle\left\langle 1_2^S\right| + \left|0_2^S\right\rangle\left\langle 0_2^S\right|\right) = \dfrac{I}{2} \\ \rho_{s_2} = \dfrac{1}{2}\left(\left|0_3^S\right\rangle\left\langle 0_3^S\right| + \left|1_3^S\right\rangle\left\langle 1_3^S\right|\right) = \dfrac{I}{2} \\ \rho_{s_4} = \dfrac{1}{2}\left(\left|+_4^S\right\rangle\left\langle +_4^S\right| + \left|-_4^S\right\rangle\left\langle -_4^S\right|\right) = \dfrac{I}{2} \end{cases}, \tag{A5}$$

Therefore, for the message c, the corresponding density operator of the signature S is $\rho_s = \frac{\otimes_{i=1}^4 I}{2^4}$. Similarly, for any signature S on the message c, we can compute the same density operator $\rho_s = \frac{\otimes_{i=1}^4 I}{2^4}$. Then, the correctness of Theorem 1 can be verified.

Theorem 2. If an adversary Eve performs some unitary operator $U = \otimes_{i=1}^n U_i$ on the signature S, the density operator of the signature will have not any change. That is, for each message–signature pair (c, S), after the unitary operator attack $U = \otimes_{i=1}^n U_i$ on S, the density operator of the state of the disturbed quantum signature S is always $\rho_s = \frac{\otimes_{i=1}^n I}{2^n}$.

For the example, the signature S and the message c satisfy Eq. (A2). If an adversary Eve applies some unitary operator $U = \otimes_{i=1}^4 U_i$ to S, the density operator of s_i can be computed as follow.

$$\begin{cases} \rho_{s_1} = \dfrac{1}{2}U_1\left(\left|-_1^S\right\rangle\left\langle -_1^S\right| + \left|+_1^S\right\rangle\left\langle +_1^S\right|\right)U_1^+ = \dfrac{I}{2} \\ \rho_{s_2} = \dfrac{1}{2}U_2\left(\left|1_2^S\right\rangle\left\langle 1_2^S\right| + \left|0_2^S\right\rangle\left\langle 0_2^S\right|\right)U_2^+ = \dfrac{I}{2} \\ \rho_{s_2} = \dfrac{1}{2}U_3\left(\left|0_3^S\right\rangle\left\langle 0_3^S\right| + \left|1_3^S\right\rangle\left\langle 1_3^S\right|\right)U_3^+ = \dfrac{I}{2} \\ \rho_{s_4} = \dfrac{1}{2}U_4\left(\left|+_4^S\right\rangle\left\langle +_4^S\right| + \left|-_4^S\right\rangle\left\langle -_4^S\right|\right)U_4^+ = \dfrac{I}{2} \end{cases}.$$

Therefore, if an adversary Eve applies some unitary operator $U = \otimes_{i=1}^4 U_i$ to S, the density operator of the state of the disturbed quantum signatures S keeps as $\rho_s = \frac{\otimes_{i=1}^4 I}{2^4}$. Therefore, for any unitary operator attack, the signature density operator will not have any change. Then, the correctness of Theorem 2 can be verified.

Theorem 3. For any message c and unitary operator attack $U = \otimes_{i=1}^n U_i$ on the signature S, the mutual information between private key space K and the probabilistic polynomial-time quantum adversary Eve is zero. That is,

$$I(K; \mathrm{Eve}|c,\ S,\ U) = 0. \tag{A6}$$

Theorem 3 depends on the result of Theorem 2, Eq. (8) and the distribution of the key space for the key generated by the unconditional secure BB84 protocol. For the proof of Theorem 3, please refer to Sect. 3.1

Theorem 4 [55]. A quantum signature has information-theoretical security only if, for each polynomial p and different messages c and c^*, the trace distance.

$$D(\rho_c, \rho_{c*}) < 1/p(n), \tag{A7}$$

where $\rho_c(\rho_{c^*})$ denotes the density operator of the signature S (S^*) on $c(c^*)$.

Theorem 5. Our new AQS has the information-theoretical security.

Let c and c^* be any two different messages. Let S and S^* be the quantum signatures on the messages c and c^*, respectively. We use ρ_c and ρ_{c^*} denote the density operators of the states of the quantum signatures S and S^*, respectively. According to Theorem 1, it follows that $\rho_c = \rho_{c^*} = \frac{\otimes_{i=1}^4 I}{2^4}$. Therefore,

$$D(\rho_c, \rho_{c*}) = 0. \tag{A8}$$

It is clear that Eq. (A8) satisfies the result of Theorem 4. Therefore, our scheme can be of information-theoretical security.

Appendix B.2: Unforgeability

Theorem 6. Given an entangled-triple sequence $\Pi = \{\pi_1, \pi_2, \ldots, \pi_k\}$, in which each entangled π_i $(1 \leq i \leq k)$ is randomly selected in the set $\left\{\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)\right\}$, there is not any unitary operator W so that the sub-system of each π_i can be cloned. That is, there is not any unitary operator W so that.

$$W\left(\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)|\varepsilon\rangle\right) = \frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$$

and

$$W\left(\frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)|\varepsilon\rangle\right) = \frac{1}{\sqrt{2}}(|++++\rangle + |----\rangle),$$

where ε is an auxiliary particle.

The proof the Theorem 3 depends on the non-orthogonality of the states $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $\frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle)$. For more detail proof of Theorem 3, please refer to Sect. 3.2.

Theorem 7. Without the knowledge of the signer's private key, it is not feasible for adversary Eve to produce a forged quantum signature.

For this example, the parameter $n = 4$ and the signer's private key $k = (k_1, k_2, k_3\ k_4) = (1001)$. Thus, $k_1 = k_4 = 1, k_2 = k_3 = 0$. Suppose Eve is a quantum adversary, who plays the role of the forger. Note that Sect. 3.1has proved the information-theoretical security for the proposed AQS, which can ensure the secrecy of signatory's key. For our scheme, to forge the quantum signature, Eve has to query the oracle f for its output. Suppose that Eve can successfully forge a signature S on some message $c = (0101100)$ without knowing the signatory's key k. And the answer for the output of the query on the oracle f about the message c is $m = (0101)$. Note that if S is a valid forgery. Then, the forgery S must satisfy Eq. (A9) as follows:

$$\begin{cases} \left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}+_1^{S}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}-_1^{S}\right\rangle\right) \\ \left|\chi_{t_2^{(T1)},t_2^{(T2)},a_2,s_2}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_2^{(T1)}0_2^{(T2)}0_2^{A}1_2^{S}\right\rangle + \left|1_2^{(T1)}1_2^{(T2)}1_2^{A}0_2^{S}\right\rangle\right) \\ \left|\chi_{t_3^{(T1)},t_3^{(T2)},a_3,s_3}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}0_3^{S}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}1_3^{S}\right\rangle\right) \\ \left|\chi_{t_4^{(T1)},t_4^{(T2)},a_4,s_4}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_4^{(T1)}+_4^{(T2)}+_4^{A}-_4^{S}\right\rangle + \left|-_4^{(T1)}-_4^{(T2)}-_4^{A}+_4^{S}\right\rangle\right) \end{cases}. \tag{A9}$$

According to $m = (0, 1, 0, 1)$ and the forged quantum signature S, Eve composes a new particle sequence $S|_{m_{i_j}=0}$. That is, for each particle s_i $(1 \le i \le 4)$ of the particle sequence S, if $m_i = 0$, Eve puts the particle s_i into the set $S|_{m_{i_j}=0}$. Then,

$$S|_{m_{i_j}=0} = \{s_1, s_3\} \tag{A10}$$

According to Eq. (A1), it follows that

$$\Phi|_{m_{i_j}=0} = \left\{ \begin{array}{l} |\phi_1\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}\right\rangle\right) \\ |\phi_3\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}\right\rangle\right) \end{array} \right\}. \tag{A11}$$

After the successful forgery, Eve queries about the private particles indexed by 1 and 3, the signing system outputs the particle sequence $\Phi|_{m_{i_j}=0}$ for Eve.

On the other hand, according to Eq. (A10) and the indexes 1 and 3, the signing system outputs a sequence

$$\chi_{T1,T2,A,S}|_{m_{i_j}=0} = \left\{\left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle, \left|\chi_{t_3^{(T1)},t_3^{(T2)},a_3,s_3}\right\rangle\right\}. \tag{A12}$$

Now, we compare the form of each particle of the particle sequence $\Phi|_{m_{i_j}=0}$ with that of the particle sequence $\chi_{T1,T2,A,S}|_{m_{i_j}=0}$. According to Eqs. (A9–A12), it follows that

$$\begin{cases} |\phi_1\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}\right\rangle\right) \\ \left|\chi_{t_1^{(T1)},t_1^{(T2)},a_1,s_1}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|+_1^{(T1)}+_1^{(T2)}+_1^{A}+_1^{S}\right\rangle + \left|-_1^{(T1)}-_1^{(T2)}-_1^{A}-_1^{S}\right\rangle\right) \end{cases}. \tag{A13}$$

$$\begin{cases} |\phi_3\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}\right\rangle\right) \\ \left|\chi_{t_3^{(T1)},t_3^{(T2)},a_3,s_3}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0_3^{(T1)}0_3^{(T2)}0_3^{A}0_3^{S}\right\rangle + \left|1_3^{(T1)}1_3^{(T2)}1_3^{A}1_3^{S}\right\rangle\right) \end{cases}. \tag{A14}$$

According to Eqs. (A10, A11, A13, A14), we can get that if Eve can produce a valid forged signature S, he can clone a particle sequence $S|_{m_{i_j}=0}= \{s_1, s_3\}$ from the entangled-triple sequence $\{\phi_1, \phi_3\}$, which is conflict to the non-cloning theorem (proved in Theorem 6) for the sub-system of each entangled ϕ_{i_j} of $\{\phi_1, \phi_3\}$. Therefore, it will be not feasible for Eve to forge the quantum signature of the signer.

References

1. Diffie, W., Hellman, M.E.: New direction in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
2. Mambo, M., Usuda, K., Okamoto, E.: Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundam. **E79-A**(5), 1338–1354 (1996)
3. Chaum, D.: Blind signatures for untraceable payments. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advance in Cryptology-CRYPTO'82, pp. 199–203. Springer, Boston (1983)
4. Chaum, D., Heyst, E.: Group signatures. In: Davies, D.W. (ed.) Advance in cryptology- EUROCRYPT'91, pp. 257–265. Springer, Berlin (1991)
5. Rastegari, P., Berenjkoub, M., Dakhilalian, M., et al.: Universal designated verifier signature scheme with non-delegatability in the standard model. Inform. Sci. **479**, 321–334 (2019)
6. Rastegari, P., Susilo, W., Dakhilalian, M.: Certificateless designated verifier signature revisited: achieving a concrete scheme in the standard model. Int. J. Inf. Secur. **18**(5), 619–665 (2019)
7. Rivest, R.L., Shamir, A., Adelman, L.: A method for obtain digital signatures and public-key cryptosystem. Commun. ACM **21**(2), 120–126 (1978)
8. Cha, C.J., Cheon, J.H.: An identity-based signature from gap Diffie-Hellman groups. In: PKC 2003, Springer, Berlin, pp. 18–30 (2003)
9. Shor, P. W.: Algorithms for quantum computation: discrete logarithm and factoring. In: Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE Computer Society Press, pp. 124–134 (1994)
10. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
11. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325–328 (1997)
12. Huang, Y., Su, Z., Zhang, F., Ding, Y.: Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. Quantum Inf. Process. **19**(62), 1–17 (2020)
13. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv: quant-ph/0105032 (2001)
14. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
15. Yang, Y.G., Zhou, Z., Teng, Y.W., Wen, Q.Y.: Arbitrated quantum signature with an untrusted arbitrator. Eur. Phys. J. D **61**, 773–778 (2011)
16. Luo, M.X., Chen, X.B., Yun, D., Yang, Y.X.: Quantum signature scheme with weak arbitrator. Int. J. Theor. Phys. **51**(7), 2135–2142 (2012)
17. Jiang, D.H., Xu, Y.L., Xu, G.B.: Arbitrary quantum signature based on local indistinguishability of orthogonal product states. Int. J. Theor. Phys. **58**(3), 1036–1045 (2019)
18. Wang, M.Q., Wang, X., Zhan, T.: An efficient quantum digital signature for classical messages. Quantum Inf. Process. **17**(10), 275 (2018)
19. Liang, X.Q., Wu, Y.L., Zhang, Y.H., Wang, S.S., Xu, G.B.: Quantum multi-proxy blind signature scheme based on four-qubit cluster states. Int. J. Theor. Phys. **58**(1), 31–39 (2019)
20. Qin, H., Tang, W.K.S., Tso, R.: Efficient quantum multi-proxy signature. Quantum Inf. Process. **18**(2), 53 (2019)
21. Xin, X., Wang, Z., Yang, Q., Li, F.: Quantum designated verifier signature based on Bell states. Quantum Inf. Process. **19**(79), 53 (2020)
22. Su, Q., Li, W.M.: Improved quantum signature scheme with weak arbitrator. Int. J. Theor. Phys. **52**(9), 3343–3352 (2013)
23. Xin, X., He, Q., Wang, Z., Yang, Q., Li, F.: Security analysis and improvement of an arbitrated quantum signature scheme. Optik **189**, 23–31 (2019)

24. Gao, F., Qin, S.J., Guo, F.Z., et al.: Cryptanalysis of the arbitrated quantum signature protocol. Phys. Rev. A **84**, 022344 (2011)
25. Li, Q., Chan, W.H., Log, D.Y.: Arbitrated quantum signature scheme using Bell states. Phys. Rev. A **79**(5), 054307 (2009)
26. Zou, X.F., Qiu, D.W.: Security analysis and improvements of arbitrated quantum signature schemes. Phys. Rev. A **82**(4), 23504–23516 (2010)
27. Li, W., Shi, R., Huang, D., et al.: Quantum blind dual-signature scheme without arbitrator. Phys. Scr. **91**, 035101 (2016)
28. Xia, C., Li, H., Hu, J.: A semi-quantum blind signature protocol based on five-particle GHZ state. Eur. Phys. J. Plus **136**, 633 (2021)
29. Zhou, B.M., Lin, L.D., Wang, W., et al.: Security analysis of particular quantum proxy blind signature against the forgery attack. Int. J. Theor. Phys. **59**, 465–473 (2020)
30. Liu, G., Ma, W.P., Cao, H., et al.: A novel quantum group proxy blind signature scheme based on five-qubit entangled state. Int. J. Theor. Phys. **58**, 1999–2008 (2019)
31. Ding, L., Xin, X., Yang, Q., et al.: Security analysis and improvements of XOR arbitrated quantum signature-based GHZ state. Mod. Phys. Lett. A **37**(2), 2250008 (2022)
32. Zheng, X.Y., Kuang, C.: Arbitration quantum signature protocol based on XOR encryption. Int. J. Quantum Inf. **18**, 2050025 (2020)
33. He, Q., Xin, X., Yang, Q.: Security analysis and improvement of a quantum multi-signature protocol. Quantum Inf. Process. **20**, 26 (2021)
34. Jiang, D.H., Hu, Q.Z., Liang, X.Q., et al.: A novel quantum multi-signature protocol based on locally indistinguishable orthogonal product states. Quantum Inf. Process. **18**(9), 268 (2019)
35. Zhang, L., Sun, H.W., Zhang, K.J., et al.: The security problems in some novel arbitrated quantum signature protocols. Int. J. Theor. Phys. **56**, 2433–2444 (2017)
36. Wang, C., Liu, J.W., Shang, T.: Enhanced arbitrated quantum signature scheme using Bell states. Chin. Phys. B **23**(6), 060309 (2014)
37. Xu, G., Zou, X.: Security analysis of an arbitrated quantum signature scheme with Bell states. Int. J. Theor. Phys. **55**, 4142–4156 (2016)
38. Liu, F., Zhang, K., Cao, T.: Security weaknesses in arbitrated quantum signature protocols. Int. J. Theor. Phys. **53**, 277–288 (2014)
39. Wang, J., Zhang, Q., Tang, C.J.: Efficient quantum signature protocol of classical messages. J. Commun. **28**(1), 64–68 (2003)
40. Dunjko, V., Wallden, P., Andersson, E.: Quantum digital signatures without quantum memory. Phys. Rev. Lett. **112**(4), 040502 (2014)
41. Wallden, P., Dunjko, V., Kent, A., et al.: Quantum digital signatures with quantum key distribution components. Phys. Rev. A **91**(4), 042304 (2014)
42. Amiri, R., Wallden, P., Kent, A., et al.: Secure quantum signatures using insecure quantum channels. Phys. Rev. A **93**(3), 032325 (2016)
43. Lu, D., Li, Z., Yu, J., et al.: A verifiable arbitrated quantum signature scheme based on controlled quantum teleportation. Entropy (Basel) **24**(1), 111 (2022)
44. Zou, X.F., Qiu, D.W., Mateus, P.: Security Analyses and improvement of arbitrated quantum signature with an untrusted arbitrator. Int. J. Theor. Phys. **52**(9), 3295–3305 (2013)
45. Zhang, M.L., Liu, Y.H., Nie, M., et al.: Arbitrated quantum signature of quantum messages with a semi-honest arbitrator. Int. J. Theor. Phys. **57**, 1310–1318 (2018)
46. Zhang, K.J., Zhang, W.W., Li, D.: Improving the security of arbitrated quantum signature against the forgery attack. Quantum Inf. Process. **12**(8), 2655–2669 (2013)
47. Zhang, L., Sun, H.W., Zhang, K.J., et al.: An improved arbitrated quantum signature protocol based on the key-controlled chained CNOT encryption. Quantum Inf. Process. **16**(3), 70 (2017)
48. Wang, Y., Xu, K., Guo, Y.: A chaos-based arbitrated quantum signature scheme in quantum crypoto-system. Int. J. Theor. Phys. **53**(1), 28–38 (2014)
49. Liu, F., Qin, S.J., Huang, W.: An arbitrated quantum signature with Bell states. Int. J. Theor. Phys **53**(5), 1569–1579 (2014)
50. Li, Q., Li, C.Q., Long, D.Y., et al.: Efficient arbitrated quantum signature and its proof of security. Quantum Inf. Process. **12**(7), 2427 (2013)
51. Li, Q., Du, R.G., Long, D.Y., et al.: Entanglement enhances the security of arbitrated quantum signature. Int. J. Quantum Inf. **7**(5), 913 (2009)

52. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. **560**, 7–11 (2014)
53. Menezes, A.J., Oorschot, P.V., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
54. Yang, L., Yang, B., Pan J.: Quantum public-key encryption with information theoretic security. In: Proceedings of SPIE, vol. 8440, p. 84400E-17 (2010)
55. Yang, L., Xiang, C., Li, B.: Quantum probabilistic encryption scheme based on conjugate coding. China Commun. **10**(2), 19–26 (2013)
56. Chen, F.L., Zhang, L.H., Zhang, H.: Controlled SWAP attack and improved quantum encryption of arbitrated quantum signature schemes. Quantum Inf. Process. **18**, 140 (2019)
57. Boykin, P.O., Roychowdhury, V.: Optimal encryption of quantum bits. Phys. Rev. A **67**(4), 645–648 (2003)
58. Buhrman, H., Cleve, R., Watrous, J., de Wolf, R.: Quantum fingerprinting. Phys. Rev. Lett. **87**(16), 167902 (2001)
59. Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with 100% qubit efficiency. IET Inf. Secur. **1**(1), 43–45 (2007)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.