Quantum Information Processing (2024) 23:49
https://doi.org/10.1007/s11128-024-04257-5

Secure quantum signature scheme without entangled state

Tianyuan Zhang[1] · Xiangjun Xin[1] · Lei Sun[2] · Chaoyang Li[1] · Fagen Li[3]

Received: 26 June 2023 / Accepted: 1 January 2024 / Published online: 6 February 2024

Abstract
The security of most quantum signatures cannot be proved with security model under chosen-message attack. No formal proof can prove that their security is fully dependent on the basic quantum theory. Based on the orthogonal quantum state and key-controlled quantum hash function, an arbitrated quantum signature is proposed. In this scheme, the signatory produces the quantum signature by quantum-encrypting the output of key-controlled quantum hash function. The signature verification is performed by decrypting the signed message and comparing the decrypted message with the output of the key-controlled quantum hash function. The security of the proposed scheme depends on the indistinguishability of the unknown quantum sequence. Its unforgeability can be formally proved with security model under chosen-message attack. Therefore, its security can be supported by the formal proof. On the other hand, in the proposed scheme, no entangled state is used. It also has better qubit efficiency as well.

Keywords Quantum signature · Security · Security model · Chosen-message attack · Unforgeability · Eavesdropping

1 Introduction

With the gradual advancement of digitalization in today's life, more and more messages need to be authenticated. That is, the receiver has to figure out the source of messages and checks whether they have been disturbed or eavesdropped or neither. To ensure the confidentiality and integrity of a message, Diffie et al. presented the theory of digital signature [1]. The signature generation process is essentially that the signer encrypts

✉ Xiangjun Xin
xin_xiang_jun@126.com

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

2 School of Mathematics and Physics, Yancheng Institute of Technology, Yancheng 224051, China

3 School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China

the message with his/her own signing key and the signing algorithm. Similarly, the signature verification process is essentially that the receiver decrypts the signature with the verifying key and verifying algorithm.

Digital signature schemes are used in various communication scenarios [2–6] to authenticate the identity of the communicator source and ensure the integrity and verifiability of communication data. Therefore, high requirements are put forward for the security of mathematic-problem-based digital signatures, whose safety barriers are built on the foundation of mathematic problems. However, according to the modern quantum research results, most of these problems such as discrete logarithm problem and prime factorization can be easily solved by quantum computers [7–9].

To keep the security of digital signature in the post-quantum era, Gottesman and Chuang introduced the idea of quantum digital signature [10] whose security was guaranteed by the quantum physics theory. Theoretically, the quantum signature not only can be unforgeable for the quantum adversary, but also can be secure against the eavesdropping attack.

The research result of reference [10] has opened up a new field of study: "quantum signatures" and many researchers have published abundant research results in this field. Among them, the most popular one is the arbitrated quantum signature (AQS) [11]. In the AQS scheme, there are three roles, signer, receiver and arbitrator. The signatory's private key can be reused to sign different messages. The receiver verifies the signed messages. The arbitrator plays a role as a trusted party who helps the other parties sign or verify a message. What is more, the potential disputations between the signatory and the receiver can be solved by the arbitrator. Therefore, it seems that the AQS scheme is more practical than the one without any arbitrator. Based on the frame work in [11], a lot of researches on AQS schemes were developed. For example, in a proxy AQS scheme [12–14], the original signer is represented by the proxy signatory to produce a signature. In the blind AQS scheme [15, 16], the signatory signs a blind message such that the signer does not know what message is signed. In a designated verifier AQS [17, 18], only the designated receiver can verify the quantum signature.

However, although many AQSs have been presented, the security analysis of most AQSs is not perfect. There is not any security model in most of AQSs. The security of these existing schemes against forgery under chosen-message attacks(FU-CMA) cannot be formally deduced as the basic quantum mechanics theories. This means the security of these schemes against forgery under chosen-message attack cannot be guaranteed by the basic quantum mechanics theories. In fact, facing the quantum adversary's chosen-message attacks, many AQSs were broken soon after being proposed. For examples, Jiang et al. [19, 20] proposed the practical AQSs based on the locally indistinguishable orthogonal product states, which were relatively easier to prepare than the entangled quantum states. Unfortunately, their schemes were insecure, because the receivers could generate the forgeries by adaptively modifying the received messages and applying some unitary operations on the corresponding quantum signatures [21, 22]. The scheme in [23] had some special properties such as blind message and proxy delegation. However, Zhou et al. [24] demonstrated that if some Hadamard operations were adaptively performed on the quantum signature in [23] then the corresponding signature could be used to generate a new forgery. Recently,

Ding et al. [25] proved that the AQS scheme in [26] was insecure because a quantum adversary may transform the original signature to a forged signature on some new message by using the controlled-NOT operations. What's more, some similar chosen-message forgery attacks for the quantum signature schemes were proposed as well [27, 28]. Recently, Xin et al. presented the provably secure AQS based on the entanglement states in [31], which introduced the provable security idea of quantum signature. However, there is no formal security model in their scheme.

In this paper, a new AQS with security model is presented. The security of our AQS is formally proved under the security model. We prove the unforgeability of the proposed signature relies on the indistinguishability of the unknown quantum sequence. Furthermore, no partner needs to prepare entanglement state in our AQS. The proposed AQS also has better virtue in qubit efficiency. So, compared with the other similar AQSs, the security of our AQS can be supported by formal proof. It also has better practicability and efficiency than the similar AQSs.

The rest sections are organized as follows. Section 2 presents some preliminaries. We describe the proposed AQS in Sect. 3. In Sect. 4, we present the security proof of our AQS. The comparisons are showed in Sect. 5. The last section presents a brief conclusion.

2 Quantum one-way function

Definition 1 [10] We call a function F: $x \rightarrow |F_x\rangle$ as a quantum one-way function, if it satisfies: (1) Given x, it is easy to compute $|F_x\rangle$ within polynomial time; (2) Given $|F_x\rangle$, it is hard to invert x within polynomial time.

In this paper, we use "||" stands for the classical-bit connection. Let $k = (k_1, k_2, \cdots, k_l)$ be an l-bit string. Let $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $Y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ stand for Hadamard operation, identity operation and Y operation, respectively. Let the operator $Y^+ = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Assume that $f : \{0,1\}^* \rightarrow \{0,1\}^n, g : \{0,1\}^* \rightarrow \{0,1\}^n$ and $h : \{0,1\}^* \rightarrow \{0,1\}^n$ are three classical one-way hash functions with uniform outputs. In the following, based on the hash functions f, g and h, the key-controlled quantum one-way hash function is constructed.

Given$k$, define the key-controlled hash function as follows:

$$F_k(m) = \otimes_{i=1}^{n} H^{g_i} Y^{h_i} |f_i\rangle, \ \forall m \in \{0,1\}^* \tag{1}$$

where $f(k||m) = (f_1, f_2, \ldots, f_n)$, $g(k||m) = (g_1, g_2, \ldots, g_n)$ and $h(k||m) = (h_1, h_2, \ldots, h_n)$.

It is clear that, given m, it is easy to compute $F_k(m)$. However, Given $F_k(m)$, it is hard to invert m due to the one-way property of the hash function f. Therefore, the

function $F_k(.)$ can be seemed as a key-controlled quantum one-way hash function.

$$F_k : \{0,1\}^{l+} \rightarrow \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n,$$

which is controlled by the parameter key k. According to Eq. (1), it follows that the input of F_k includes the parameter k and message m. Therefore, the bit length of the input of F_k is at least l, while the qubit length of the output of F_k is n. It is necessary to require that $l - n >> 1$. This is because that, according to Holevo's theorem [35], no more than n bits of information can be extracted by measuring n qubits. Then, given $F_k(m)$, no more than n bits of information on the input can be extracted. Therefore, the probability of successfully guessing the key k remains small when $l - n >> 1$. That is, the probability of successfully guessing the key k is

$$p(k) = 1/2^{(l-n)} \rightarrow 0(1 \rightarrow \infty).$$

For example, if $l = 256$ and$n = 128$, it follows that$p(k) \approx 2.938735877055719 \times 10^{-39}$. Therefore, the parameter l can be set by the system according the security level.

3 The proposed AQS scheme

The AQS involves three partners: Trent (a trusted arbitrator), Alice (the signatory) and Bob (the signature receiver). The scheme contains three processes: initialization process, signing process and verification process.

3.1 Initialization process

Signatory Alice shares secret key $k = (k_1, k_2, \cdots, k_l)$ $(l > > n)$ with Trent by the secure quantum key distribution protocol (QKDP) [29]. Similarly, she shares secret keys $x = (x_1, x_2, \cdots, x_n)$ and $y = (y_1, y_2, \cdots, y_n)$ with the receiver Bob by the QKDP [29].

3.2 Signing process

The message $m \in \{0,1\}^*$ is signed by performing the following signing steps:

Sign-1. Alice computes the hash value $F_k(m)$ with the key-controlled quantum one-way hash function and her secret$k$:

$$F_k(m) = |M\rangle = \otimes_{i=1}^{n} |M_i\rangle. \tag{2}$$

Sign-2. Alice generates her signature $|S\rangle = \otimes_{i=1}^{n} |S_i\rangle$ by performing the controlled H operator and Y operator on each $|M_i\rangle$ with the secret keys x and y, where each

$$|S_i\rangle = Y^{x_i} H^{y_i} |M_i\rangle. \tag{3}$$

Sign-3. Alice generates sufficient decoy particles for eavesdropping detection. All decoy particles are picked randomly in $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$. Then, Alice inserts these decoy states into $|S\rangle$ randomly and records the location and state of every decoy state. After that, she obtains a non-orthogonal qubit string $|S_A\rangle$. Then, Alice sends $(m,|S_A\rangle)$ to Bob.

3.3 Verification process

The signed message is verified by the steps as follows:

Verify-1. While Bob receives Alice's $(m,|S_A\rangle)$, Alice publishes the information of all the decoy states in the qubit string $|S_A\rangle$ such as their states and locations. Bob measures all decoy states in $|S_A\rangle$ and compares the measurement results with the decoy states published by Alice. If the error rate of the measurement is higher than the threshold set by the communication system, the signature scheme should restart. If not, Bob obtains the signature $|S\rangle$ from the $|S_A\rangle$ by discarding all the decoy states.

Verify-2. Bob performs the key-controlled Hadamard operation and Y operation on all quantum states in $|S\rangle$ with the shared keys x and y and gets.

$$\left|M'\right\rangle = \otimes_{i=1}^{n}\left|M_i'\right\rangle, \tag{4}$$

where each

$$\left|M_i'\right\rangle = H^{y_i}\left(Y^{+}\right)^{x_i}|S_i\rangle. \tag{5}$$

Next, he generates sufficient decoy states for eavesdropping detection. Then, he inserts these decoy states into $\left|M'\right\rangle$ and gets $\left|M_B'\right\rangle$. Bob records the locations and states of all the decoy qubits. Finally, Bob sends $(m, \left|M_B'\right\rangle)$ to Trent.

Verify-3. After Trent receives Bob's $(m, \left|M_B'\right\rangle)$, Trent performs the eavesdropping check operations which are similar as those did in the step Verify-1. If the quantum channel is not eavesdropped, Trent obtains $\left|M'\right\rangle = \otimes_{i=1}^{n}\left|M_B'\right\rangle$ by discarding the decoy states. By using the key-controlled quantum hash function and the shared k, Trent computes $F_k(m)$. Theoretically, the quantum signature is valid only if

$$F_k(m) = \left|M'\right\rangle. \tag{6}$$

Then, to verify Eq. (6), Trent calculates $g(k||m) = (g_1, g_2, \ldots, g_n)$ and $h((k||m) = (h_1, h_2, \ldots, h_n)$. Then, he performs the key-controlled operations and gets $\left|f'\right\rangle = \otimes_{i=1}^{n}\left|f_i'\right\rangle$, where each $\left|f_i'\right\rangle = \left(Y^{+}\right)^{h_i}H^{g_i}\left|M_i'\right\rangle$. Next, he measures each $\left|f_i'\right\rangle$ with base $\{|0\rangle, |1\rangle\}$ and gets the measurement result $f_i' := \begin{cases} 0, \text{ if } \left|f_i'\right\rangle = |0\rangle \\ 1, \text{ if } \left|f_i'\right\rangle = |1\rangle \end{cases}$. Let $f' = \left(f_1', f_2', \cdots, f_n'\right)$. Trent calculates $f(k||m)$ and checks whether $f(k||m) = f'$. If $f(k||m) = f'$, Trent confirms Eq. (6) holds and publishes "True," and Bob accepts the signature. Or Trent publishes "False" and Bob rejects the signature.

On the other hand, after the information "True" is published, Trent stores (m, f') as the verification proof.

4 Security analysis

The correctness of our AQS is obvious. This section mainly presents the security analysis of the proposed AQS.

The security of the secret keys is analyzed in Sect. 4.1. The formal proof of unforgeability of the quantum signature is presented in Sect. 4.2.

4.1 The security of the secret keys

During initialization phase, signatory Alice generates secret keys k, x and y by performing QKD protocol such as the BB84 protocol in [29]. According to the research result in [30], it follows that the BB84 protocol should be unconditional secure. Therefore, there is no adversary who has the ability of breaking the secret keys of the signatory in initialization phase.

During the signing phase, the signatory Alice generates the signature by computing quantum hash function value and encrypting the quantum states. This means that the quantum signature must include some information of these keys. For a signing system, anyone including the quantum adversary can access to the system and get the signer's signature. A quantum adversary may adaptively ask polynomial quantum signatures from the signing system. He/She measures the quantum signatures so as to obtain some bits of the signer's keys. However, the security proof as follow shows that the AQS is information-theoretically secure so that it is impracticable for quantum adversary to deduce the secret information from the signature.

Suppose there is a quantum-adversary Eve (for example, the signature receiver Bob), who wants to get some information about the secret keys through message-signature pair. That means Eve should measure the quantum signatures. However, in the following, by computing the trace distance of density operators for different quantum signatures, the indistinguishability of the quantum signatures can be proved.

Theorem 1 Any quantum signature always has the same density operator.

Proof In our scheme, we use QKD protocol [29] to ensure the secret keys x and y are unconditionally secure during the system initialization. Assume$x$ and y have the uniform distribution. According to Eq. (3), for the adversary, the state of S_i depends on the distributions of the random x_i and y_i. Then, S_i can be seemed as mixed ensembles with distribution.

$$\begin{Bmatrix} |M_i\rangle & Y|M_i\rangle & H|M_i\rangle & YH|M_i\rangle \\ 1/4 & 1/4 & 1/4 & 1/4 \end{Bmatrix}.$$

A density operator is commonly used to represent the state of the mixed ensembles. Therefore, the state of S_i can be described as its density operator ρ_{S_i}. By Eq. (3), the density operator ρ_{S_i} of S_i is computed as below:

$$\rho_{S_i} = \frac{1}{4} \sum_{x_i, y_i \in \{0,1\}} Y^{x_i} H^{y_i} |M_i\rangle\langle M_i| H^{y_i} \left(Y^{+}\right)^{x_i}$$

$$= \frac{1}{4}\left(|M_i\rangle\langle M_i| + Y|M_i\rangle\langle M_i|Y^+ + H|M_i\rangle\langle M_i|H + YH|M_i\rangle\langle M_i|HY^+\right)$$
$$= \frac{I}{2}$$

Note that the signature $|S\rangle = \otimes_{i=1}^{n}|S_i\rangle$. Then, it follows that for any quantum signature, its density operator should be the same $\rho_S = \otimes_{i=1}^{n}\rho_{S_i} = \frac{I^{\otimes n}}{2^n}$.

According to the concept of indistinguishability for the classical private-key encryption [32], Yang et al. [33] defined the information-theoretic indistinguishability for a quantum private-key encryption scheme.

Definition 2 [33] A quantum private-key encryption scheme (G, E, D) is information-theoretically indistinguishable if, for every quantum circuit family $\{C_n\}$, for every positive polynomial $p(\cdot)$, for all sufficiently large n, and for every $x, y \in \{0,1\}^{\text{poly}(n)}$ (i.e., $|x| = |y|$),

$$\left|\Pr\left[C_n\left(E_{G(1^n)}(x) = 1\right)\right] - \Pr\left[C_n\left(E_{G(1^n)}(y) = 1\right)\right]\right| < 1/p(n),$$

where the encryption algorithm E should be a quantum algorithm, G is an internal coin tosser for the algorithm, and the ciphertexts $E(x)$,$E(y)$ are quantum states.

What is more, in [33], Yang et al. proved that the information-theoretical security of a quantum private-key encryption scheme depended on the distance of the density operators of cipher states.

Theorem 2 [33] For all plaintexts x and y, let the density operators of cipher states $E(x)$ and $E(y)$ be ρ_x and ρ_y, respectively. A quantum private-key encryption scheme is said to be information-theoretically indistinguishable if, for every positive polynomial $p(\cdot)$ and every sufficiently large n, $D(\rho_x, \rho_y) < 1/p(n)$.

A quantum signature scheme can be seemed as a quantum private-key encryption scheme. Therefore, according to Theorem 2, it follows Corollary 1, which can be used to prove the information-theoretical security a quantum signature scheme [31].

Corollary 1 [31] For any positive polynomial $p(.)$ and two different quantum signatures $|S\rangle$ and $|S^*\rangle$, if their trace distance $D(\rho_S, \rho_{S^*}) < \frac{1}{p(n)}$, the quantum signature scheme will be information-theoretically secure. This means no distinguishing algorithm can efficiently draw a distinction between quantum signatures $|S\rangle$ and $|S^*\rangle$.

Theorem 3 The proposed quantum signature has the information-theoretical security.

Proof According to Theorem 1, it follows that for any two different quantum signatures $|S\rangle$ and $|S^*\rangle$, their density operators are the same. This means $D(\rho_S, \rho_{S^*}) = 0$. Therefore, according to Corollary 1, it follows that the proposed quantum signature has the information-theoretical security. This means there is no any algorithm which can efficiently distinguish $|S\rangle$ and $|S^*\rangle$.

Theorem 3 shows that it is infeasible for Eve to get some useful information about the secret keys x and y by measuring and distinguishing the quantum signatures.

Theorem 4 For different inputs, the outputs of $F_k(\cdot)$ have the same density operator.

Proof Note the outputs of $F_k(\cdot)$ is $F_k(m) = |M\rangle = \otimes_{i=1}^{n}|M_i\rangle$. Assume the hash functions f,g and h have the uniform outputs. Note that f: $\{0, 1\}^* \rightarrow (f_1, f_2, \ldots, f_n)$, g: $\{0, 1\}^* \rightarrow (g_1, g_2, \ldots, g_n)$ and h: $\{0, 1\}^* \rightarrow (h_1, h_2, \ldots, h_n)$. For the adversary, because the distributions of the outputs $(f_1, f_2, \ldots, f_n)$, $(g_1, g_2, \ldots, g_n)$ and $(h_1, h_2, \ldots, h_n)$ are all uniform, each g_i, h_i and f_i $(i = 1, 2, \ldots, n)$ can randomly take the values of 0 and 1. Then, by Eq. (1), we can obtain the density operator of M_i.

$$\begin{aligned}\rho_{M_i} &= \frac{1}{8}\sum_{g_i,h_i,f_i\in\{0,1\}} H^{g_i}Y^{h_i}|f_i\rangle\langle f_i|\left(Y^+\right)^{h_i}H^{g_i}\\ &= \frac{1}{8}\sum_{f_i\in\{0,1\}}\left(|f_i\rangle\langle f_i| + Y|f_i\rangle\langle f_i|Y^+ + H|f_i\rangle\langle f_i|H + HY|f_i\rangle\langle f_i|Y^+H\right)\\ &= \frac{I}{2}\end{aligned}$$

It follows that $\rho_M = \otimes_{i=1}^{n}\rho_{M_i} = \frac{I^{\otimes n}}{2^n}$.

Theorem 5 The key-controlled hash value $F_k(m) = |M\rangle = \otimes_{i=1}^{n}|M_i\rangle$ is information-theoretically secure.

Proof It follows from Theorem 4 that, for any $m \neq m'$, $\rho_M = \rho_{M'} = \frac{I^{\otimes n}}{2^n}$. Therefore, $D(\rho_M, \rho_{M'}) = 0$. Therefore, the key-controlled hash value is information-theoretically secure.

In our scheme, the signature receiver Bob can get $|M\rangle$ the during the signature verification phase. However, Theorem 5 shows that $|M\rangle$ is information-theoretically secure. This means $|M\rangle$ is theoretically indistinguishable. Therefore, it is infeasible for Eve to get some useful information about $(f_1, f_2, \cdots, f_n)$, $(g_1, g_2, \cdots, g_n)$ and $(h_1, h_2, \cdots, h_n)$ by distinguishing $|M\rangle$. Note that $f(k||m) = (f_1, f_2, \ldots, f_n)$, $g(k||m) = (g_1, g_2, \ldots, g_n)$ and $h(k||m) = (h_1, h_2, \ldots, h_n)$, where f, g and h are the one-way hash functions. Without $(f_1, f_2, \cdots, f_n)$, $(g_1, g_2, \cdots, g_n)$ and $(h_1, h_2, \cdots, h_n)$, it's hard for Eve to obtain the secret key k from $|M\rangle$.

Moreover, in our scheme, the quantum channel is checked by using eavesdropping detection technology. The adversary's eavesdropping will disturb the decoy particles inserted into the quantum channel. Therefore, the adversary's eavesdropping will be detected by the partners.

4.2 Unforgeability

The security of most AQSs against forgery attack was analyzed without security model and formal security proof. In this section, we formally prove the unforgeability of our AQS with security model under chosen-message attack.

4.2.1 Random oracle F_k

In our scheme, the key-controlled quantum hash function F_k is used. According to Theorem 4, it follows the output of F_k can be uniform if the hash functions f, g and h have the uniform distributions. Then, in the security analysis as follows, F_k is seemed as a random oracle mapping each possible query $m \in \{0,1\}^*$ to a fixed random response $|M\rangle = \otimes_{i=1}^{n} |M_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n$.

4.2.2 Existential unforgeability

To our knowledge, most of the forgery attacks are FU-CMA. Simply speaking, the adversary generates the forgery based on the received quantum signatures. As discussed in Sect. 1, although many AQSs have been presented, their security against FU-CMA cannot be formally proved. No sufficient proof can prove that their security depends on the basic quantum mechanics theories. Some AQSs have been proved to be insecure against FU-CMA.

This section presents the formal security proof of the new AQS against FU-CMA. Its security can be guaranteed by the basic quantum mechanics principle, the indistinguishability of the unknown quantum state.

For an AQS, the FU-CMA game can be described as follows:

Initialization(l) $\rightarrow$ ($\mathbf{k}_r$, k_T). Given the security parameter l as input, this algorithm outputs the private keys **($\mathbf{k}_r$, k_T).** That is, by performing the unconditionally secure QKDP, the challenger shares private keys k_r and k_T with the receiver and the trusted arbitrator, respectively.

In the game, the signer Alice plays the role of challenger:

Signature query($\mathbf{m_i}$) $\rightarrow$ σ_{m_i}. Given a message $m_i \in \{0,1\}^*$ as input, this algorithm outputs a quantum signature σ_{m_i}. That is, the adversary can adaptively select polynomial messages m_1, m_2,…, $m_{p(n)}$ for signature query, where $p(.)$ is a polynomial. For the message m_i submitted by the adversary, the challenger executes the signature generation algorithm and produces the signature σ_{m_i}. Then, the challenger sends the signature to the adversary.

In the game, the signature receiver Bob plays the role of adversary:

Forgery. After the polynomial signature queries, the adversary Ad outputs a forged signature σ_{m^*} for some message m^*.
If σ_{m^*} is valid and the signature on m^* has never been queried before, the adversary wins the game. Let $FogWin_{Ad}$ be the probability that adversary Ad wins the game.

Definition 3 A quantum forger Ad (q_S, q_F, ε)-breaks a quantum signature scheme if Ad wins the FU-CMA game with the probability at least ε by querying at most q_S signatures to the signature oracle and at most q_F queries to the random oracle. An AQS scheme is (q_S, q_F, ε)-existentially secure against UF-CMA if no forger can (q_S, q_F, ε)-break it.

Theorem 6 Our AQS is (q_S, q_F, ε)-secure against UF-CMA in the random oracle model. No forger can (q_S,q_F,ε)-break it.

Proof Assume there is a quantum adversary Ad, who can (q_S, q_F, ε)-break our AQS. We construct the FU-CMA game between a challenger Ch and the adversary Ad. To simplify the game description, in the following, let the signer Alice play role of challenger Ch. Bob plays the role of adversary Ad, who masters more quantum sources than the outside adversary. Trent is a trusted arbitrator. Now, Alice receives an unknown particle sequence $N = (N_1, N_2, \ldots, N_n)$, whose state is $|N\rangle = \otimes_{i=1}^{n}|N_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}^n$. Alice's goal is to accurately distinguish the unknown quantum sequence N.

Initialization. It is the same as that described in Sect. 3.1.

Random oracle query. Assume that the random oracle F_k (please refer to Sect. 4.2.1) can be queried at most q_F times. Ch keeps a list RO-List, which is initially empty. If the oracle is queried about the message m_j, the following steps are performed.

Ch checks the RO-List.

If RO-List has contained a record (m_j, b_j, r_j, w_j) on m_j, where $b_j = 0$, $r_j = \left(r_j^1, r_j^2, \cdots, r_j^n\right) \in \{0,1\}^n$ and $w_j = \left(w_j^1, w_j^2, \cdots, w_j^n\right) \in \{0,1\}^n$, Ch computes $\left|N^j\right\rangle = \otimes_{i=1}^{n} H^{r_j} Y^{w_j}|N_i\rangle$ and outputs $\left|N^j\right\rangle$ as the answer.

If RO-List has contained a record (m_j, b_j) on m_j, where $b_j = 1$, according to Eqs. (1–2), Ch computes $\left|N^j\right\rangle = F_k(m_j) = |M\rangle = \otimes_{i=1}^{n}|M_i\rangle$ and outputs $\left|N^j\right\rangle$ as the answer.

If RO-List does not contain any record on m_j, Ch flips a random coin with the result $b_j \in \{0,1\}$ such that the probability $p(b_i = 0) = \frac{1}{q_S+1}$. If $b_j = 0$, Ch randomly generates two n-tuples $r_j = \left(r_j^1, r_j^2, \cdots, r_j^n\right) \in \{0,1\}^n$ and $w_j = \left(w_j^1, w_j^2, \cdots, w_j^n\right) \in \{0,1\}^n$, computes $\left|N^j\right\rangle = \otimes_{i=1}^{n} H^{r_j} Y^{w_j}|N_i\rangle$ and outputs $\left|N^j\right\rangle$ as the answer. Then, Ch adds the record (m_j, b_j, r_j, w_j) to the RO-List. If $b_j = 1$, according to Eqs. (1–2), Ch computes $\left|N^j\right\rangle = F_k(m_j) = |M\rangle = \otimes_{i=1}^{n}|M_i\rangle$ and outputs $\left|N^j\right\rangle$ as the answer. Then, Ch adds the record (m_j, b_j) to the RO-List.

Signature oracle query. Assume that the signature oracle can be queried at most q_S times. When the signature oracle is queried on m_j, Ch queries the random oracle on m_j. If the record on m_j in RO-List is (m_j, b_j, r_j, w_j), it means that $b_j = 0$. In this case, Ch outputs '*Fail*'. If the record on m_j in RO-List is (m_j, b_j), it means that $b_j = 1$. In this case, Ch performs the signing steps described in Sect. 3.2 and outputs the valid quantum signature $(m_j, |S\rangle)$ as the answer.

Assume that the signature oracle successfully outputs all the answers without 'Fail,' and after the querying phase, Ad generates a forgery $(m^*, |S^*\rangle = \otimes_{i=1}^{n}\left|S_i^*\right\rangle)$ which can pass the signature verification, while the signature oracle has never output the AQS on m^*. Note that before generating the forgery $(m^*, |S^*\rangle)$, Ad has to query the random oracle on m^*. If the record on m^* in RO-List is $\left(m^*, b_j^*, r_j^*, w_j^*\right)$, the game outputs 'Success,' or it outputs 'Fail.'

If the game outputs 'Success,' it follows that the forgery satisfies the signature verification Eqs. (4–6). That is $F_k(m^*) = \otimes_{i=1}^{n} H^{y_i}\left(Y^+\right)^{x_i}\left|S_i^*\right\rangle$, where $F_k(m^*) = |N^*\rangle$ is the output of the random oracle in the game. Therefore, according to the output of the random oracle in the game and Eqs. (4–6), it follows that

$$\left|N^*\right\rangle = \otimes_{i=1}^{n} H^{r_i^*} Y^{w_i^*}|N_i\rangle = \otimes_{i=1}^{n} H^{y_i}\left(Y^+\right)^{x_i}\left|S_i^*\right\rangle. \tag{7}$$

According to Eq. (7), it follows that

$$|N\rangle = \otimes_{i=1}^{n}|N_i\rangle = \otimes_{i=1}^{n}\left(Y^{+}\right)^{w_i^*} H^{r_i^* \oplus y_i}\left(Y^{+}\right)^{x_i}\left|S_i^*\right\rangle, \tag{8}$$

in which $|S^*\rangle = \otimes_{i=1}^{n}\left|S_i^*\right\rangle$ is the forgery generated by the adversary, who masters the generation process of each $\left|S_i^*\right\rangle$. Therefore, by performing the game, the state of the unknown quantum sequence N can be accurately distinguished as $|N\rangle$ described in Eq. (8). Therefore, based on Eq. (8) and the knowledge of Ad's (the generation process of each $\left|S_i^*\right\rangle$), we can master the evolution history of $|N\rangle$, which conflicts with the indistinguishability of the unknown particle sequence $N = (N_1, N_2, \ldots, N_n)$.
Now, we analysis the probability of obtaining the evolution history of $|N\rangle$. Note that the adversary can (q_S, q_F, ε)-break our quantum signature scheme. This means that the following conditions should be satisfied. (i) The signature oracle successfully outputs all the answers. (ii) The adversary successfully generates a forgery $(m^*, |S^*\rangle = \otimes_{i=1}^{n}\left|S_i^*\right\rangle)$ which can pass the signature verification. (iii) The record on m^* in RO-List is $\left(m^*, b_j^*, r_j^*, w_j^*\right)$. The conjunction of these occurs with the probability

$$p = \left(1 - \frac{1}{1+q_S}\right)^{q_s} \cdot \varepsilon \cdot \frac{1}{1+q_S}, \tag{9}$$

according to which we can get $p \geq \frac{\varepsilon}{eq_S}$, where e is natural constant approximately equal to 2.718. This means that if ε is non-negligible probability, the sequence N can be accurately discriminated with a non-negligible probability p as well, which conflicts with the indistinguishability of N. Therefore, our AQS scheme is (q_S, q_F, ε)-secure against UF-CMA.

4.2.3 Non-repudiation

Section 4.2.2 shows the proof that the outside adversaries including Bob cannot forge the signature. Note that Trent is a trusted arbitrator, who will not forge any of the signer's signatures. Therefore, Alice and Bob cannot refuse a valid signature because of the property of unforgeability.

In our scheme, after the AQS verification, Trent stored (m, f') for each valid AQS. If Alice denies the generation of AQS on m, Trent can verify whether $f(k||m) = f'$. If $f(k||m) = f'$, it follows that Alice has produced the AQS for the receiver, since only Alice shares the secret k with the arbitrator. What is more, Bob cannot refuse that he has ever get the AQS on m, since the signature-proof (m, f') is derived from $(m, \left|M_B'\right\rangle)$, which was sent by Bob.

5 Comparisons

First, in our scheme, the security model for AQS under chosen-message attack is introduced. Our AQS can be proved to be secure against FU-CMA with formal security

Table 1 Comparisons of the similar schemes

Schemes	Have security model	Provably secure	Need entanglement particles	Qubit efficiency (%)
[25]	No	No	Yes	33
[31]	No	Yes	Yes	50
Ours	Yes	Yes	No	50

proof. In [25], neither security model no provable security proof was presented to support the corresponding security analysis results. In [31], the security of the scheme was proved without any security model.

Second, in [25, 31], the signer has to prepare the entangled particles so as to sign a message. In our scheme, there is not any entangled particle used to generate signatures.

Finally, we analysis the qubit efficiency of the similar schemes. The qubit efficiency [34] is defined as $\delta = \frac{\delta_1}{\delta_2}$, where $\delta_1(\delta_2)$ is the count of transmitted bits (qubits) in the protocol. (Decoy states for detecting eavesdropping are ignored.) In our scheme, $2n$ qubits are transmitted, while n-bit message is authenticated. Then, the qubit efficiency of our scheme is $\delta = \frac{n}{2n} = 50\%$. The qubit efficiency of the similar schemes is showed in Table 1 as follows.

6 Conclusions

There is not any security model in most of AQSs. Their security cannot be formally proved. This means no sufficient proof can support their security against FU-CMA.

Then, the security model for AQS under FU-CMA was introduced. We propose a new AQS with security model. The security of the proposed quantum signature against FU-CMA can be proved under random oracle.

The proposed AQS can be used to sign bit message without using any entangled state.

The qubit efficiency of our AQS achieves 50%.

Table 1 shows the advantages of the proposed AQS.

Acknowledgements This work is supported by the National Natural Science Foundation of China (Grant No.62272090) and the Key Scientific Research Project of Colleges and Universities in Henan Province (Grant No.22A413010). In addition, we are grateful to the anonymous reviewers who have helped to improve the paper.

Author's contribution The scheme and security model were proposed by XX, TZ and LS. The security of the scheme was analyzed by HL and XX. The efficiency analysis was presented by CL and FL. The draft of the manuscript was written by XX and TZ. All authors read and approved the final manuscript.

Data availability The manuscript has no associated data.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Diffie, W., Hellman, M.: New direction in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
2. Chaum, D., Heyst, E.: Group signatures. In: Advance in Cryptology- EUROCRYPT'91, pp. 257–265. Springer, Berlin (1991)
3. Mambo, M., Usuda, K., Okamoto, E.: Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundam. **E79-A**(5), 1338–1354 (1996)
4. 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)
5. Rastegari, P., Berenjkoub, M., Dakhilalian, M., et al.: 2019 Universal designated verifier signature scheme with non-delegatability in the standard model. Inform. Sci. **479**, 321–334 (2019)
6. Chaum, D.: Blind signatures for untraceable payments. In: Advance in Cryptology-CRYPTO'82, pp. 199–203. Plenum, New York (1983)
7. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput. **26**(5), 1484–1509 (1997)
8. Wang, B., Hu, F., Yao, H., et al.: Prime factorization algorithm based on parameter optimization of ising model. Sci. Rep. **10**(1), 1–10 (2020)
9. Huang, Y., Su, Z., Zhang, F., et al.: Quantum algorithm for solving hyper elliptic curve discrete logarithm problem. Quantum Inf. Process. **19**(62), 1–17 (2020)
10. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv: quant-ph/0105032 (2001)
11. Zeng, G.H., Keitel, C.H.: Arbitrated quantum-signature scheme. Phys. Rev. A **65**(4), 042312 (2002)
12. Liang, X.Q., Wu, Y.L., Zhang, Y.H., et al.: Quantum multi-proxy blind signature scheme based on four-qubit cluster states. Int. J. Theor. Phys. **58**(1), 31–39 (2019)
13. Qin, H., Tang, W.K.S., Tso, R.: Efficient quantum multi-proxy signature. Quantum Inf. Process. **18**(2), 53 (2019)
14. Zheng, T., Chang, Y., Yan, L.L., et al.: Semi-quantum proxy signature scheme with quantum walk-based teleportation. Int. J. Theor. Phys. **59**(10), 3145–3155 (2020)
15. Xia, C., Li, H., Hu, J.: A semi-quantum blind signature protocol based on five-particle GHZ state. Eur. Phys. J. Plus **136**(6), 633 (2021)
16. Chen, B., Yan, L.: Quantum and semi-quantum blind signature schemes based on entanglement swapping. Int. J. Theor. Phys. **60**(10), 4006–4014 (2021)
17. Zhang, Y., Xin, X., Li, F.: Secure and efficient quantum designated verifier signature scheme. Mod. Phys. Lett. A **35**(18), 2050148 (2020)
18. Xin, X., Wang, Z., Yang, Q.: Quantum designated verifier signature based on Bell states. Quantum Inf. Process. **19**(3), 79 (2020)
19. 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)
20. 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)
21. Xin, X., He, Q., Wang, Z., et al.: Security analysis and improvement of an arbitrated quantum signature scheme. Optik **189**, 23–31 (2019)
22. He, Q., Xin, X., Yang, Q.: Security analysis and improvement of a quantum multi-signature protocol. Quantum Inf. Process. **20**(1), 26 (2021)
23. 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**(6), 1999–2008 (2019)
24. 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**(2), 465–473 (2020)
25. 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)

26. Zheng, X.Y., Kuang, C.: Arbitration quantum signature protocol based on XOR encryption. Int. J. Quantum Inf. **18**(5), 2050025 (2020)
27. Gao, F., Qin, S.J., Guo, F.Z., et al.: Cryptanalysis of the arbitrated quantum signature protocol. Phys. Rev. A **84**(2), 022344 (2011)
28. Yang, C.W., Liu, J., Tsai, C.W., et al.: Cryptanalysis of a semi-quantum bi-signature scheme based on w states. Entroy **24**(10), 1048 (2022)
29. Bennett C.H., Brassard G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, New York (1984)
30. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**(2), 441–444 (2000)
31. Xin, X., Ding, L., Zhang, T., et al.: Provably secure arbitrated-quantum signature. Quantum Inf. Process. **21**(12), 390 (2022)
32. Goldreich, O.: Foudations of Cryptography: Basic Applications. Publishing House of Electronics Industry, Beijing (2004)
33. Yang, L., Xiang, C., Li, B.: Quantum probabilistic encryption scheme based on conjugate coding. China Commun. **10**(2), 19–26 (2013)
34. Hwang, T., Lee, K.C.: EPR quantum key distribution protocols with 100% qubit efficiency. IET Inf. Secur. **1**(1), 43–45 (2007)
35. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information, pp. 531–536. Cambridge University Press, Cambridge (2000)