Hindawi
Security and Communication Networks
Volume 2022, Article ID 8954767, 13 pages
https://doi.org/10.1155/2022/8954767

Research Article

New Constructions of Existential Unforgeable Aggregate Signature Scheme from CSP

Bo Mi,[1] **Yongxing Zou**,[1] **Darong Huang**,[1] **Yang Liu**,[1] **and Lu Chen**[2]

[1]*School of Information Science and Engineering, Chongqing Jiaotong University, Chongqing, China*
[2]*Naval University of Engineering, Wuhan, China*

Correspondence should be addressed to Yongxing Zou; yongxing_zou1998@163.com

Received 29 July 2022; Revised 8 September 2022; Accepted 22 September 2022; Published 9 November 2022

Academic Editor: Lei Liu

In future, hundreds of years of mathematical problems that the security of public key cryptography algorithms rely on may be defeated by quantum algorithms. How can a digital signature scheme gracefully balance security and efficiency? This study uses the conjugate search problem and the left self-distributive system to combine and uses the RSA-like algorithm as the underlying structure to propose a new aggregated signature scheme. We, through the EUF game, under the random metaphor model, prove that the security of the scheme satisfies the adaptation unforgeability under selective message attack, the scheme can be finally reduced to the discrete logarithm problem or large prime number decomposition problem. In addition, we can achieve anti-quantum attack and exhaustive attack by performing matrix calculations on the message, defining and changing the structure of the matrix by encoding, and setting thresholds for the matrix dimension and the length of the private key. In terms of efficiency, the message signature implementation is linear compared with the expansion rate in terms of storage and computing overhead, and the generation and verification of the final signature pair have nothing to do with the number of users. In addition, the length of the signature is fixed and the size is only the length of a single group, which effectively reduces the generation of public and private key pairs and saves a lot of storage space. The storage space and computational complexity are also effectively improved compared with other solutions.

1. Introduction

Throughout the ages, information security has played an important role in both ordinary life and military strategy. Cryptography provides the theory and technical support of information security and meets the four requirements of information security from the two aspects of data encryption and digital signature: confidentiality means information content cannot be accessed by unauthorized persons. Integrity means no information modification during transmission and storage. Authentication means identification and authentication service technology applied to both the entity and the information itself. Nonrepudiation means users cannot deny their existing actions and commitments [1–3]. Among them, data encryption can realize the confidentiality of data, and a digital signature can realize the integrity, authentication, and nonrepudiation of information. The digital signature is a digital simulation of a handwritten signature. With the advent of the information age, most standard protocols, and software support digital signatures, at present, many countries have legislation that stipulates that digital signatures and handwritten signatures have the same legal effect. In 1978, Rivest et al. realized the first public-key encryption scheme [4] for the large integer factorization problem, and at the same time, using this public-key encryption scheme, we realized the first digital signature scheme, namely, the famous RSA scheme. Since the proposal of this scheme, the research on digital signatures has always been one of the main research topics and hotspots in the field of cryptography. Digital signatures often involve multiuser scenarios: on the one hand, the signature itself needs to be signed by multiple users; on the other hand, although the signature is generated by a single user, security in a multiuser environment needs to be considered. Boneh

et al. first proposed the concept of aggregated signatures in 2003 [5] and constructed the first aggregated signature scheme using pairings on elliptic curves. Roughly speaking, the aggregated signature σ is the synthesis of n different signatures by n users to different pairs of documents $m_1, m_2, \ldots, m_n$ into a single signature σ, which reduces not only the storage space requirements for signatures but also the requirements for transmission network bandwidth. At the same time, the verification of multiple signatures is simplified into one verification, which reduces the workload of the verifier. Especially, in some computing resources and a large number of fast authentication situations at the same time, such as online ticket purchases, virtual currency, safety routing protocol, and vehicle ad hoc networks, whether it is the Spring Festival transport of 1.4 billion people in China or the routing topology in a certain area, it has a greater application demand for short-signed fast algorithms. In the direction of protecting user data privacy and communication security, even 6 G networks with endogenous security face many problems, such as AI-induced concerns about security and privacy issues, including data security, AI model and algorithm security, and malicious use of AI technology. Traditional computational complexity-based cryptographic mechanisms (such as encryption, authentication, authorization, signature, and privacy protection) will remain the primary method for maintaining network security and data privacy. However, due to the characteristics of 6 G networks, lightweight and efficient encryption and signature mechanisms are very popular. The combination of 6 G and blockchain, through the application of encryption algorithms such as aggregate signature and ring signature in the data structure, makes the data highly anonymous and improves the efficiency of authentication, which is also a promising solution. The achievement of these goals requires an efficient and secure signature algorithm as the underlying technical support. In the near future, quantum computers are expected to break the modern public key cryptosystem. Postquantum cryptography must be an important means to protect future information security. The past cryptosystems cannot be abandoned. How to migrate from public key cryptosystems to postquantum cryptosystems has become a hot topic.

1.1. Contributions. Given the problems of existing schemes such as excessive storage signature overhead, low signature verification efficiency, insufficient security, and inability to achieve antiquantum computing in the future, we propose a new scheme; the main contributions of this study are summarized as follows:

(1) This study uses the combination of RSA, CSP (conjugate search problem), and LD (left self-distributive system) to construct a new aggregated signature scheme, and we utilize the RSA-like as the underlying structure of the scheme, which can eventually be reduced to the DLP problem or the large prime number decomposition problem because the RSA algorithm is based on the large prime number decomposition problem.

(2) In terms of security, the proposed scheme satisfies that EUF-CMA can resist existential forgery attacks under adaptive selection messages. Through the EUF game, adversary A uses his scheme to attack the challenger as a subroutine, designs computational targets for adversary B, and then defines the advantage that B can solve for a given RSA-like scheme to achieve the proof.

(3) In terms of efficiency, since all messages are encoded as low-dimensional matrices with a certain regularity, and with the help of the characteristics of the CSP-LD system, the signatures of all signers will be synthesized into the final unique signature through calculation.As a result, the signature storage and verification become more efficient. The overhead is greatly reduced, the expansion rate of message signature implementation is linear compared with the storage and computing overhead, and the length of the final aggregated signature is fixed, which saves the maximum amount of signed storage space without losing accuracy.

(4) What is more prominent is that the scheme we propose can customize the format of the encoded message matrix. By setting the system parameters to reach a certain threshold, it can achieve antiquantum attacks. Other problems using RSA or DLP include digital signature schemes based on pairing problems, neither can resist the quantum computer attack under Shor's algorithm.

2. Related Work

How to construct efficient and secure aggregated signatures has always been highly concerning for cryptographers. Hashimoto and Ogata [6] proposed the first unrestricted and compact aggregated signature scheme, in which the signature size is constant, and the generated pair signatures can have different information states and can aggregate any combination of signatures. Iwasaki et al. [7] extended from the two perspectives of structured signature and identity-based signature and constructed an identity-based structured aggregated signature scheme, and the security of the scheme will not be reduced due to the ability of the adversary. It can successfully defend against switching attacks (CCS 2007, Boldyreva et al. [8]) and reordering attacks (ISPEC 2007, Shao [9]). In recent years, the combination of signature scheme and blockchain technology [10–12], federated learning technology [13], 6G network [14], homomorphic learning [15], network routing protocol [16], edge computing [17], vehicular ad hoc networks [18], and software-defined vehicular network [19–21] by applying signature algorithms and encryption algorithms to the experimental scheme to further strengthen the security of the scheme and improve the privacy protection capability of the scheme is also a hot topic. In the blockchain, the digital signature is one of the three basic technologies, and its importance is self-evident. The blockchain mainly uses digital signatures to control permissions, identify the legal

identity of transaction initiators, and prevent malicious nodes from impersonating. Coincidentally, the distributed and decentralized edge nodes inherent in the 6 G network allow blockchain technology to be used to improve the endogenous security performance of 6 G, based on blockchain technology to achieve what is considered a promising solution in the field of data security and privacy in 6 G networks. Data have a high level of anonymity by applying encryption algorithms such as aggregate signature signatures and ring signatures in the data structure. In edge computing, federated learning, and homomorphic learning, edge computing processes and applies data to the nearest computing facility to protect its privacy or federated learning uses other remote data and protects the privacy of remote data, and at the same time collaborative modeling, or the cloud computing model based on homomorphic encryption, solves the problem of users trusting cloud service providers not to steal or even user data and to achieve data confidentiality and computability. Verifying the identity legitimacy of a user or terminal based on a digital signature is both basic and necessary work. SDVN (software-defined virtual network) is a new type of VANET (vehicle ad hoc network), a promising networking paradigm, that can provide intelligent information exchange by separating network management and data transfer. For such applications that combine vehicles with networks, frequently changing topology networks, real-time routing calculations, and efficient service requests all play a crucial role in vehicle networks. Before designing a routing strategy for vehicles in these operations, it is undoubtedly a wise move to use an aggregated signature scheme that is fast and can protect its identity privacy to verify the legitimacy of vehicle units. Domestic Li et al. [22] constructed an efficient aggregated signature scheme under the certificateless public-key cryptosystem based on bilinear pairing, and the signature length of the scheme is only two group elements. Only 4 pair operations (of constant magnitude) and n scalar multiplication operations are required in signature verification, which has a fast signature verification algorithm and fast transmission efficiency. Zhou et al. [23] proposed two certificateless aggregated signature schemes that do not use bilinear mapping for different network environments. However, due to the long aggregate signature length of Scheme I, it can only be used in a network environment with high bandwidth and the final signature length is positively correlated with the number of users, Scheme II has a shorter signature length, and the length has nothing to do with the number of users and will be used in a network environment with low bandwidth. Whether the security proofs of these two schemes have existential unforgeability under adaptive chosen message attack remains to be further analyzed. At present, most aggregated signature schemes are constructed according to the pairings on elliptic curves. For example, Yang et al. [24], aiming at the problems of privacy leakage and low signature verification efficiency in VANET (vehicular ad hoc network), combined with identity-based cryptography and aggregated signature technology, designed a message authentication scheme for VANET to improve the security of the system and the efficiency of road traffic.

However, there are still many deficiencies in the pairing-based scheme: one is that the hardware devices currently implemented are all oriented towards RSA and DLP (discrete logarithm problem), and the pairing-based cryptography scheme still has a long way to go before it can be applied in reality. Another is that the pairing problem was not introduced into cryptography for research until 2000. Unlike RSA and DLP problems, hundreds of years of research have made them well-understood in the cryptography community. Therefore, most of the current digital signature schemes are based on the discrete logarithm problem and the RSA problem. For example, many people learn from the ideas of Bellare and Neven [25] and propose RSA-based identity-based sequential signature schemes, which need to be further strengthened and improved in terms of the storage efficiency of signatures and whether they can achieve EUF-CMA (existential unforgeability under adaptive chosen message attack) security. What makes us more motivated is that almost no one aggregates signatures based on RSA.

More importantly, with the development of quantum computers, the abovementioned mathematical problems that the security of public key cryptographic algorithms depends on can be solved by efficient quantum algorithms [26, 27]. As the underlying mathematical problems are solved, including discrete logarithms (elliptic curve versions) and large integer factorization, all these public key cryptographic algorithms will no longer be secure, which directly affects Diffie-Hellman, Elliptic Curve, RSA, and those currently used algorithms. In 2016–2017, NIST focused on the solicitation of the following three categories of postquantum cryptographic algorithms: encryption, key exchange, and digital signatures. Among the 69 "complete and suitable" candidate drafts, postquantum cryptographic algorithms constructed by the following 4 mathematical methods are mainly included lattice-based, code-based, multivariate-based, and hash-based. The scheme discussed in this study does not have a self-made wheel, but through the fusion of CSP and matrix, using the encoding of the message to achieve antiquantum attacks, the specific form is in the follow-up content.

3. Preliminaries

Before introducing definitions, let us review the concept of groups.

When an algebraic system has a certain operation $\langle G, * \rangle$, $*$ is a binary operation. When $*$ satisfies the following properties, we call the algebraic system a group, in which $\langle G, * \rangle$ is simply denoted as G:

(1) Closedness: it means for $\forall a, b \in G$ satisfying $a * b \in G$.

(2) Unitary: it means, for $\forall a \in G, \exists e$, there are existing $a * e = e * a = a$. At the same time, we call e the identity element of $\langle G, * \rangle$.

(3) Inverse element exists: it means, for $\forall a \in G, \exists b \in G$, there are existing $a * b = b * a = e$. Then, b is called the inverse of a, denoted as a^{-1}.

(4) Associativity: it means $\forall a, b, c \in G$ satisfying $(a * b) * c = a * (b * c)$.

An algebraic system $\langle G, * \rangle$ is called a semigroup if it only satisfies closure and associativity. For example, multiplication and addition of real numbers. If the $*$ operation in an algebraic system $\langle G, * \rangle$ also satisfies the commutative law, that is, $\forall a, b \in G$ has $a * b = b * a$, then $\langle G, * \rangle$ is called a commutative group, also called an Able group.

Note that not all elements in G have inverses. At the same time, $a^n = a * * * a$, n times, and $a^{-n} = b * * * b$, n times, where $n > 1$.

Let G^{-1} be the set of all invertible elements belonging to G, expressed as follows:

$$G^{-1} = \{a \in G: \exists b \in G, \text{ so that } a * b = b * a = e\}. \tag{1}$$

The so-called CSP problem can be roughly explained in the group: there is a group G, where $a \in G$ and $x \in G^{-1}$; there must be an element $b \in G$; a and b are isomorphic so that $b = xax^{-1}$; we say that, for the element x, a, and b are conjugated.

Definition 1 (conjugacy search problem, CSP). Suppose G is a noncommutative group, a and b are two elements belonging to G, denoted as $a, b \in G$, and the unknown x is an element in G^{-1}, denoted as $x \in G^{-1}$, satisfying $b = xax^{-1}$. The so-called CSP (conjugate search problem) problem in the noncommutative group G refers to finding another x' in G^{-1}, denoted as $x' \in G^{-1}$, so that $b = x'ax'^{-1}$, where x' does not need to be exactly the same as x.

Lemma 1. *The same applies to transforming a and b into matrix form in the above search problem. For example, write a and b as the simplest two-dimensional upper triangular matrix:*

$$a = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}, b = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix}. \tag{2}$$

Satisfying $b = xax^{-1}$,

$$b = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ 0 & x_3 \end{pmatrix} \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix} \begin{pmatrix} \frac{1}{x_1} & -\frac{x_2}{x_1 x_3} \\ 0 & \frac{1}{x_3} \end{pmatrix}. \tag{3}$$

CSP (conjugate search problem) problem in the noncommutative group G refers to finding another x' in G^{-1}, denoted as $x' \in G^{-1}$, so that $b = x'ax'^{-1}$, where x' does not need to be exactly the same as x:

$$x' = \begin{pmatrix} x_1' & x_2' \\ 0 & x_3' \end{pmatrix}. \tag{4}$$

Theorem 1. *If the matrix A is invertible, then the inverse matrix of A is unique, and the proof is omitted.*

Definition 2 (left self-distributive system, LD [28]). W is a nonempty subset and F is a complete and closed function satisfying F: $W \times W \longrightarrow W$; we denote $F(a, b)$ as $F_a(b)$. If F satisfies the following formula, then we call $F(\cdot)$ a left self-distributive system or LD system for short:

$$F_r(F_s(p)) = F_{F_r(s)}(F_r(p)), \quad (\forall p, r, s \in W). \tag{5}$$

If we consider $F_r(s)$ as a binary operation $r * s$, the above expression becomes

$$r * (s * p) = (r * s) * (r * p). \tag{6}$$

The operator $*$ is left self-distributive.

Definition 3 (CSP-LD system [29]). Assuming that G is a noncommutative group, the binary function F satisfies the following conjugation operations:

$$F: G^{-1} \times G \longrightarrow G, \quad (a, b) \longrightarrow aba^{-1}. \tag{7}$$

Then, $F(\cdot)$ is a CSP-LD system.

The proof is as follows:

$$\begin{aligned} F_r(F_s(p)) &= F_r\left(sps^{-1}\right) = rsps^{-1}r^{-1} \\ &= rsr^{-1} \cdot rpr^{-1} \cdot rs^{-1}r^{-1} \\ &= rsr^{-1} \cdot rpr^{-1} \cdot \left(rsr^{-1}\right)^{-1} \\ &= F\left(rsr^{-1}, rpr^{-1}\right) = F_{F_r(s)}(F_r(p)). \end{aligned} \tag{8}$$

The CSP-LD system also has some very simple but very useful properties in the field of cryptography. A few are listed below, and readers can prove it by themselves.

Property 1: $F_a(a) = a, a \in G^{-1}$

Property 2: $F_a(b) = c \Leftrightarrow F_{a^{-1}}(c) = b, a \in G^{-1}, b \in G$

Property 3: $F_a(bc) = F_a(b)F_a(c), a \in G^{-1}, b, c \in G$

The power-law property of F in the CSP-LD system will be described in detail below.

Lemma 2. *Suppose a and b are given and fixed, $a \in G^{-1}$ and $b \in G$. Then, for any three integers m, s, t, as long as $m = s + t$ is satisfied, there must be the following formula:*

$$\begin{aligned} &F_a(b^m) = F_a(b^s)F_a\left(b^t\right) = F_a^m(b) \\ &F_{a^m}(b) = F_{a^s}(F_{a^t}(b)) \end{aligned}. \tag{9}$$

The first proof of the formula is as follows:

$$\begin{aligned} F_a(b^m) &= ab^m a^{-1} = ab \cdots\cdots ba^{-1} \\ &= aba^{-1} \cdot aba^{-1} \cdots\cdots aba^{-1} \\ &= \left(aba^{-1}\right)^m = F_a^m(b). \end{aligned} \tag{10}$$

The second proof of the formula is as follows:

$$F_{a^m}(b) = a^m b a^{-m} = a^s a^t b a^{-t} a^{-s} = a^s F_{a^t}(b) a^{-s} = F_{a^s}\left(F_{a^t}(b)\right). \tag{11}$$

The two formulas are of great help to our follow-up content. One satisfies the internal and external exchange of power, transforming the exponent of the variable into the exponent of the function, and the other satisfies the addition of the power law.

Definition 4 (security definition of EUF-CMA). Currently, there are two main types of attacks against digital signatures: key-only attacks and known-message attacks. A key-only attack means that the adversary only knows the signer's public key without any other message. Among the many known-message attacks, the attack method with the highest attack strength is called adaptively chosen message attacks. In this type of attack, the adversary uses the signer as a querier, which can query not only the challenger for messages that depend on the signer's public key but also the signed message that has already been queried. If a signature scheme still has signature unforgeability under this attack, in other words, the signature constructed by the adversary through this optional challenge is still illegal and cannot be verified, the scheme is said to have existential unforgeability under adaptive chosen message attack, which is referred to as EUF-CMA security [30, 31]. The advantage of the adversary A in the following experiments is negligible:

$$\begin{aligned} &\mathrm{Exp}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k): \\ &(vk, sk) \leftarrow \mathrm{SigGen}(k), \\ &(M, \sigma) \leftarrow A^{\mathrm{Sign}_{sk}(\cdot)}(vk). \end{aligned} \tag{12}$$

Let Q denote that A accesses the message set of signature metaphor $\mathrm{Sign}_{sk}(\cdot)$.

Returns 1 if $\mathrm{Vrfy}_{vk}(M, \sigma) = 1 \hat{M} \in \neq Q$, otherwise returns 0, where A has access to the signed idiom machine polynomial bounded q_H degree. The specific meaning is whether the challenger can judge whether the signature σ of the message M comes from the message set of the signature metaphor $\mathrm{Sign}_{sk}(\cdot)$ visited by the adversary A through $\mathrm{Vrfy}_{vk}(M, \sigma)$. If it returns 1, it means that the challenger believes that the signature σ of the message M is naturally generated by legal means. If it returns 0, it means that the challenger believes that the signature σ of the message M is generated by A accessing the metaphor $\mathrm{Sign}_{sk}(\cdot)$.

The advantage of A is defined as follows:

$$\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = \left|\Pr\left[\mathrm{EXP}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = 1\right]\right|. \tag{13}$$

When $\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) < \mathrm{negl}(k)$, which is a negligible function, then we say the scheme is EUF-CMA safe.

4. EUF-CMA Security Signature Scheme Based on CSP

We first review the basic process of the RSA algorithm and specifically prove why the classical RSA signature algorithm does not have the existence of unforgeability under the adaptive chosen message attack.

The basic description of the RSA-like signature algorithm is as follows.

(1) Key generation is as follows:

$$\begin{aligned} &\mathrm{GenRSA}(k): \\ &p, q \leftarrow \mathrm{GenPrime}(k), \\ &N = pq, \varphi(n) = (p-1)(q-1), \\ &\text{Choose } e, \text{for } 1 < e < \varphi(n) \text{and} (\varphi(n), e) = 1, \\ &\text{Calculate } d, \text{ for } d \cdot e \equiv 1 \bmod \varphi(n), \\ &pk = (n, e), sk = (n, d). \end{aligned} \tag{14}$$

(2) Signature is as follows:

$$\begin{aligned} &\mathrm{Sign}_{sk}(M): \\ &\sigma = M^d \bmod n. \end{aligned} \tag{15}$$

(3) Verify is as follows:

$$\begin{aligned} &\mathrm{Vrfy}_{pk}(M, \sigma): \\ &\text{Return 1, if } \sigma^e = M \bmod n, \text{otherwise return 0.} \end{aligned} \tag{16}$$

Obviously, this signature algorithm is not antiforgery under the adaptive chosen message attack. When the attacker A performs a q_H-bounded query, A can submit $M_i = r^e \cdot M$ for the signature query. At this point, the challenger answers, computes $u_i = M_i^d \bmod n, i = 1, 2, \ldots, q$, and returns it to A. A forges the signature of message M and outputs $(M, \sigma) = (M, u_i/r)$ because of

$$u_i \equiv \left(r^e M\right)^d \bmod n \equiv r M^d \bmod n. \tag{17}$$

Therefore, $\sigma = u_i/r \equiv M^d \bmod n$ is the legal signature of M.

According to the previous Definition 4, EUF-CMA security definition, we can make the following analysis:

$$\begin{aligned} &\mathrm{Exp}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k): \\ &(vk, sk) \leftarrow \mathrm{SigGen}(k), \\ &(M, \sigma) \leftarrow A^{\mathrm{Sign}_{sk}(\cdot)}(vk). \end{aligned} \tag{18}$$

Let Q denote the message set of A accessing signature metaphor $\mathrm{Sign}_{sk}(\cdot)$, denoted as $M \in Q$, where A has access to the signed metaphor polynomial bounded q_H times.

At this time, the adversary A has the message M and its corresponding signature σ after accessing the signature machine $\mathrm{Sign}_{sk}(\cdot)$. At the same time, A calculates $M' = r^e \cdot M$, and the challenger calculates $u' = M'^d \bmod n$ and returns it to A. Then, A has another pair of signatures $(M, \sigma') = (M, u'/r)$. Verified by the challenger for legitimacy,

$$\sigma' = \frac{u'}{r} \equiv \frac{(r^e M)^d}{r} \bmod n \equiv \frac{rM^d}{r} \bmod n \equiv M^d \bmod n = \sigma. \quad (19)$$

However, the adversary A has not used M' to access the signature metaphor, so $M' \notin Q$. That is to say, the challenger believes that the message M signature σ' is naturally generated through legal means. The advantage of A at this time is defined as follows:

$$\mathrm{Adv}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = \left|\Pr\left[\mathrm{EXP}_{\mathrm{Sig},A}^{\mathrm{EUF}}(k) = 1\right]\right| = 1. \quad (20)$$

How to solve this problem? The previous method is to use the FDH (global hash function) that the output bit length of the hash function is the same as the modulus bit length to ensure the security of the scheme [32], but the hash function itself is a relatively complex algorithm, and the so-called randomness itself is controversial. Because no algorithm is truly random, such as $h = H(m)$, whose output is a pseudorandom process from m to h. In addition, using a hash function will reduce the efficiency of the scheme. Below, we will propose a new solution that satisfies EUF-CMA and prove that its security is improved based on the comparison above.

4.1. Definition of the RSA Problem (RSAP). Given a positive integer n (n is the product of two different odd prime numbers p, q), a positive integer $e(\gcd(e, (p-1)(q-1)) = 1)$, and an integer c, we find an integer m such that $m^e \equiv c \bmod n$. That is to say, the RSA problem is to find the root of e times in the case of modulo n (n is a composite integer).

4.2. The Difficult Problem of CSP Based on DDH. G is a noncommutative group. Suppose F is a function that satisfies the above CSP-LD system while having an adversary A. For any $a \in G^{-1}$, $b \in G$, we perform the following two experiments in parallel:

Experiment $\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-real}}$	Experiment $\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-rand}}$
$i \xleftarrow{\$} T, X \leftarrow F_{a^i}(b)$,	$i \xleftarrow{\$} T; X \leftarrow F_{a^i}(b)$,
$j \xleftarrow{\$} T, Y \leftarrow F_{a^j}(b)$,	$j \xleftarrow{\$} T; Y \leftarrow F_{a^j}(b)$,
$Z \leftarrow F_{a^{i+j}}(b)$,	$L \xleftarrow{\$} T, Z \leftarrow F_{a^L}(b)$,
$b \leftarrow A(X, Y, Z)$,	$b \leftarrow A(X, Y, Z)$,
Return b.	Return b.

(21)

For adversary A, the advantage of successful attacks in a CSP system based on the DDH assumption is defined as follows:

$$\mathrm{Adv}_{F,A}^{\mathrm{csp-ddh}} = \left|\Pr\left[\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-real}} = 1\right] - \Pr\left[\mathrm{EXP}_{F,A}^{\mathrm{CSP-ddh-rand}} = 1\right]\right|. \quad (22)$$

In other words, when i, j, L are taken randomly from T, we can consider that $(F_{a^i}(b), F_{a^j}(b), F_{a^{i+j}}(b))$ and $(F_{a^i}(b), F_{a^j}(b), F_{a^L}(b))$ are computationally indistinguishable when distributed. At present, there is no specific statement in the academic community to judge whether the CSP-DDH problem is hard, but we know that, in a general cyclic group, the DLP problem and the DDH problem are equivalent. From the above CSP-LD system reasoning, we know that, on a noncommutative semigroup, the CSP problem and the CSP-DDH problem can be directly replaced by the DLP problem and the DDH problem. Therefore, by logical reasoning, we can conclude that in a general noncommutative semigroup, the CSP problem and the CSP-DDH problem are equivalents [27].

4.3. Digital Signature Scheme Based on CSP-LD System. Assuming that a and b are random numbers, $a \in G^{-1}$ and $b \in G$, which have been fixed for the system parameters. Assuming that G is a general noncommutative semigroup, the binary function F satisfies the following conjugate operations:

$$F: G^{-1} \times G \longrightarrow G, (a, b) \longrightarrow aba^{-1}. \quad (23)$$

We mark $F(a, b) = aba^{-1}$ as $F_a(b)$.

(1) Key generation is as follows:

$$\begin{aligned} p, q &\leftarrow \mathrm{GenPrime}(k), \\ N = pq, \varphi(n) &= (p-1)(q-1), \\ \text{Choose } e, \text{for } 1 < e < \varphi(n) &\text{and } (\varphi(n), e) = 1, \\ \text{Calculate } d, \text{ for } d \cdot e &\equiv 1 \bmod \varphi(n), \\ pk = (n, e), sk &= (n, d). \end{aligned} \quad (24)$$

(2) Signature is as follows:

$$\begin{aligned} &\mathrm{Sign}_{sk}(M): \\ H &= F_a(M), \\ \sigma &= H^d \bmod n. \end{aligned} \quad (25)$$

(3) Verify is as follows:

$$\begin{aligned} &\mathrm{Vrfy}_{pk}(M, \sigma): \\ &\text{Return } 1, if\ \sigma^e = H \bmod n, \text{ otherwise return } 0. \end{aligned} \quad (26)$$

Under the CSP-LD system, the above scheme RSA-CSP-LD is EUF-CMA safe if the GenRSA-related RSA problem is difficult. Compared with the predecessors using the global hash function FDH to map M to prevent signature forgery, our scheme has a more compact security reduction.

Theorem 2. *Specifically, assuming that there is an adversary A that breaks the RSA-CSP-LD scheme with the advantage of ε, then there must be an adversary B that solves the RSA problem at least with the advantage of the following:*

$$\mathrm{Adv}_B^{\mathrm{RSA}}(k) \geq \frac{\varepsilon(k)}{eq_s}. \quad (27)$$

Proof. The EUF game is as follows.

In this proof process, all references to G refer to a universal noncommutative group, F is the CSP-LD system function defined on G, and $a \in G^{-1}$ and $b \in G$ are two fixed elements.

(1) The challenger runs Key generation (k) to get (n, e, d) and runs CSP-LD to get $F_a(b)$. Adversary A gets the public key (n, e).

(2) The adversary A can ask the challenger $F_a^{(\cdot)}(b)$ and the signature of the message; when A requests the signature of the message M, the challenger returns $\sigma = F_a(b^{|M|})^d \bmod n$ to A.

(3) A outputs a message-signature pair (M, σ) where A has not previously requested a signature for a message M. If $\sigma^e = F_a(b^M) \bmod n$, the adversary attack is successful.

The following proves that the RSA-CSP-LD scheme can be reduced to the RSA problem.

The adversary B knows (n, e, y^*) where y^* is uniformly random on Z_n^*. Using A to attack RSA-CSP-LD as a subroutine, the goal is to calculate $(y^*)^{1/e} \bmod n$. Because if B can get σ such that $\sigma^e \equiv y^* \bmod n$, then $\sigma \equiv (y^*)^{1/e} \bmod n$. Because of $\sigma^e \equiv y^* \bmod n$, if y^* is the value of $F_a(M)$ of a message M in the CSP-LD system, then σ is the signature of the message. (M, σ) is generated by adversary A, but $F_a(M)$ is generated by B, and B can be set to $F_a(M) = y^*$. Since B does not know which message A generates a forged pair signature when generating y^*, B has to make a guess, where the jth query of A corresponds to the final forged result of A. Before the reduction, for the sake of generality, we assume that the adversary A will not issue the same query to $F_a(M)$ twice. If A requests the signature of M, we take that it has been asked $F_a(M)$ before.

The reduction process is as follows:

(1) B gives the public key (n, e) to A.

(2) $F_a(\cdot)$ inquiry (at most q_s times): B creates a list query, which is initially empty and the element type is a quadruple $(M_i, \sigma_i, y_i, c_i)$, indicating that B has set $F_a(M) = y_i$, $\sigma_i^e \equiv y_i \bmod n$. When A initiates a query (set to M), B will answer as follows:

(a) If there is already an item $(M_i, \sigma_i, y_i, c_i)$ corresponding to M in query, we reply with y_i.

(b) Otherwise, B randomly chooses a $c_i \leftarrow \{0, 1\}^R$ and sets $\Pr[c_i = 0] = \delta$.

If $c_i = 0$, we return y^*.

Otherwise, we select a random value $\sigma_i \leftarrow Z_n^{*R}$, calculate $y_i \equiv \sigma_i^e \bmod n$, take y_i as the answer to this query, and store $(M_i, \sigma_i, y_i, c_i)$ in the table query.

(3) Signature query (up to q_s times): when A requests message M as a signature, B looks up $(M_i, \sigma_i, y_i, c_i)$ in the list query such that $M_i = M$.

If $c_i \neq 0$, we return σ_i.

Otherwise, $c_i = 0$, interrupts.

(4) Output: A outputs (M, σ). B looks for M in the query list corresponding to the quadruple $(M_i, \sigma_i, y_i, c_i)$, if $c_i \neq 0$, B interrupts.

In the above reduction process, c_i is the guess of B. $c_i = 0$ corresponding to the message that M in the quadruple is the signature that A will eventually forge and the role of c_i in the quadruple $(M_i, \sigma_i, y_i, c_i)$ is an identifier.

The success of B is determined by the following three events:

π_1: B does not break in A 's signature query

π_2: A produces a valid message-signature pair (M, σ)

π_3: π_2 occurs and c is equal to 0 in the quadruplet (M, σ, y, c) corresponding to M.

$\Pr[\pi_1] = (1 - \delta)^{q_s}$, $\Pr[\pi_2|\pi_1] = \varepsilon(K)$, and $\Pr[\pi_3|\pi_2\pi_1] = \Pr[0|\pi_2\pi_1] = \delta$. So, the success rate of B is $\Pr[\pi_3\pi_1] = \Pr[\pi_1] \cdot \Pr[\pi_2|\pi_1] \cdot \Pr[\pi_3|\pi_2\pi_1] = (1 - \delta)^{q_s} \in \delta$.

Considering $(1 - \delta)^{q_s} \in \delta$ as a function of δ, when $\delta = 1/q_s + 1$ can be obtained, $(1 - \delta)^{q_s} \in \delta$ reaches the maximum, and the maximum value is $\varepsilon(k)/e(q_s + 1) \approx \varepsilon(k)/e(q_s)$. The proof is complete.

Compared to previous pair schemes, our scheme has a larger pair advantage in terms of efficiency, since all messages are encoded as low-dimensional matrices, and the scaling rate in terms of storage and computational overhead is linear compared to plaintext implementations. Horan K. et al. [33] mentioned that the CSP problem is in a general linear group $GL_d(R)$ (where R represents the real number field); if $d > 4$, CSP can be proved to be anti-quantum secure, so when we encode the message M as a matrix, it is necessary to keep its dimension greater than 4. Specifically, we assume that G is a general noncommutative semigroup, $a \in G^{-1}$ and $b \in G$, and the function $F_a(M)$ can be regarded as a pair of preprocessing for the message M. For any message M originating from the real domain R, we can encode $b^{|M|}$ as a 6-dimensional upper triangular matrix, denoted by $M \in R^{6\times 6}$.

We use three pairs of random numbers (m_1, m_2), (m_3, m_4), (m_5, m_6) to represent the message M, while satisfying certain properties: $m_1 + m_2 = M, m_3 + m_4 =$

$m_5 + m_6 = r$, where r is a system random number. With these elements, we construct the matrix as follows:

$$M_1 = \begin{pmatrix} m_1 & m_2 \\ m_2 & m_1 \end{pmatrix},$$
$$M_2 = \begin{pmatrix} m_3 & m_4 \\ m_4 & m_3 \end{pmatrix}, \quad (28)$$
$$M_3 = \begin{pmatrix} m_5 & m_6 \\ m_6 & m_5 \end{pmatrix}.$$

Combining the above three small matrices, the final encoding form of the message M is as follows:

$$M = \begin{pmatrix} M_1 & R_1 & R_2 \\ 0 & M_2 & R_3 \\ 0 & 0 & M_3 \end{pmatrix}. \quad (29)$$

0 here also represents an all-zero matrix of 2×2. R_i $(i = 1, 2, 3)$ represents a random matrix uniformly sampled from the real number domain $R^{2\times 2}$.

Next, we perform the encoding operation on a. We uniformly randomly sample a matrix from $R^{6\times 6}$ to represent a, which can also be considered as 9 random matrices of 2×2, as expressed in the following form:

$$a = \begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9 \end{pmatrix}, \text{for } a_i = \begin{pmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4} \end{pmatrix}, (i = 1, 2, \ldots, 9). \quad (30)$$

The probability that message space M communicates with elements in a is negligible. It can be understood in this way that a here is similar to a key for encrypting a message M, so there are the following operations:

$$H = F_a(M) = aMa^{-1} = a\begin{pmatrix} M_1 & R_1 & R_2 \\ 0 & M_2 & R_3 \\ 0 & 0 & M_3 \end{pmatrix}a^{-1}, \quad (31)$$

where H is the input parameter for the subsequent execution of the RSA algorithm, which can also be regarded as the encryption of the message M, where a can be understood as a symmetric key. In some specific cases, we can perform conflict tracking, use a to solve H, recover the message from M_1, and recover the signer pair identity from M_2 (assuming the user identity information is placed in it).

The security (antiforgery) of $F_a(M) = aMa^{-1}$ proves the following.

First, we carry out the following operations:

$$\det\left(H^* - TH'\right) = \det(a)\det\left(\begin{pmatrix} M_1^* - TM_1' & R_1^* & R_2^* \\ 0 & M_2^* - TM_2' & R_3^* \\ 0 & 0 & M_3^* - TM_3' \end{pmatrix}\right)\det\left(a^{-1}\right), \quad (32)$$

where R_i^*, $(i = 1, 2, 3)$ are random matrices. The representation of T is as follows:

$$T = \begin{pmatrix} t & R_1 & R_2 \\ 0 & t & R_3 \\ 0 & 0 & t \end{pmatrix}, \quad (33)$$

among them

$$t = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (34)$$

R_i, $(i = 1, 2, 3)$ is randomly sampled from $R^{2\times 2}$. The adversary is defined to launch a forgery attack according to the following algorithm, which is formally described as follows [34]:

$$\begin{aligned}
&\mathrm{Exp}_{\pi,A}^{\mathrm{CPA}}(K):\\
&(k)\leftarrow \mathrm{KeyGen}(K),\\
&(M_0, M_1, H)\leftarrow A^{F_k(\cdot)}, \text{there} |M_0| = |M_1|,\\
&H' = F_k(H), \text{and } M_0 < H < M_1,\\
&\beta\leftarrow R_{\{0,1\}}, H^* = \varepsilon_k(M_\beta),\\
&\beta' = 1, if \det(H^* - TH'), \beta' = 0, \text{otherwise},\\
&\text{Output } 1, if \beta = \beta', \text{Output } 0, \text{otherwise}.
\end{aligned} \tag{35}$$

The adversary's advantage is defined as follows:

$$\mathrm{Adv}_{\pi,A}^{\mathrm{CPA}}(K) = \left|\Pr\left[\mathrm{Exp}_{\pi,A}^{\mathrm{CPA}}(K) = 1\right] - \frac{1}{2}\right|. \tag{36}$$

We will try to expand the content of the if conditional statement $\det(H^* - TH^{'})$:

$$\det(H^* - TH') = \det(p)\det(M_i^* - tM_i')\det\left(p^{-1}\right), (i = 1, 2, 3), \tag{37}$$

among them

$$\det(M_i^* - tM_i') = (a_{2i-1}^* - a_{2i}')^2 - (a_{2i}^* - a_{2i-1}')^2 = (m^* - m')((a_{2i-1}^* - a_{2i}^*)t - (a_{2i}' - a_{2i-1}')n). \tag{38}$$

However, by borrowing the scheme of Li et al. [35], we can clarify $a_{2i-1} > a_{2i}$. So, the part of $((a_{2i-1}^* - a_{2i}^*)t - (a_{2i}' - a_{2i-1}')n)$ always satisfies positive, and $\det(p)\det(p^{-1}) = 1$. Therefore, for an attacking adversary, to distinguish whether the signed message is M_0 or M_1, he only needs to calculate $\det(H^* - TH')$ according to the sign of the returned value. If a positive value is returned, 1 is output, representing the guessed signature message as $M^* = M_1$. If a negative value is returned, 0 is output, which means the guessed signature message is $M^* = M_0$. Therefore, the advantage of the adversary is 1, which means that the scheme is not anticounterfeiting.

The advantage of our proposed scheme is that we are a probabilistic encryption scheme. There can be multiple encoding forms for m'. First, a random even number ρ is selected to encrypt m', and the following form is obtained:

$$\begin{aligned}
H' &= F_a\left(M'^{\rho}\right) = aM'^{\rho}a^{-1}\\
&= a\begin{pmatrix} M_1^{\rho} & R_1 & R_2\\ 0 & M_2^{\rho} & R_3\\ 0 & 0 & M_3^{\rho}\end{pmatrix}a^{-1} = F_a^{\rho}(M').
\end{aligned} \tag{39}$$

According to the properties $F_a(b^m) = F_a^m(b)$ of the CSP-LD system, we mentioned earlier, and the upper triangular matrix encoding form of M is

$$M = \begin{pmatrix} M_1 & R_1 & R_2\\ 0 & M_2 & R_3\\ 0 & 0 & M_3\end{pmatrix}. \tag{40}$$

We can infer

$$\left|M^{\rho}\right| = |M|^{\rho}, (i = 1, 2, 3). \tag{41}$$

Therefore,

$$\begin{aligned}
\det(H^* - TH') &= \det(p)\det(M_i^* - tM_i')^{\rho}\det\left(p^{-1}\right), (i = 1, 2, 3) = \det(M_i^* - tM_i')^{\rho},\\
&= (m^* - m')^{\rho}((a_{2i-1}^* - a_{2i}^*)t - (a_{2i}' - a_{2i-1}')n)^{\rho}.
\end{aligned} \tag{42}$$

Because ρ is an even number, the adversary always has a positive value when calculating $\det(H^* - TH^{'})$, and it is impossible to determine whether the signature comes from M_0 or M_1. □

5. RSA-like Aggregate Signature Scheme Based on CSP-LD System

Before formally introducing the aggregate signature scheme, we need to make a formal specification of the paired element in G for a secure and valid pair.

Specification 1: in a CSP-LD system, the representation of elements in G is unique

Specification 2: it is possible to efficiently convert an element in G to its regular form

Specification 3: the length of $F_{a^t}(b)$ does not show any information about a^t.

According to Definition 3, we suppose a and b are random numbers, $a \in G^{-1}$ and $b \in G$, which are given and fixed for the system parameters, and we assume that G is a general noncommutative semigroup, and the binary function F satisfies the following conjugation operations:

$$F\colon G^{-1}\times G\longrightarrow G,\quad (a,b)\longrightarrow aba^{-1}. \tag{43}$$

We denote $F(a,b)=aba^{-1}$ as $F_a(b)$.

Assuming that there are different users $p_1, p_2, \ldots, p_N$, in a multiuser environment, the message M needs to be co-signed. Our RSA aggregate signature scheme based on the CSP-LD system consists of the following algorithms.

(1–1) message encoding: the message M is composed of $m_{i\ (i=1,2,\ldots,6)}$ satisfying some certain property, $m_1+m_2=M$ and $m_3+m_4=m_5+m_6=r$, where r is a system random number, and an even number ρ is sampled from the random number in the real number domain. We construct the matrix as follows:

$$M_i^{\rho}=\begin{pmatrix} m_{(2*i)-1}^{\rho} & m_{2*i}^{\rho} \\ m_{2*i}^{\rho} & m_{(2*i)-1}^{\rho}\end{pmatrix},\ (i=1,2,3). \tag{44}$$

Combining the above three submatrices, the final encoding form of the message M is as follows:

$$M^{\rho}=\begin{pmatrix} M_1^{\rho} & R_1^{\rho} & R_2^{\rho} \\ 0 & M_2^{\rho} & R_3^{\rho} \\ 0 & 0 & M_3^{\rho}\end{pmatrix}. \tag{45}$$

0 here also represents an all-zero matrix of 2×2. $R_i\ (i=1,2,3)$ represents a random matrix uniformly sampled from the real number domain $R^{2\times 2}$.

(1–2) coding form of a: we uniformly randomly sample a matrix from $R^{6\times 6}$ for encoding, representing a, which can also be considered as 9 random matrices of 2×2, expressed in the following form:

$$a=\begin{pmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ a_7 & a_8 & a_9\end{pmatrix},\ \text{for}\ a_i=\begin{pmatrix} a_{i1} & a_{i2} \\ a_{i3} & a_{i4}\end{pmatrix},\ (i=1,2,\ldots,9). \tag{46}$$

(1) Key generation is as follows:

$$\begin{aligned} &\text{GenRSA}(k):\\ &s_{i,(i=1,2,\ldots,N)}, p, q\leftarrow\text{GenPrime}(k),\\ &N=pq, \varphi(n)=(p-1)(q-1),\\ &\text{Take } e, \text{satisfying } 1<e<j(n) \text{and } (j(n),e)=1,\\ &\text{Compute } d, \text{satisfying } d\cdot e\equiv 1 \bmod \varphi(n),\\ &\text{Calculate } w, w=\sum_{i=1}^{N} s_i,\\ &pk=(n,e,w), sk=(n,d,s_i). \end{aligned} \tag{47}$$

(2) Signature is as follows:

$$\begin{aligned} &\text{Sign}_{sk}(M):\\ &H=\sum_{i=1}^{N} F_{a^{s_i}}^{\rho}(M),\\ &\sigma=H^{d} \bmod n. \end{aligned} \tag{48}$$

(3) Verify is as follows:

$$\text{Vrfy}_{pk}(M,\sigma). \tag{49}$$

If $\sigma^e=F_{a^w}^{\rho}(M) \bmod n$, we return 1; otherwise, we return 0.

Proof of the correctness of the scheme: according to Lemma 2, the CSP-LD system satisfies the following properties:

$$\begin{aligned} F_{a^m}(b)&=a^m b a^{-m}=a^s a^t b a^{-t} a^{-s}\\ &=a^s F_{a^t}(b) a^{-s}=F_{a^s}\left(F_{a^t}(b)\right). \end{aligned} \tag{50}$$

Because of $w=\sum_{i=1}^{3} s_i$, we get $\prod_{i=1}^{3} F_{a^{s_i}}^{\rho}(M)=F_{a^w}^{\rho}(M)$. On the question of whether the security is satisfied, we can infer from the previous point that since M is an upper triangular matrix, it satisfies

$$\left|M^{\rho}\right|=|M|^{\rho},\ (i=1,2,3). \tag{51}$$

When the adversary tries to distinguish M_0 or M_1 by computing the determinant,

$$\begin{aligned} \det\left(H^*-TH'\right)&=\det(p)\det\left(M_i^*-tM_i'\right)^{\rho}\det\left(p^{-1}\right),\ (i=1,2,3)=\det\left(M_i^*-tM_i'\right)^{\rho}\\ &=\left(m^*-m'\right)^{\rho}\left((a_{2i-1}^*-a_{2i}^*)t-(a_{2i}'-a_{2i-1}')n\right)^{\rho}. \end{aligned} \tag{52}$$

Table 1: The efficiency comparison between our scheme and literature [24, 36].

	Assumption	Signature length	Signature algorithm	Verification algorithm	Saving rate
Literature 24	Pairing	320	$2nE + nH$	$nH + (3n - 1)P$	50%
Literature 36	RSA	160	nE	$(n + 1)E$	50%
Our scheme	RSA	160	nE	$2E$	Fixed length

Table 2: The security comparison between our scheme and [3, 6, 24].

	EUF-CMA	Antiquantum security
Literature 24	No	No
Literature 36	Yes	No
Our scheme	Yes	Yes

Table 3: Notations.

Notations	Description
k	The system parameters
p, q	Two large prime numbers are chosen at random
pk, sk	The public key and private key
σ	Result of signing the message
$F_a(b)$	Functions satisfying certain properties under the CSP-LD system
G	A general noncommutative semigroup
p_i	Users
M	Message
$m_{i(i=1,2,\ldots,6)}$	They together according to certain rules to form a message M
r	Random number
ρ	Random even number
a	9 random matrices of 2×2
$(M_i, \sigma_i, y_i, c_i)$	The quadruple, σ_i, is the signature of M_i, y_i is the query result of an adversary A to M_i, and c_i is a random value of 0 1
s_i	User ID number
w	The sum of all s_i
t	Special 0 and 1 matrix
R_i, $(i = 1, 2, 3)$	The randomly sampled matrices from $R^{2\times2}$
T	The upper triangular encoding matrix
H	Regarded as the encryption of the message M under the function F

Because the value of ρ is an even number (it can be set to $\rho = 2$), the adversary cannot determine whether the signature comes from M_0 or M_1 based on the value calculated by $\det(H^* - TH')$, so H satisfies the selection of plaintext antiforgery. According to the previous inference in Definition 4, the aggregated signature scheme proposed by us is still antiforgery under the adaptive chosen message attack.

According to the algorithm proposed by Shor, a quantum computer with N qubits can perform 2^N operations at a time. In theory, the key is the 1024 bit long RSA algorithm, which can be cracked in 1 second with a 512 bit quantum computer. At present, as long as the proposed scheme is set s_i to a 160 bit integer, it can resist the exhaustion-resistant attack [27].

6. Efficiency Analysis

Now, we compare the computational efficiency of the RSA aggregate signature scheme under the CSP-LD system with some other aggregate signature schemes. Still assume that there are N users signing messages M at the same time. For each signature, if the aggregation method is not used, the original RSA signature method without aggregation method needs to store a total of N pairs of $(M, \sigma_1), \ldots, (M, \sigma_N)$ signatures. While the scheme in [36] improves the efficiency by 50%, the signature they store is $(M, \sigma_1, \ldots, \sigma_N)$. In our scheme, no matter how many users there are, we only need to store a pair of signatures, namely, (M, σ), which benefits from the advantages of the CSP-LD system. Compared with [36], our improved efficiency has a linear relationship with the value of N, and the larger the value, the greater the advantage of our scheme. Compared with the pairing-based scheme in [24], our advantage is even more obvious, since it is known that a pairing operation takes approximately 6–20 times the time of a modulo-exponential operation [25].

In addition, since all messages are encoded as low-dimensional matrices, the scaling rate in terms of storage and computation overhead is linear compared to message signature implementations and the length of aggregated signatures is fixed, maximizing signature storage savings space without losing accuracy. In terms of security, our scheme is also indestructible to a large extent, and the strongest attack method against the signature scheme, the adaptive chosen message attack, is still existentially unforgeable. Moreover,

by setting the system parameter thresholds on the matrix dimension and the length of the private key, antiquantum attacks, and exhaustive attacks can be achieved.

Explanation of symbols in Table 1: Exp represents a power of 1 operation, H represents a hash operation, P represents a bilinear pairing operation, and n represents the number of users. Assuming that the following three schemes all select the group G whose order is the same prime number q, if the system parameter k is 160 bits, the length of the group G is calculated as $|G| = 160$bit. The details are shown in Table 1.

The details of the security comparison between our scheme and literature are shown in Table 2.

7. Conclusion

This study improves the RSA-like signature scheme by proposing new schemes that take advantage of CSP-LD systems to encode messages with the low-dimensional matrix. By flexibly changing the encoding structure, it can perfectly satisfy the antiforgery under the adaptive choice message attack (EUF-CMA) without using the global hash function. Setting the matrix dimension greater than the critical value can achieve the antiquantum attack, and controlling the length of the user's s_i element longer than a certain bit can resist exhaustive attacks. In the environment where N users sign a message, we implement the aggregated signature under the RSA structure according to the CSP-LD system, which greatly reduces the generation of public and private key pairs. Moreover, the final signature pair has nothing to do with the number of users, which saves a lot of storage space and improves computing efficiency. In the future, we look forward to combining the signature scheme with cutting-edge technologies such as blockchain technology, smart contracts [37], and machine learning [38] to improve the deployment of the scheme, learn from each other's strengths, and furthermore, improve efficiency and security.

7.1. The notations of this work. In this section, we explain all the specific characters in the study; the details are shown in Table 3.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the "Chengdu-Chongqing Economic Circle Construction" Scientific and Technological Innovation Project of Chongqing Municipal Education Commission, under Grant KJCX2020033, the National Natural Science Foundation of P.R., China, under Grants 61903053 and 62273065, the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, under Grant AGK2020006, and the Chongqing Municipal Education Commission Research Program, under Grants KJQN201900702 and KJZD-K201800701.

References

[1] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press LLC, Second Edition, 2002.

[2] A. J. Menezs, P. C. V. Oorchot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[3] B. Schneier, *Applied Cryptography. Protocols, Algorithms and Source in C*, John Wiley & Sons, Second Edition, 1995.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[5] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proceedings of the International conference on the theory and applications of cryptographic techniques*, pp. 416–432, Springer, Berlin, Heidelberg, May 2003.

[6] K. Hashimoto and W. Ogata, "Unrestricted and compact certificateless aggregate signature scheme," *Information Sciences*, vol. 487, no. 1, pp. 97–114, 2019.

[7] T. Iwasaki, N. Yanai, M. Inamura, and K. Inamura, "Tightly-secure identity-based structured aggregate signature scheme under the computational diffie-hellman assumption," in *Proceedings of the 2016 IEEE 30th International Conference on Advanced Information Networking and Applications*, pp. 669–679, IEEE, Crans-Montana, Switzerland, March 2016.

[8] A. Boldyreva, C. Gentry, and A. O'Neill, "Ordered multi-signatures and identity-based sequential aggregate signatures, with applications to secure routing," in *Proceedings of the 14th ACM conference on Computer and communications security*, pp. 276–285, ACM, Alexandria, Egypt, January 2007.

[9] Z. Shao, "On the sequentiality of three optimal structured multisignature schemes," in *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 105–115, Springer, Berlin, Heidelberg, 2007.

[10] Z. Guan, N. Wang, X. Fan, X. Liu, L. Wu, and S. Wan, "Achieving secure search over encrypted data for e-commerce: a blockchain approach," *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–17, 2021.

[11] L. Zhao, M. B. Saif, A. Hawbani, G. Min, S. Peng, and N. Lin, "A novel improved artificial bee colony and blockchain-based secure clustering routing scheme for FANET," *China Communications*, vol. 18, no. 7, pp. 103–116, 2021.

[12] Y. Liu, W. Yu, Z. Ai, G. Xu, L. Zhao, and Z. Tian, "A blockchain-empowered federated learning in healthcare-based cyber physical systems," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 6, pp. 4482–4494, 2022.

[13] C. Wang, X. Wu, G. Liu, T. Deng, K. Peng, and S. Wan, "Safeguarding cross-silo federated learning with local differential privacy," *Digital Communications and Networks*, vol. 8, pp. 446–454, 2021.

[14] L. Zhao, H. Li, N. Lin, M. Lin, C. Fan, and J. Shi, "Intelligent content caching strategy in autonomous driving toward 6G," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9786–9796, 2022.

[15] S. Wan, "Topology hiding routing based on learning with errors," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 14, pp. 1–10, 2020.

[16] L. Zhao, C. Wang, K. Zhao, D. Tarchi, S. Wan, and N. Kumar, "INTERLINK: A digital twin-assisted storage strategy for satellite-terrestrial networks," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 5, pp. 3746–3759, 2022.

[17] S. Mao, L. Liu, N. Zhang et al., "Reconfigurable intelligent surface-assisted secure mobile edge computing networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 6, pp. 6647–6660, 2022.

[18] J. Feng, L. Liu, Q. Pei, and K. Li, "Min-max Cost Optimization for efficient hierarchical federated learning in Wireless edge networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 11, pp. 1–2700, 2022.

[19] L. Zhao, Z. Bi, A. Hawbani, K. Yu, Y. Zhang, and M. Guizani, "ELITE: An intelligent digital twin-based hierarchical routing scheme for softwarized vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 12, pp. 4667–4685, 2022.

[20] L. Zhao, Z. Li, A. Y. Al-Dubai et al., "A novel prediction-based temporal graph routing algorithm for software-defined vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 8, pp. 13275–13290, 2022.

[21] L. Zhao, T. Zheng, M. Lin, A. Hawbani, J. Shang, and C. Fan, "SPIDER: A social computing inspired predictive routing scheme for softwarized vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9466–9477, 2022.

[22] Y. P. Li, H. H. Nie, and Y. W. Zhou, "A novel and provably secure certificateless aggregate signature scheme," *Journal of Cryptologic Research*, vol. 2, no. 6, pp. 526–535, 2015.

[23] Y. W. Zhou, B. Yang, and W. Z. Zhang, "Efficient and provide security certificateless aggregate signature scheme," *Journal of Software*, vol. 26, no. 12, pp. 3204–3214, 2015.

[24] X. D. Yang, X. Z. Pei, and F. Y. An, "Message authentication scheme for vehicular ad hoc network using identity-based aggregate signature," *Computer Engineering*, vol. 46, no. 2, pp. 170–174+182, 2020.

[25] M. Bellare and G. Neven, "Identity-based multi-signatures from RSA," *Cryptographers' Track at the RSA Conference*, pp. 145–162, Springer, Berlin, Heidelberg, 2007.

[26] J. Buchmann, C. Coronado, M. Döring et al., *Post-quantum Signatures*, Cryptology ePrint Archive, 2004.

[27] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[28] P. Dehornoy, "Using shifted conjugacy in braid-based cryptography," *Contemporary Mathematics*, vol. 418, no. 9, pp. 65–74, 2006.

[29] L. Wang, L. Wang, and Z. Cao, "New constructions of public-key encryption schemes from conjugacy search problems," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 1–17, Springer, Berlin, Heidelberg, 2010.

[30] S. Goldwasser, S. Micali, and R. L. Rivest, "A paradoxical solution to the signature problem," *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, 2019.

[31] S. Goldwasser, S. Micali, and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1988.

[32] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," *Annual International Cryptology Conference*, pp. 41–55, Springer, Berlin, Heidelberg, 2004.

[33] K. Horan and D. Kahrobaei, "The hidden subgroup problem and post-quantum group-based cryptography," in *International Congress on Mathematical Software*, pp. 218–226, Springer, Cham, 2018.

[34] F. T. Kuang, B. Mi, Y. Li, Y. Weng, and S. Wu, "Multiparty homomorphic machine learning with data security and model preservation," *Mathematical Problems in Engineering*, vol. 2021, Article ID 6615839, 8 pages, 2021.

[35] J. Li, X. Kuang, S. Lin, X. Ma, and Y. Tang, "Privacy preservation for machine learning training and classification based on homomorphic encryption schemes," *Information Sciences*, vol. 526, no. 1, pp. 166–179, 2020.

[36] B. Dou, C. H. Chen, H. Zhang, and C. Xu, "Identity-based sequential aggregate signature scheme based on RSA," *International journal of innovative computing information and control*, vol. 8, no. 9, pp. 6401–6413, 2012.

[37] K. Peng, M. Li, H. Huang, C. Wang, S. Wan, and K. K. R. Choo, "Security challenges and opportunities for smart contracts in Internet of Things: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12004–12020, 2021.

[38] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis et al., "Modeling, detecting, and mitigating threats against industrial healthcare systems: a combined software defined networking and reinforcement learning approach," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 2041–2052, 2022.