

1 of 1

[Download](#) [Print](#) [Save to PDF](#) [Save to list](#) [Create bibliography](#)

Artificial Intelligence, Blockchain, Computing and Security: Volume 1 • Volume 1, Pages 653 - 661 • 1
January 2023

Document type

Book Chapter

Source type

Book

ISBN

978-100384581-2, 978-103249393-0

DOI

10.1201/9781003393580-98

[View more](#) [v](#)

Blockchain-Aware secure lattice aggregate signature scheme

Rasool, Motashim^a [✉](#) ; Khatri, Arun^b [✉](#) ;

Maaliw, Renato R.^c [✉](#) ; Manjula G.^d [✉](#) ;

Varma, M.S. Kishan^e [✉](#) ; Agarwal, Sohith^f [✉](#)

[Save all to author list](#)

^a Computer Science and Engineering, SR Institute of Management and Technology, Uttar Pradesh, Lucknow, India

^b JK Business School, Gurgaon, India

^c College of Engineering, Southern Luzon State University, Lucban, Quezon, Philippines

^d RMK College of Engineering and Technology, Thiruvallur, India

[View additional affiliations](#) [v](#)

[Full text options](#) [v](#) [Export](#) [v](#)

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)

Related documents

Find more related documents in Scopus based on:

[Authors >](#) [Keywords >](#)

Abstract

Author keywords

SciVal Topics

Abstract

In the Forward Secure Ordered Aggregation (FssAgg) signature system, the signer gradually and orderly aggregates the signatures under different keys in different periods into one signature in a hierarchical "onion-like" manner. Among them, the innermost signature is the first signature. In addition, compared with ordinarily ordered aggregate signatures, forward secure requested aggregate signatures are the aggregation of different signatures of the same signer rather than the signatures of additional signers so that the signature verifier can use public key complete verification of all aggregation processes. The forward-safe ordered aggregate signature has the advantages of both forward-secure signature and aggregate signature. It has been widely used in many application scenarios, such as log systems and blockchains. Several existing forward-safe ordered aggregate signatures are based on traditional number theory problems, which will no longer be problematic in the post-quantum era. Therefore, finding a forward-safe requested aggregate signature in the quantum computing environment is imminent. Based on the small integer solution problem on the lattice, a forward-secure lattice-based rated aggregate signature scheme under the standard model is constructed. To achieve high efficiency, the system uses fixed-dimensional lattice-based delegation technology to realize critical updates and achieve forward security; then, the message to be signed and the difficulty problem on the lattice are respectively embedded into the signature using message addition technology and preimage sampling algorithm, making the signature unforgeable under the standard model. © 2024 selection and editorial matter, Arvind Dagur, Karan Singh, Pawan Singh Mehra & Dharendra Kumar Shukla; individual chapters, the contributors.

Author keywords

Aggregation processes; Blockchain; Forward-safe ordered; Secure Lattice; Signature Scheme

Blockchain-Aware Secure Lattice Aggregate Signature Scheme

Motashim Rasool¹, Dr. Arun Khatri², Renato R. Maaliw III³, G. Manjula⁴, M S Kishan Varma⁵, Sohiti Agarwal⁶

¹Assistant Professor, Computer Science and Engineering, SR Institute of Management and Technology, Lucknow, Uttar Pradesh, India,

²Professor, JK Business School, Gurgaon, India

³Associate Professor, College of Engineering, Southern Luzon State University, Lucban, Quezon, Philippines

⁴Assistant Professor, RMK College of Engineering and Technology, Thiruvallur

⁵Assistant Professor, Department of Management Studies, VFSTR Deemed to be University, Guntur

⁶Assistant Professor, Department of Computer Engineering and Information Technology, Suresh Gyan Vihar, University, Jaipur, India

Email: ¹mail2motashim@gmail.com, ²khatrirun@yahoo.com, ³rmaaliw@slsu.edu.ph, ⁴manjulacse@rmkcet.ac.in, ⁵mskishanvarma@gmail.com, ⁶sohiti.agarwal@gmail.com

Abstract: In the Forward Secure Ordered Aggregation (FssAgg) signature system, the signer gradually and orderly aggregates the signatures under different keys in different periods into one signature in a hierarchical "onion-like" manner. Among them, the innermost signature is the first signature. In addition, compared with ordinarily ordered aggregate signatures, forward secure requested aggregate signatures are the aggregation of different signatures of the same signer rather than the signatures of additional signers so that the signature verifier can use public key complete verification of all aggregation processes. The forward-safe ordered aggregate signature has the advantages of both forward-secure signature and aggregate signature. It has been widely used in many application scenarios, such as log systems and blockchains. Several existing forward-safe ordered aggregate signatures are based on traditional number theory problems, which will no longer be problematic in the post-quantum era. Therefore, finding a forward-safe requested aggregate signature in the quantum computing environment is imminent. Based on the small integer solution problem on the lattice, a forward-secure lattice-based rated aggregate signature scheme under the standard model is constructed. To achieve high efficiency, the system uses fixed-dimensional lattice-based delegation technology to realize critical updates and achieve forward security; then, the message to be signed and the difficulty problem on the lattice are respectively embedded into the signature using message addition technology and preimage sampling algorithm, making the signature unforgeable under the standard model.

Keywords: *Blockchain, Signature Scheme, forward-safe ordered, secure Lattice, aggregation processes*

I. Introduction

Logs are a key component of computer information systems, they record "when and by whom what happened" in the system, and have certain forensic value. Therefore, it is particularly important to protect the log security of the system. In order to prevent attackers from tampering with historical logs, traditional audit methods write logs to devices that can only append records, or perform remote recording, but this cannot prevent malicious system administrators from tampering with logs. In order to reduce the threat brought by malicious system administrators, forward security signature technology is introduced into the log system.

The concept of forward secure signature [1] introduces to reduce the problem of key leakage. In order to achieve forward security, the key generation center (key generation center, KGC) divides time into k discrete time periods, and uses different keys in different periods. Among them, the signature key of period $i + 1$ is calculated by the key update algorithm using the signature key of period i as input, where $1 \leq i < k$. Therefore, as long as the key update algorithm satisfies the characteristics of the one-way trapdoor function, even if the key of a given period is leaked, it will not be safe for the signature (the signature here is the signature of the log) of the previous period

create a threat. Therefore, the forward security signature can effectively reduce the problem of key exposure, thereby reducing the threat of malicious log tampering by system administrators.

One of the main obstacles to deploying a forward-safe signature scheme in a secure logging system is its overhead. Storing a signature for each message is a heavy workload for a logging system that generates a large number of messages. The introduction of the concept of ordered aggregate signature [2] can effectively solve this problem. In an ordered aggregation signature scheme, the aggregation of the certificate chain is carried out step by step. For example, user U_1 first uses its signature private key SK_1 to calculate and output the signature sg_{i_1} for message m_1 ; then, taking sg_{i_1} as input, user U_2 uses its signature private key SK_2 to calculate and output the signature sg_{i_2} for messages m_1 and m_2 ; Taking the signature $sg_{i_{i-1}}$ of users U_1, U_2, \dots, U_{i-1} on messages m_1, m_2, \dots, m_{i-1} as input, U_i uses its signature private key SK_i to calculate and output the signature $sg_{i_{i-1}}$ for messages m_1, m_2, \dots, m_i Sign sg_{i_i} ; until U_k finishes signing. When k users sign in such a step-by-step manner, while retaining the minimum communication overhead of the aggregate signature, it also fully guarantees the non-repudiation of the signature to the message.

In order to take into account the security and efficiency of the log system, the first forward-secure ordered aggregate signature scheme - BLS-FssAgg signature [3] came into being. However, since the construction of the BLS-FssAgg signature depends on the bilinear pairing problem, the huge overhead of the bilinear pairing operation will inevitably make the signature verification cost huge. In the following year, Ma proposed two practical FssAgg signature schemes [4], namely BM-FssAgg signature and AR-FssAgg signature. In these two FssAgg signature schemes, the multiplication operation on the QRn group is used in the signature construction process, so that the public key, private key and signature size reach a constant level, and the time complexity of secret key update and signature is also constant, which reflects its practicability; and compared with the BLS-FssAgg signature in [3], the verification speeds of these two signatures are increased by 16 times and 4 times respectively. In 2018, based on the strong RSA assumption and the discrete logarithm problem on the elliptic curve, Wei Xingjia successively proposed a non-repudiation identity-based aggregate signature scheme with forward security [5] and an identity-based aggregate signature scheme with forward security properties. Proxy aggregate signature scheme [6], and prove that it satisfies forward security and existence unforgeability under the random oracle model. However, the above two aggregated signatures are out of order, so they cannot be applied to the log system. Literature [7] proposed an efficient forward-secure ordered aggregate signature scheme for secure log systems- FAS signature. In addition to satisfying forward security and unforgeable existence, it is worth mentioning that the size of the public key and private key of the FAS signature is constant, and the key size is the same as that of the forward secure non-aggregate signature BM signature [1] At the same time, the FAS signature reduces the verification complexity of the BM signature from $O(k^2)$ to $O(lk)$, where l represents the output length of the hash function. Literature [8] used the Chinese remainder theorem, combined with bilinear pairing technology, to propose an aggregate signature scheme with forward security properties based on elliptic curve cyclic groups. The forward security of the scheme is determined by strong RSA the assumption is guaranteed, and the two-way verifiability and enforceability of the scheme are also provable. However, several existing practical forward-secure ordered aggregate signatures are based on traditional number theory problems. At the same time, research on forward-secure signatures with other special properties [9-12] is also in full swing. Literature [13] those classical number theory problems are no longer safe in the quantum computing environment. With the gradual commercialization of quantum computers, the post-quantum era has come to people, and it is imminent to find quantum-immune forward-safe orderly aggregate signatures.

The US National Institute of Standards and Technology has been collecting post-quantum cryptography standards from around the world since 2016. In the competition for the third round of cryptographic standards that just ended in July 2020, there were a total of 7 winning algorithms, of which only lattice public key cryptography schemes accounted for 5 (including 3 encryption algorithms and 2 signature algorithms). In the view of the National Institute of Standards and Technology, these lattice-hard problem-based schemes are the most promising general-purpose algorithms for public-key encryption and digital signature schemes. Therefore, constructing a forward-safe ordered aggregate signature based on the Lattice difficulty problem may open a new situation for ensuring the security of the log system in the post-quantum era.

Based on the small integer solution problem on the lattice, this paper constructs a forward-secure lattice-based ordered aggregation signature scheme under the standard model. In order to achieve high efficiency, the scheme uses fixed-dimensional lattice-based delegation technology to realize key update and achieve forward security; then, the message to be signed and the difficulty problem on the lattice are respectively embedded into the

signature by means of message addition technology and preimage sampling algorithm. , making the signature unforgeable under the standard model, and compared with the existing lattice-based ordered aggregation signature scheme [14-17], the new scheme is still forward secure in the quantum computing environment.

II. Related Work

Definition 1 [18] (lattice) Let $B = (b_1 || b_2 || \dots || b_n)$, where $b_1, b_2, \dots, b_n \in R_m$ are n linearly independent vectors. Then the lattice Λ generated by matrix B is defined as:

$$\Lambda = L(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^n a_i b_i \mid a_i \in Z \right\}$$

At this time, n and m are the rank and dimension of Λ of the lattice respectively, and B is its basis.

Definition 2 [18] (q-ary lattice) Define m-dimensional full-rank q-ary lattice as:

$$\Lambda_q^T(A) = \{x \in Z^m \mid Ax = \mathbf{0} \pmod{q}\}$$

$$\Lambda_q^u(A) = \{x \in Z^m \mid Ax = u \pmod{q}\}$$

Among them, the parameters are prime number q , positive integers n and m , matrix $A \in Z_q^{n \times m}$, and vector $u \in Z_q^n$, and $\Lambda_q^T(A)$ and $\Lambda_q^u(A)$ are often abbreviated as $\Lambda^T(A)$ and $\Lambda^u(A)$.

Definition 3 [18] (Gaussian function) Given positive integers n and m , define the Gaussian function with $\sigma \in R^+$ as the parameter and $c \in R^m$ as the center as $\rho_{\sigma,c}(x) = \exp(-\pi ||x - c||^2 / \sigma^2)$. Define the discrete Gaussian function with c as the center and σ as the parameter on the n -dimensional lattice Λ as:

$$D_{\Lambda,\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\Lambda)}$$

Among them, the Gaussian function satisfies $\rho_{\sigma,c}(\Lambda) = \sum_{x \in \Lambda} \rho_{\sigma,c}(x)$. When the center vector $c = 0$, the discrete and Gaussian functions can be abbreviated as $D_{\Lambda,\sigma}(x)$ and $\rho_{\sigma}(x)$.

Definition 4 [19] ($D_{m \times m}$ distribution) It is known that q is a prime number, a positive integer $\geq 6n lbq$, and the parameter $\sigma \geq \sqrt{nlbq \cdot \omega(\sqrt{lbm})}$. $D_{m \times m}$ represents the distribution of the invertible matrix $A_i = [a_{i1} || a_{i2} || \dots || a_{im}]$ on the space $Z_q^{m \times m}$, where $a_{ij} \sim D_{Z^m, \sigma}, j \in [m]$.

Lemma 1 [20] (GPV08 Lattice Trapdoor Generation Algorithm) There is a probabilistic polynomial time algorithm $\text{TrapGen}(1^n)$ that takes prime number $q \geq 3$ and positive integer $m \geq 6nlbq$ as input, and can output $A \in Z_q^{n \times m}$ and lattice $\Lambda^T(A)$ short basis T of, satisfying the distribution of A is statistically indistinguishable from the uniform distribution on $Z_q^{n \times m}$, and $||T|| \leq O(n lb q)$, $||T|| \leq O(n lb q)$. Here, T represents the basis after performing Gram-Schmidt orthogonalization on T .

Lemma 2 [18] (common sampling algorithm on] lattice) Known positive integer $q \geq 2, m > n$, matrix $A \in Z_q^{n \times m}$, a set of basis T of lattice $\Lambda^T(A)$, Gaussian parameter $\sigma \geq ||T||\omega(lbm)$, and any vector $c \in R^m, u \in Z_q^n$.

(1) There is a probabilistic polynomial time algorithm $\text{SampleD}(A, T, \sigma, c)$ that can output a vector v whose distribution statistics are close to $D_{\Lambda^T(A), \sigma, c}$.

(2) There exists a probabilistic polynomial time algorithm $SamplePre(A, T, \sigma, u)$ that can output a vector v whose distribution statistics are close to $D_{\Lambda^u(A), \sigma}$.

Lemma 3 [19] (Lattice-based delegation algorithm) Input full-rank matrix $A \in Z_q^{n \times m}$, matrix $R \sim D_{m \times m}$, a set of basis T of lattice $\Lambda^T(A)$, Gaussian parameters satisfy $\sigma > ||T|| \cdot \sigma_R \sqrt{m} \cdot \omega(lb^{\frac{3}{2}}m)$, and then there is a probabilistic polynomial time algorithm $BasisDel(A, R, T, \sigma)$ that can output a set of basis T' of $\Lambda^T(AR^{-1})$, satisfying $||T'|| < \sigma / \omega(\sqrt{lbm})$. Where the Gaussian parameter satisfying $\sigma_R = \sqrt{nlbq} \cdot \omega(\sqrt{lbm})$, $D_{m \times m}$ represents the distribution of matrices in $Z^{m \times m}$ that satisfy $(D_{\sigma_R}^m)^m$ and whose modulus q is invertible. If R is the product of l matrices extracted from $D_{m \times m}$, the parameters satisfy $\sigma > ||T|| \cdot \left(\sigma_R \sqrt{m} \cdot \omega(lb^{\frac{1}{2}}m) \right)^l \cdot \omega(lbm)$.

Lemma 4 [21] Input a full-rank matrix $A \in Z_q^{n \times m}$, then there is a probabilistic polynomial time algorithm $SampleRwithBasis(A)$ that can output a matrix $R \sim D_{m \times m}$ and a set of basis T of the lattice $\Lambda^T(AR^{-1})$, satisfy $||T'|| < O(\sqrt{n lb q})$.

Definition 5 [18] (Small integer solution problem on the lattice, $SIS_{q,m,\beta}$) Given a random matrix $A \in Z_q^{n \times m}$ and a real number $\beta > 0$, the so-called small integer solution (SIS) problem on the lattice That is to find a vector $v \in Z^m$ satisfying $Av = 0 \bmod q$ and $0 < ||v|| \leq \beta$.

Lemma 5 [22] (Difficulty Reduction of Small Integer Solving Problems) Knowing any polynomially bounded real number $m, \beta = poly(n)$ and prime number $q \geq \beta \cdot \omega(\sqrt{n lb n})$, solve the $SIS_{q,m,\beta}$ of the average instance the difficulty of the problem is comparable to that of solving the shortest independent vectors problem ($SIVP_\gamma$) under the worst instance on the lattice, where $\gamma = \beta \cdot \alpha(n)$.

III. Proposed Model

3.1 Ordered Aggregate Signature

This chapter describes the definition of forward-safe ordered aggregate signature and security proof as follows.

Definition 6 (forward secure ordered aggregate signature scheme) A complete forward secure ordered aggregate signature scheme consists of six polynomial time algorithms, which are the system establishment algorithm $Setup$, the signature key generation algorithm $FssAgg - Keygen$, and the signature private key Extraction algorithm $FssAgg - Extract$, signature key update algorithm $FssAgg - KeyUpdate$, aggregate signature algorithm $FssAgg - Sign$ and signature verification algorithm $FssAgg - Verify$.

Setup: Taking the system security parameter n as input, KGC generates and outputs the system public parameter PP .

$FssAgg - Keygen$: Input PP , and KGC runs the algorithm to output the master/private key pair (msk, mpk) .

$FssAgg - Extract$: Taking user U 's identity id as input, the algorithm generates user U 's key $sk_{id|0}$.

$FssAgg - KeyUpdate$: The private key $sk_{id|i-1}$ of the previous time period and the current time period i are input, the algorithm calculates and outputs the signature private key $sk_{id|i}$ of the current period i .

$FssAgg - Sign$: Input the message m_i to be signed and the previous aggregate signature $sk_{id|i-1}$, the algorithm uses $sk_{id|i}$ to calculate the aggregate signature sig_i of the output period i .

$FssAgg - Verify$: Input aggregate signature sig_i and message set $m_j (j \leq i)$, if and only if the aggregate signature sig_i is the legal signature of message set $m_j (j \leq i)$, the algorithm output is "1", otherwise it outputs "0".

3.2 Correctness And Forward Enforceability

In general, forward-secure ordered aggregate signatures should satisfy the following two conditions: correctness and forward unforgeability.

Definition 7 (Correctness) In the forward-secure ordered aggregation signature scheme above, the correctness of the signature scheme means that $FssAgg - Verify$ can output "1" with a probability of approximately 1.

Definition 8 [23] (The existence of forward security cannot be forged) If there is no polynomial time adversary A can win the following game with non-negligible probability, then the $Fss - Agg$ signature scheme is said to be forward-secure under the aggregation attack model Existence cannot be forged.

Setup: Input the security parameter n , and the adversary gets the system public parameter PP.

Queries: Adversary A can make the following queries of polynomial order.

(1) $FssAgg - Extract\ Queries$: Input the identity id of user U , and challenger C returns its key $sk_{id|0}$.

(2) $Break\ in\ Queries$: When adversary a makes a Breakin Queries query for period j , challenger C returns the signature private key $sk_{id|j}$ of this period to the adversary.

(3) $FssAgg - Sign\ Queries$: Taking the current period i , the message to be signed m_i , the private key $sk_{id|i}$, and the previous signature sk_{i-1} as input, the challenger C returns the aggregated signature sk_i of the current period i to the adversary A.

Forgery: After finishing the above query, adversary A outputs the aggregated signature sig_k for messages m_1, m_2, \dots, m_k . Adversary A wins the above game if and only if the following conditions are met: (1) signature sig_k satisfies correctness; (2) signature sig_k is non-trivial, that is, there exists at least one time period $i^* \in [k]$ not Perform aggregate signature query on messages m_1, m_2, \dots, m_{i^*} ; (3) $1 \leq i^* < j \leq k$.

3.3 Aggregation signature scheme

Based on the difficulty of lattice, this chapter constructs a forward-secure lattice-based ordered aggregation signature scheme under the standard model. Compared with the traditional signature scheme on the lattice, in order to achieve efficient forward security, the scheme uses the fixed-dimensional lattice-based delegation technology to realize the key update; the above hard problem is embedded into the signature, making the signature un-forgeable under the standard model.

Let n be a security parameter, prime number $q \geq \beta \cdot \omega(\ln n)$, $\beta = poly(n)$, $m \geq 6n \ln q$, $L \leq O(\sqrt{n \ln q})$. Then the forward-secure ordered aggregation signature scheme on lattice is described as follows.

Setup: Input the security parameter n of the system, and the KGC generates the system public parameter PP as follows. k is the pre-specified number of time periods and Gaussian parameters $(\sigma_0, \sigma_1, \dots, \sigma_k)$, Gaussian parameters $(\sigma'_0, \sigma'_1, \dots, \sigma'_k)$, where $\sigma_i \geq Lm^i \cdot \omega(\ln^{i+1} m)$, $\sigma'_i \geq \sigma_i \cdot \omega(\sqrt{\ln m})$, $\eta \geq m \cdot \sqrt{\omega \ln m}$, t_1, t_2, l is a positive integer. $2(k+1)t_1$ random matrices $R_{i,j}^0, R_{i,j}^1 \leftarrow D_{m \times m}(i \in \{0, 1, \dots, k\}, j \in [t_1])$, t_2 random matrices satisfying $C_i \leftarrow Z_q^{n \times m}(i \in [t_2])$. The three hash functions are $H: \{0, 1\}^* \rightarrow \{0, 1\}^{t_1}$, $H': \{0, 1\}^* \rightarrow \{0, 1\}^{t_2}$, $H1: \{0, 1\}^* \rightarrow \{0, 1\}^{l_1}$ and $G_{f_A}: \{0, 1\}^{l_1} \rightarrow Z_q^n$, and the trapdoor function $f_A: Z_q^m \rightarrow Z_q^n$ and the encryption function $enc: \{0, 1\}^* \rightarrow \{0, 1\}^* \times Z_q^n$ and the decryption function $dec: \{0, 1\}^* \times Z_q^n \rightarrow \{0, 1\}^*$.

$FssAgg - KeyGen$: Input the public parameter PP, KGC runs the trapdoor generation algorithm $TrapGen(1^n)$ in **Lemma 1** to generate lattice $\Lambda^T(A)$, and its trapdoor base $T \in Z^{m \times m}$, satisfying $A \in Z_q^{n \times m}$, $\|T\| \leq L$. Finally, KGC saves the matrices A and T as the master public key and master private key, respectively.

$FssAgg - Extract$: In order to obtain the key of user U (identity is id), KGC first calculates the hash value $H(id|0) = \rho_0 = \rho id|0$, $R_0 = R_{0,t_1}^{\rho_0[t_1]}$, $R_{0,t_1-1}^{\rho_0[t_1-1]} \dots R_{0,1}^{\rho_0[1]}$. Then run the lattice-based delegation algorithm

$BasisDel(A, R_0, T, \sigma_0)$ in **Lemma 3** to output the matrix $T_{id|0} = [t_1 || t_2 || \dots || t_m]$ as the key $sk_{id|0}$. Finally, KGC sends $T_{id|0}$ to user U.

FssAgg – KeyUpdate: Input the key $T_{id|i-1}$ and the current period i , KGC first calculates $R_i = R_{i,t_1}^{\rho_{i,t_1}} R_{i,t_1-1}^{\rho_{i,t_1-1}} \dots R_{i,1}^{\rho_{i,1}}$, $R_{id|i-1} = R_{i-1} R_{i-2} \dots R_0$ and the matrix $A_{id|i-1} = A R_{id|i-1}^{-1}$. Subsequently, KGC runs the lattice-based delegation algorithm $BasisDel(A_{id|i-1}, R_i, T_{id|i-1}, \sigma_i)$ to generate the signature private key $T_{id|i}$ for the current period.

FssAgg – Sign: Input the current message m_i and the current period i , the signature algorithm works as follows:

(1) If $i = 1$, then

(2) $\Sigma_0 \leftarrow (e, e, e, e, 0^n)$, end.

Where e represents an empty string or an empty vector, if $i = 2, 3, \dots, k$, it is performed as follows.

(3) Split Σ_{i-1} into $(f \cdot Aid|i, m \cdot i-1, \alpha \cdot i-1, sig_{i-1}, h'i-1)$,

Where $f \cdot Aid|i$ is lattice trap A set of gate functions, satisfying $f \cdot Aid|i = fAid|1 || fAid|2 || \dots || fAid|i$, sig_{i-1} is the aggregate signature of the previous period, α_{i-1} is the encrypted signature of sig_{i-1} , $\alpha \cdot i-1$ is the set of encrypted signatures, that is, $\alpha \cdot i-1 = \alpha_1 || \alpha_2 || \dots || \alpha_{i-1}$; $h'i-1$ is the hash value with a constant length l .

(4) If $FssAgg-Verify(\Sigma_{i-1}) == (\perp, \perp)$, then end.

(5) Calculate $(\alpha_i, \beta_i) \leftarrow encfAid|i(sig_{i-1})$.

(6) Set $\alpha \cdot i = \alpha \cdot i-1 || \alpha_i$.

(7) Calculate $h_i = h_{i-1} \oplus H1(f \cdot Aid|i, m \cdot i, \alpha \cdot i-1, sig_{i-1})$.

(8) Calculate $g_i \leftarrow GfAid|i(h_i)$.

(9) Choose a random string $r_i \in \{0,1\}^n$ and calculate the vector

IV. Result Analysis

Currently, there are schemes [14-17] for the existing ordered aggregation signatures on the grid, and they are all signature schemes under the random oracle model. This section compares the efficiency of the ordered aggregation signature scheme on the lattice with the previous signature scheme from three aspects: public key, private key, and signature size; see Table 1 for details. Among them, the parameters satisfy $L \leq O(n \log q)$, $M = \omega(\log m)$, $m \geq 5n \log q$, k represents the number of periods specified in Section 3.1, I represents the stage of the current classification, and $i = 1, 2, \dots, k$. It is easy to see from Table 1 that the public key, signature private key, and signature size of the schemes in [14-17] are all equivalent. However, the forward-secure aggregate signature scheme proposed in this paper adopts the grid-based delegation technology to achieve forward security. Therefore, compared with the literature [14-17], the private key and signature length will vary with the classification (i.e.) increases with increasing. Therefore, it can be understood that the new scheme sacrifices a slightly larger signature private key size and signature size in exchange for higher security guarantees, thereby adapting to a more stringent security environment. The specific implementation of the signature scheme can be completed in the C++ language with the help of the FLINT library.

Based on the model, numerical simulations are performed to verify the information dissemination performance with blockchain support in the lattice model and compare the results with the information dissemination performance without blockchain support. Assuming simulations in a fixed population of $T(u) + J(u) + S(u) = 5000$, the process of information propagation from the initial stage $u = 0$ to the end-stage $u = 20$ is studied. In the two cases of the above information dissemination process, as shown in Figure 1-2, when the contract node exists, the user's dissemination behavior is shown in Figure 2. When the contract node does not exist, as shown in Figure 2 with table, From the analysis of the above figure, it can be seen that the number of communicators in the model without contract nodes exceeds 80% compared with the existence of contract nodes and the non-existence of contract nodes. Conversely, with the addition of contract nodes, the number of information communicators decreases to 20%, indicating that user information dissemination in the blockchain lattice is rationalized. User information in the blockchain environment can better completely curb distorted news than traditional lattice information dissemination, and the dissemination is relatively stable.

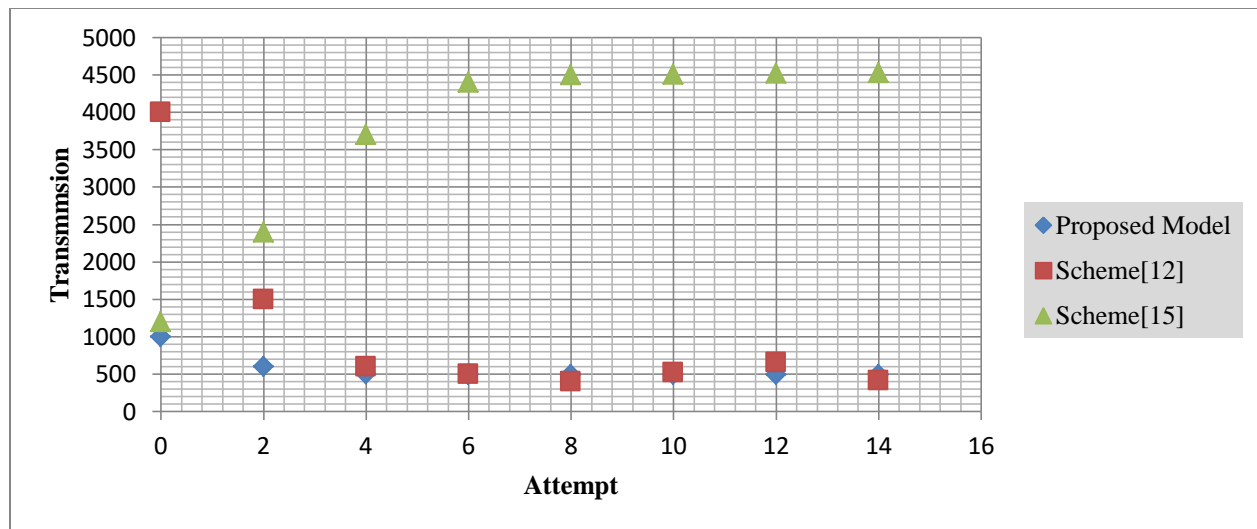


Figure 1: Attack transmission over the lattice

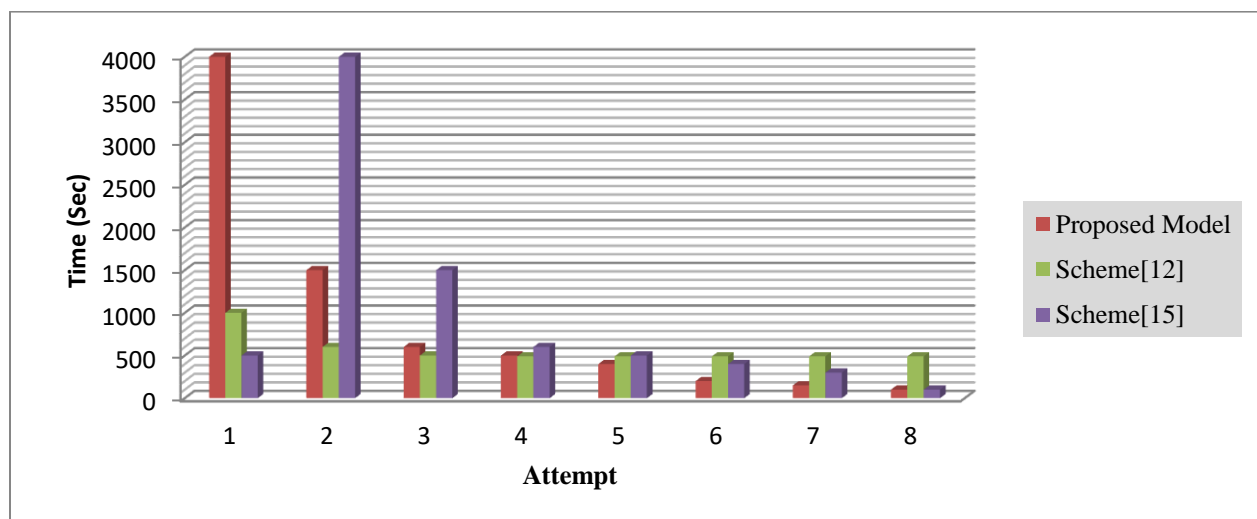


Figure 2: Attack Time over the lattice

V. Conclusion

Due to the advantages of both forward security and small storage space, the forward-secure ordered aggregate signature scheme has been widely used in log systems once it was proposed. However, with the gradual commercialization of quantum computers, the existing forward-secure ordered aggregation signature scheme can no longer meet the security requirements. Therefore, finding forward-secure rated aggregation signature schemes with quantum immunity is imperative. It is not difficult to see in the three-round post-quantum cryptography alternatives announced by the National Institute of Standards and Technology that lattice public key cryptography occupies a pivotal position, so compared with hash-based public key cryptography and encoding-based public key In terms of cryptographic systems and multivariate public key cryptosystems, lattice public key cryptography is undoubtedly the best choice for cryptographic standards in the post-quantum era. Based on the lattice-hard problem——SIS problem, this paper proposes a quantum-safe forward-safe ordered aggregation signature scheme under the standard model. The system realizes critical updates using fixed-dimensional lattice-based delegation technology and achieves forward security; then, the message to be signed and the difficulty problem on the lattice are respectively embedded into the signature through the message addition technology and the preimage sampling algorithm so that the signature is in the standard Models are unforgeable. To further compress the block size in the blockchain, the construction of the ordered aggregate signature of the specified verifier will be the focus of the follow-up work.

Reference

- [1] Y. Quan, "Improving Bitcoin's Post-Quantum Transaction Efficiency With a Novel Lattice-Based Aggregate Signature Scheme Based on CRYSTALS-Dilithium and a STARK Protocol," in *IEEE Access*, vol. 10, pp. 132472-132482, 2022, doi: 10.1109/ACCESS.2022.3227394.
- [2] Q. Li, M. Luo, C. Hsu, L. Wang and D. He, "A Quantum Secure and Noninteractive Identity-Based Aggregate Signature Protocol From Lattices," in *IEEE Systems Journal*, vol. 16, no. 3, pp. 4816-4826, Sept. 2022, doi: 10.1109/JSYST.2021.3112555.
- [3] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," in *IEEE Access*, vol. 7, pp. 134422-134433, 2019, doi: 10.1109/ACCESS.2019.2941905.
- [4] P. Zheng, Q. Xu, Z. Zheng, Z. Zhou, Y. Yan and H. Zhang, "Meepo: Multiple Execution Environments per Organization in Sharded Consortium Blockchain," in *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3562-3574, Dec. 2022, doi: 10.1109/JSAC.2022.3213326.
- [5] C. Xu, Y. Qu, T. H. Luan, P. W. Eklund, Y. Xiang and L. Gao, "A Lightweight and Attack-Proof Bidirectional Blockchain Paradigm for Internet of Things," in *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4371-4384, 15 March 15, 2022, doi: 10.1109/JIOT.2021.3103275.
- [6] P. Zheng et al., "Aeolus: Distributed Execution of Permissioned Blockchain Transactions via State Sharding," in *IEEE Transactions on Industrial Informatics*, vol. 18, no. 12, pp. 9227-9238, Dec. 2022, doi: 10.1109/TII.2022.3164433.
- [7] J. Qian, Z. Cao, X. Dong, J. Shen, Z. Liu and Y. Ye, "Two Secure and Efficient Lightweight Data Aggregation Schemes for Smart Grid," in *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 2625-2637, May 2021, doi: 10.1109/TSG.2020.3044916.
- [8] Y. -C. Chan and S. A. Jafar, "Secure GDoF of the Z-Channel With Finite Precision CSIT: How Robust are Structured Codes?," in *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2410-2428, April 2022, doi: 10.1109/TIT.2021.3137151.
- [9] Y. Yang, Y. Chen and F. Chen, "A Compressive Integrity Auditing Protocol for Secure Cloud Storage," in *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1197-1209, June 2021, doi: 10.1109/TNET.2021.3058130.

- [10] J. Qian, Z. Cao, M. Lu, X. Chen, J. Shen and J. Liu, "The Secure Lattice-Based Data Aggregation Scheme in Residential Networks for Smart Grid," in *IEEE Internet of Things Journal*, vol. 9, no. 3, pp. 2153-2164, 1 Feb.1, 2022, doi: 10.1109/JIOT.2021.3090270.
- [11] X. Lu, W. Yin, Q. Wen, Z. Jin and W. Li, "A Lattice-Based Unordered Aggregate Signature Scheme Based on the Intersection Method," in *IEEE Access*, vol. 6, pp. 33986-33994, 2018, doi: 10.1109/ACCESS.2018.2847411.
- [12] Q. Li, M. Luo, C. Hsu, L. Wang and D. He, "A Quantum Secure and Noninteractive Identity-Based Aggregate Signature Protocol From Lattices," in *IEEE Systems Journal*, vol. 16, no. 3, pp. 4816-4826, Sept. 2022, doi: 10.1109/JSYST.2021.3112555.
- [13] Y. Yao, Z. Zhai, J. Liu and Z. Li, "Lattice-Based Key-Aggregate (Searchable) Encryption in Cloud Storage," in *IEEE Access*, vol. 7, pp. 164544-164555, 2019, doi: 10.1109/ACCESS.2019.2952163.
- [14] K. O. -B. O. Agyekum, Q. Xia, E. B. Sifah, C. N. A. Cobblah, H. Xia and J. Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," in *IEEE Systems Journal*, vol. 16, no. 1, pp. 1685-1696, March 2022, doi: 10.1109/JSYST.2021.3076759.
- [15] P. Alemany, R. Vilalta, R. Munoz, R. Casellas and R. Martinez, "Evaluation of the abstraction of optical topology models in blockchain-based data center interconnection," in *Journal of Optical Communications and Networking*, vol. 14, no. 4, pp. 211-221, April 2022, doi: 10.1364/JOCN.447833.
- [16] R. Chen et al., "BIIdM: A Blockchain-Enabled Cross-Domain Identity Management System," in *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 44-58, March 2021, doi: 10.23919/JCIN.2021.9387704.
- [17] F. D. Giraldo, B. Milton C. and C. E. Gamboa, "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept," in *IEEE Latin America Transactions*, vol. 18, no. 10, pp. 1743-1751, October 2020, doi: 10.1109/TLA.2020.9387645.
- [18] S. Yao et al., "Blockchain-Empowered Collaborative Task Offloading for Cloud-Edge-Device Computing," in *IEEE Journal on Selected Areas in Communications*, vol. 40, no. 12, pp. 3485-3500, Dec. 2022, doi: 10.1109/JSAC.2022.3213358.
- [19] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao and Y. Xiang, "A Blockchained Federated Learning Framework for Cognitive Computing in Industry 4.0 Networks," in *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2964-2973, April 2021, doi: 10.1109/TII.2020.3007817.
- [20] A. Wellington dos Santos Abreu, E. F. Coutinho and C. Ilane Moreira Bezerra, "Performance Evaluation of Data Transactions in Blockchain," in *IEEE Latin America Transactions*, vol. 20, no. 3, pp. 409-416, March 2022, doi: 10.1109/TLA.2022.9667139.
- [21] W. Liang, D. Zhang, X. Lei, M. Tang, K. -C. Li and A. Y. Zomaya, "Circuit Copyright Blockchain: Blockchain-Based Homomorphic Encryption for IP Circuit Protection," in *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 3, pp. 1410-1420, 1 July-Sept. 2021, doi: 10.1109/TETC.2020.2993032.
- [22] H. Xiong et al., "On the Design of Blockchain-Based ECDSA With Fault-Tolerant Batch Verification Protocol for Blockchain-Enabled IoMT," in *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977-1986, May 2022, doi: 10.1109/JBHI.2021.3112693.
- [23] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han and F. -Y. Wang, "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 11, pp. 2266-2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

Close

"Blockchain-Aware Secure Lattice Aggregate Signature Scheme"

Original Submission

Reviewer/s Recommendation Term:

Major revisions necessary

Comments to Author:

1. The review could benefit from a comparison table that highlights the features and limitations of each discussed method. This would visually enhance the understanding of where the proposed scheme stands relative to existing solutions.
2. Ensure all technical terms and definitions are accessible to readers not familiar with lattice cryptography. Adding simple examples or visual aids might help in understanding complex concepts like q-ary lattices.
3. Provide more intuitive explanations or graphical representations for the lemmas to make the mathematical concepts more accessible to practitioners who might not have a deep mathematical background.
4. A detailed flowchart of the algorithmic steps involved in the signature scheme would enhance readability and comprehension, especially outlining the interactions between different algorithmic components.
5. A more detailed security proof regarding forward security and resistance to quantum attacks is needed. This should ideally include reductions to well-known hard problems or simulations demonstrating resistance to quantum algorithms.
6. Adding more detail about the setup conditions, like hardware specifics and software versions, would help in replicating the experiments, which is crucial for scientific validation.
7. Discuss the computational complexity in more detail, possibly including Big O notation for the major steps in the key generation, signing, and verification processes.
8. Include benchmarks against non-lattice based schemes to highlight the efficiency gains or losses with the proposed approach, using a variety of metrics such as execution time and memory usage.
9. Elaborate on specific features of the lattice problems used that contribute to quantum resistance. Discuss any known quantum algorithms that might impact the security assumptions of the proposed scheme.
10. Discuss potential real-world applications and deployment scenarios for this signature scheme. Address any implementation challenges or operational considerations that might affect its viability in production environments.
11. Suggest areas for further research, such as integration with other blockchain technologies or improvements in the efficiency of lattice operations.

Close






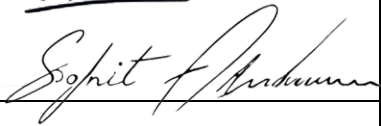


FACULTY POSITION RECLASSIFICATION FOR SUCS
(DBM-CHED Joint Circular No. 3, series of 2022)


CERTIFICATION OF PERCENTAGE CONTRIBUTION
(Research Output with Multiple Authors)

Title of Research: Blockchain-Aware Secure Lattice Aggregate Signature Scheme
Type of Research Output: Book Chapter (Scopus-Indexed, CRC Press (Taylor & Francis))

Instruction: Supply ALL the names of the authors involved in the publication of Research output and indicate the contribution of each author in percentage. Each author shall sign the conforme column if he/she agrees with the distribution. The conforme should be signed by all the authors in order to be considered. Please prepare separate Certification for each output.

	Name of Authors	Current Affiliations	% Contribution	Conforme <i>(Sign if you agree with the % distribution)</i>
1	Motashim Rasool	SR Institute of Management & Technology	16.67%	
2	Arun Khatri	JK Business School	16.67%	
3	Renato R. Maaliw III	SLSU	16.67%	
4	G. Manjula	RMK College of Engineering & Technology	16.67%	
5	Kishan Varma	VFSTR University	16.67%	
6	Sohit Agrawal	SGV University	16.67%	
<i>* Should have a total of 100%</i>			100.00%	

Prepared by:


Renato R. Maaliw III, DIT
(Name and Signature)
Faculty

Certified by:

Nicanor L. Guinto, Ph.D
(Name and Signature)
Director, Office of Research Services