Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 8431874, 14 pages
https://doi.org/10.1155/2022/8431874

Research Article

Efficient Linkable Ring Signature Scheme over NTRU Lattice with Unconditional Anonymity

Qing Ye, Mengyao Wang, Hui Meng, Feifei Xia, and Xixi Yan

School of Software, Henan Polytechnic University, Jiaozuo 454000, China

Correspondence should be addressed to Hui Meng; menghui@hpu.edu.cn

Received 18 March 2022; Revised 2 April 2022; Accepted 7 April 2022; Published 13 May 2022

Academic Editor: Le Sun

In cloud and edge computing, senders of data often want to be anonymous, while recipients of data always expect that the data come from a reliable sender and they are not redundant. Linkable ring signature (LRS) can not only protect the anonymity of the signer, but also detect whether two different signatures are signed by the same signer. Today, most lattice-based LRS schemes only satisfy computational anonymity. To the best of our knowledge, only the lattice-based LRS scheme proposed by Torres et al. can achieve unconditional anonymity. But the efficiency of signature generation and verification of the scheme is very low, and the signature length is also relatively long. With the preimage sampling, trapdoor generation, and rejection sampling algorithms, this study proposed an efficient LRS scheme with unconditional anonymity based on the e-NTRU problem under the random oracle model. We implemented our scheme and Torres et al.'s scheme, as well as other four efficient lattice-based LRS schemes. It is shown that under the same security level, compared with Torres et al.'s scheme, the signature generation time, signature verification time, and signature size of our scheme are reduced by about 94.52%, 97.18%, and 58.03%, respectively.

1. Introduction

In most scenarios involving data transmission, including blockchain, cloud computing, edge computing, etc., the sender of data usually wants to be anonymous, while the receiver of data always excepts the data to be reliable. Ring signature (RS) proposed by Rivest et al. [1] is a good technology that can meet the above requirements. RS has two essential security properties: (1) unforgeability, which requires the verifier is able to verify whether the signature was signed by a reliable signer; and (2) anonymity, which requires the verifier could not identify the real signer from a group of users. Similar to group signature [2, 3], RS is group-oriented. However, different from group signature, in RS, the group is formed spontaneously, that is, there is no special manager, and the setup and revocation procedures are not required. Any user can select a group of ring members and sign any message with his own private key and the public keys of other members without their consent. And the verifier only can verify whether the signature comes from a member in the ring without knowing which member the signer is.

Due to the anonymity of RS, it is widely used in anonymous tip off, e-cash [4], and other fields. It is worth noting that while protecting the anonymity of signers, RS also brings a new problem, that is, the same signer can sign multiple times without being detected.

In 2004, Liu et al. [5] introduced an extended property called linkability to RS, and the corresponding primitive is now known as linkable ring signatures (LRS). LRS not only satisfies the properties of ordinary RS (such as correctness, unforgeability, and anonymity) but also can be used to judge whether two different signatures are signed by the same signer (linkability). LRS is useful in situations where anonymity and nonrepeatability are required. For example, in the system of blockchain [6], if some user signs the same amount of money twice, LRS will help the verifier detect it and the verifier will deny the second signature, thus avoiding the so-called "double spending" problem. In smart grid systems [7], the electricity consumption data of users are automatically collected by the smart meter, and specific electricity consumption information is fed back to the service provider. Thus, malicious attackers can infer the life and rest rules of the user from the large amount of electricity

consumption data recorded by the smart meter. LRS can not only conceal the specific information of the meter user but also eliminate the redundant data of the same meter and provide the system with abnormal user monitoring and tracking functions.

In 2013, Liu et al. [8] constructed an unconditional anonymous linkable ring signature (UALRS) scheme, which addressed the open problem that RS could not have linkability and strong anonymity simultaneously and made it more secure. RS schemes have two types of anonymity: computational anonymity and unconditional anonymity. Computational anonymity refers to the protection of anonymity under certain number theory problems. The anonymity of RS is destroyed if this potential problem can be solved by an adversary. By contrast, unconditional anonymity means that the probability that any adversary with unlimited computing power and time knows the actual signer of a given RS is no better than random guessing. In other words, assuming that there are l users in RS, the probability of any adversary with unlimited computing power and time correctly indicating the public key of the actual signer is no more than $1/l$.

It is not difficult to design a RS scheme with unconditional anonymity. In fact, most traditional RS schemes can satisfy unconditional anonymity [1, 9–16]. However, it is not an easy work to construct a UALRS scheme. The difficulty lies in the following two aspects. First, in a computational anonymous linkable ring signature (CALRS) scheme, the linking tag can always be designed as a pseudorandom function about the private key of the signer based on some mathematical problem. But unconditional anonymity means that the adversary has unlimited computing power, that is it can calculate out the solution of any NP-hard problem, such as NTRU-SIS, large integer factorization, discrete logarithm, and the preimage of a given hash value. Therefore, only designing the linking tag using mathematical problems is not enough, and it should consider more skills. Second, in order to achieve unconditional anonymity, the generation and verification of a linking tag are often more complex, which may increase the length of public and private keys and signatures, as well as reduce the computational efficiency of the scheme. In fact, from 2004 to 2013, only the LRS scheme proposed by Liu et al. [8] can achieve unconditional anonymity.

The above schemes are all constructed based on classical number theory problems, that is, discrete logarithm and the decomposition of large integer problems. With the development of quantum computers, cryptosystems under classical number theory problems are faced with severe challenges. Shor [17] constructed a quantum algorithm in 1994 to solve the problem of large integer factorization in polynomial time under quantum computing conditions, and this algorithm made most existing public key cryptosystems no longer secure under quantum attacks.

In this case, post-quantum cryptography began to be studied by scholars in the field of cryptography. In the alternatives, lattice-based cryptography appeals to scholars because of its high efficiency, simplicity, high parallelizability, and strong provable security guarantees. In 2016, Libert et al. [18] constructed a lattice-based RS scheme based on zero-knowledge proofs and accumulators. Thereafter, other lattice-based RS schemes have been proposed [19–21]. In 2017, Yang et al. [22] proposed a lattice-based LRS scheme based on week pseudorandom functions, accumulators, and zero-knowledge proofs. In 2018, Baum et al. [23] proposed the lattice-based one-time LRS scheme based on the module-SIS problem (a variant of SIS problem) and module-LWE problem (a variant of LWE problem). In the same year, Alberto Torres et al. [24] proposed a lattice-based one-time LRS scheme based on the ring-SIS problem. Subsequently, Zhang et al. [25] proposed a LRS scheme over ideal lattice based on the homomorphic commitment scheme and $\sum$ protocol. In 2019, Liu et al. [26] proposed a lattice-based LRS scheme supporting stealth addresses under the module-SIS and module-LWE problems. In 2020, Beullens et al. [27] constructed a LRS scheme whose signature size scales logarithmically with the ring size from isogeny and lattice assumptions.

However, in the above lattice-based LRS schemes, only Alberto Torres et al.'s scheme [24] satisfies unconditional anonymity. By analyzing Torres et al.'s scheme, it is found that in order to achieve unconditional anonymity, the linking tag of Torres et al.'s scheme is generated using an m-dimensional polynomial vector over a polynomial ring. Since the linking tag is so large, Torres et al.'s scheme generates signatures m times longer than a normal CALRS scheme over a polynomial ring, and its efficiency in generating and verifying signatures is also significantly reduced.

Hoffstein et al. [28] proposed the NTRU lattice-based cryptosystem in 1996. Considering that it only involves multiplication on polynomial rings and small integer modulo operations, the NTRU-based cryptosystem usually requires smaller public and private keys and is more efficient compared with that on the general lattice. Therefore, it has received extensive attention from scholars. In 2016, Zhang et al. [29] proposed an efficient RS scheme on NTRU lattice whose security can be reduced to the e-NTRU problem (a variant of the SIS problem on NTRU lattice) in the random oracle model. In 2019, Lu et al. [30] constructed Raptor, a practical NTRU lattice-based LRS scheme based on a variant of chameleon hash functions. In 2021, Tang et al. [31] constructed an identity-based LRS scheme over NTRU lattice by employing the technologies of trapdoor generation and rejection sampling. The security of this scheme relies on the small integer solution (SIS) problem on NTRU lattice.

1.1. Our Contribution. To reduce the signature size, as well as promote the efficiency of signature generation and verification of lattice-based UALRS scheme [24], in this study, a LRS scheme is reconstructed on NTRU lattice, and its architecture is shown in Figure 1. The main contributions of this article are as follows:

(1) In the key generation stage, the public and private keys of the LRS scheme are generated by the trapdoor and the preimage sampling algorithms on NTRU lattice. Then, the linking tag is produced by the public and private keys of the signer, and a LRS

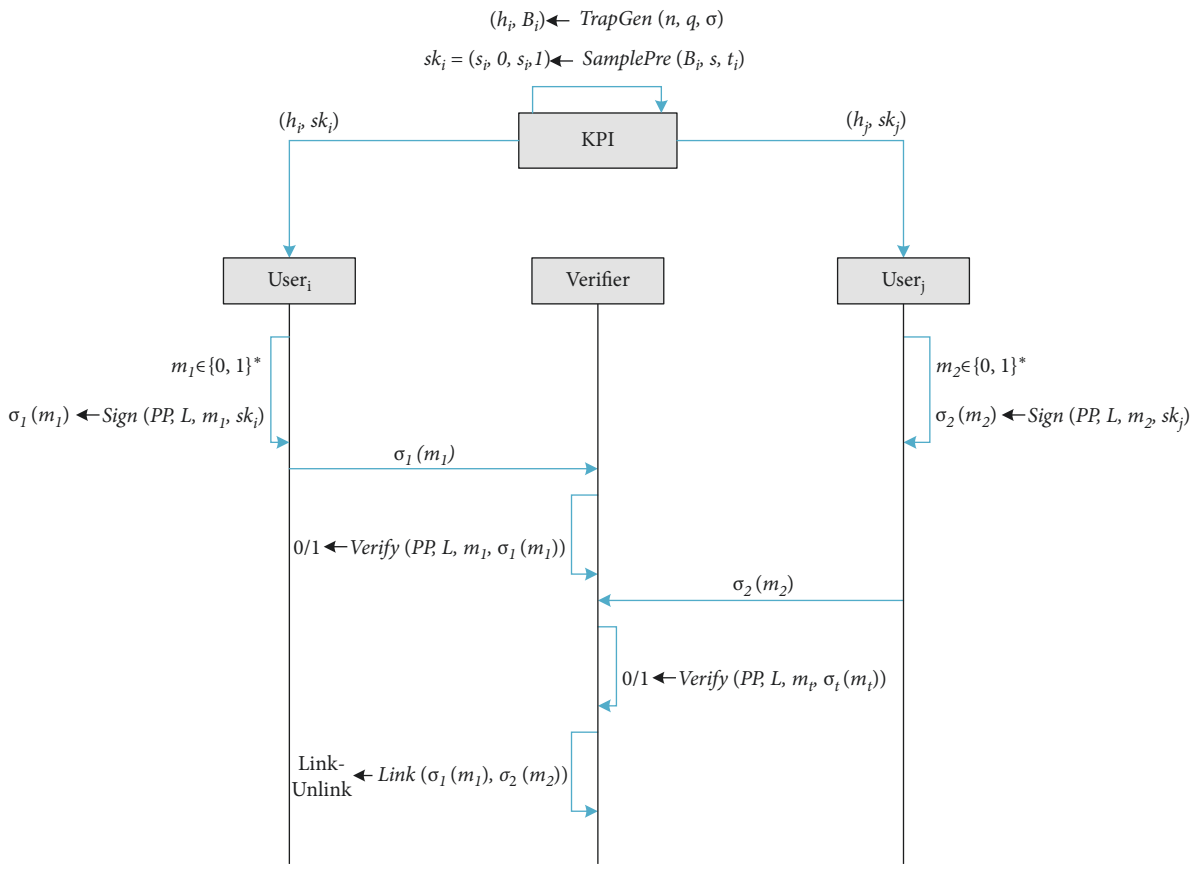

Figure 1: Linkable ring signature on NTRU lattice.

is generated based on the signature algorithm of Zhang et al. [29] combined with the rejection sampling algorithm.

(2) In terms of security analysis, strict security proof is conducted based on the security model of UALRS proposed by Liu et al. [8]. The result of the proof shows that the unforgeability and linkability of the proposed scheme can be reduced to the difficulty of e-NTRU problem under the random oracle model, and, meanwhile, the proposed scheme satisfies unconditional anonymity.

(3) In terms of performance analysis, the proposed scheme is compared with the latest and efficient lattice-based LRS schemes in [23, 24, 26, 27, 30], and a detailed analysis is given. The possible parameter settings of the proposed scheme are also analyzed and provided under the premise of ensuring the security of the proposed scheme.

(4) We implement our scheme and Torres et al.'s scheme [24], as well as other four efficient lattice-based LRS schemes [23, 26, 27, 30], and it is shown that under the same security level, the signature generation and verification time of the proposed scheme are respectively reduced by 56.61% and 65.18%. Especially compared with Torres et al.'s scheme, the signature generation and verification time of the proposed scheme are respectively reduced by 94.52% and 97.18%, and the signature size of the proposed scheme is reduced by 58.03% on average.

1.2. Paper Organization. In Section 2, we introduce some definitions, lemmas, difficult problems, and related algorithms which we will use to construct the scheme. We introduce the definition of LRS and the relevant security model in Section 3. Section 4 contains the construction and correctness statement of the LRS scheme and the proof of correctness. Section 5 contains the security statements of the proposed scheme and the proofs of unforgeability, unconditional anonymity, and linkability. In Section 6, we discuss the parameter settings and post-quantum security of the proposed scheme. Finally, in Section 7 and Section 8, we respectively give the performance analysis and experimental results of the proposed scheme and the lattice-based LRS schemes of [23, 24, 26, 27, 30] and also make a comparison between them.

2. Preliminaries

2.1. Symbol Definition. Descriptions of the used notations are listed in Table 1.

2.2. Related Definitions of NTRU Lattice

Definition 1 (lattice). Lattice Λ generated by m linearly independent vectors $\mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_m \in \mathbb{R}^n$ is the set of linear

Table 1: Symbol description.

Notations	Explanation
$\mathbb{R}$	Set of real numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Z}_q$	Set of integers modulo q
$\mathbb{Z}^m$	Set of m-dimensional column vectors over $\mathbb{Z}$
$\mathbb{Z}_q^{n\times m}$	Set of matrices of n rows and m columns over $\mathbb{Z}_q$
R	Polynomial ring $\mathbb{Z}[x]/(x^n+1)$
R_q	Polynomial ring $\mathbb{Z}_q[x]/(x^n+1)$
$\mathbf{A}$	Matrix
$\mathbf{x}$	Vector
$\mathbf{x}\leftarrow D$	Randomly choosing vector $\mathbf{x}$ from probability distribution D
$\|\mathbf{x}\|$	Euclidean norm of vector $\mathbf{x}$
$f\cdot g$	Multiplication of polynomials
$negl(n)$	Negligible function about n
$g(n)=\omega(f(n))$	$g(n)>f(n)$

combinations of all integer coefficients of the m linearly independent vectors, namely

$$\Lambda = L(\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_m) = \left\{\sum_{i=1}^{m} a_i\mathbf{b}_i | a_i\in\mathbb{Z}\right\}, \tag{1}$$

where m and n are the rank and dimension of lattice Λ, respectively, and $\mathbf{b}_1,\mathbf{b}_2,\cdots,\mathbf{b}_m$ is called a basis of lattice Λ.

Definition 2 (convolutional polynomial ring). Let $R=\mathbb{Z}[x]/(x^n+1)$ be an ordinary polynomial ring. If the addition operation remains unchanged and the multiplication operation is replaced by a convolution operation on R, then R is called a convolution polynomial ring. Similarly, given a prime number q, the modulus convolution polynomial ring is $R_q = R/qR$.

Let $f=\sum_{i=0}^{n-1} f_i x^i, g=\sum_{i=0}^{n-1} g_i x^i \in R_q$, then the two operations on R_q are defined as follows:

(i) Addition operation +:

$$f+g=\sum_{i=0}^{n-1}(f_i+g_i)x^i \bmod q \in R_q. \tag{2}$$

(ii) Convolution operation $*$:

$$f*g = f\cdot g \bmod (x^n+1) \bmod q \in R_q. \tag{3}$$

Definition 3 (anticirculant matrix). Let the coefficient vector of polynomial f be $(f_0,f_1,\cdots,f_{n-1})$. Then, the coefficient vector of polynomial $x\cdot f$ is $(-f_{n-1},f_0,\cdots,f_{n-2})$ and the coefficient vector of polynomial $x^{n-1}\cdot f$ is $(-f_1,-f_2,\cdots,f_0)$. The anti-circulant matrix defined by polynomial f is as follows:

$$\mathbf{A}_n(f)=\begin{bmatrix} f_0 & f_1 & \cdots & f_{n-1}\\ -f_{n-1} & f_0 & \cdots & f_{n-2}\\ \vdots & \vdots & \cdots & \vdots\\ -f_1 & -f_2 & \cdots & f_0 \end{bmatrix} = \begin{bmatrix} f\\ x\cdot f\\ \vdots\\ x^{n-1}\cdot f \end{bmatrix}. \tag{4}$$

Definition 4. (NTRU lattice). Let a positive integer $q\geq 2$, n is a power of two and $f,g\in R_q$, $f^{-1}\in R_q$ be the inverse of f, $h=g*f^{-1} \bmod q$. The NTRU lattice corresponding to q and h is as follows:

$$\Lambda_{q,\mathbf{h}} = \{(u,v)\in R^2 | u+v*h=0 \bmod q\}. \tag{5}$$

Apparently, lattice $\Lambda_{q,h}$ is a $2n$-dimensional full-rank lattice, and $\mathbf{A}_{q,h}=\begin{pmatrix} -\mathbf{A}_n(h) & \mathbf{I}_n\\ q\mathbf{I}_n & \mathbf{O}_n\end{pmatrix}\in\mathbb{Z}_q^{2n\times 2n}$ is a set of basis matrices. $\mathbf{A}_{q,h}$ can be uniquely determined by the polynomial $h\in R_q$, whereas the others can be compressed during storage. Thus, the storage space required is relatively small. However, in NTRU lattice-based cryptographic schemes, $\mathbf{A}_{q,\mathbf{h}}$ cannot be used as a trapdoor basis because it has poor orthogonality.

Definition 5. (discrete gaussian distribution) [32]. For any $\sigma>0$ and m-dimensional integer lattice Λ, the discrete Gaussian distribution on integer lattice Λ with vector $\mathbf{c}\in\mathbb{R}^m$ as the center and σ as the parameter is defined as follows:

$$\forall\mathbf{x}\in\Lambda, D_{\Lambda,\mathbf{c},\sigma}^m(\mathbf{x}) = \frac{\rho_{\mathbf{c},\sigma}^m(\mathbf{x})}{\rho_{\mathbf{c},\sigma}^m(\Lambda)}, \tag{6}$$

where $\rho_{\mathbf{c},\sigma}^m(\mathbf{x})=\exp(-\pi\|\mathbf{x}-\mathbf{c}^2\|/\sigma^2)$. When $c=0$, let $\rho_{\mathbf{c},\sigma}^m$ and $D_{\Lambda,\mathbf{c},\sigma}^m$ be abbreviated as ρ_σ^m and $D_{\Lambda,\sigma}^m$, respectively. And throughout the article, $D_{\mathbf{c},\sigma}^m$ denotes the discrete Gaussian distribution over $\mathbb{Z}^m$.

2.3. Hardness Assumption

Definition 6 (NTRU small-integer solution, NTRU-SIS) [33]. For a polynomial $h=g*f^{-1} \bmod q\in R_q$ and a real number $\beta>0$, to find two nonzero polynomials $(u,v)\in R_q^2$ such that $u+v*h=0 \bmod q$ and $\|u\|,\|v\|\leq\beta$.

Definition 7 (extended NTRU, e-NTRU) [29]. Given N polynomials $h_i=g_i*f_i^{-1} \bmod q\in R_q, i\in\{1,\cdots,N\}$, where $N\ll q$, to find a tuple of short polynomials $(u_i,v_i)\in R_q^2$, $u_i,v_i\neq 0 \bmod q, i\in\{1,\cdots,N\}$ such that

$$\sum_{i=1}^{N}(u_i+v_i*h_i)=0 \bmod q, \|u_i\|,\|v_i\|\leq\beta, i\in\{1,\cdots,N\}. \tag{7}$$

Theorem 1 (see [29]). *Let integer $k>0, n=2^k, q=1 \bmod 2n$ and integer $N\ll q$, then the e-NTRU problem is polynomially equivalent to the NTRU-SIS problem.*

2.4. Related Algorithm

Lemma 1 (see [34]). *Let an integer $n=2^k$ for $k>0$, a prime number $q=1 \bmod 2n$, and a parameter $\sigma=1.17\sqrt{q/2n}$. Then, a probabilistic polynomial time (PPT) algorithm $TrapGen(n,q,\sigma)$ can output a sample matrix $\mathbf{B}_{f,g}\in\mathbb{Z}_q^{2n\times 2n}$ from (a distribution close to) $D_{h,\sigma}^{2n\times 2n}$ and a polynomial $h=g*f^{-1} \bmod q\in R_q$ on the NTRU lattice $\Lambda_{h,q}$.*

Lemma 2 (see [34]). *Given a matrix* $\mathbf{B}_{f,g}$ *and a parameter* $s = 0.585/\pi\sqrt{q \ln(2 + 2/\eta)}$ *for* $\eta = 2^{-\lambda}/2n$, *where* λ *is the security parameter. For any polynomial* $t \in R_q$, *a PPT algorithm* $Sample\mathrm{Pre}(\mathbf{B}_{f,g}, s, t)$ *may output* $\mathbf{z} = (z_1, z_2) \leftarrow D_{h^{\perp}+\mathbf{c},s}$, *such that* $z_1 + z_2 * h = t$, $\|\mathbf{z}\| \le s\sqrt{2n}$.

Definition 8 (rejection sampling algorithm) [35]. In 2012, Lyubashevsky proposed rejection sampling technique for the first time and gave the first signature scheme without trapdoor on lattice with this technique. It can be applied to the signature system and can make the distributions of the signature and private key independent of each other. Thus, it can effectively prevent the leakage of the private key.

Lemma 3. *Let* $V = \{\mathbf{v} \in \mathbb{Z}^m : \|\mathbf{v}\| < t\}$, $\sigma = \omega(t\sqrt{\log m})$, *and* $h: V \longrightarrow \mathbb{R}$ *is a probability distribution. Then, for constant* $M = O(1)$, *the statistical distance of output distributions of Algorithms 1 and 2 is less than* $2^{-\omega(\log m)}/M$.

Algorithm 1. $v \leftarrow h$, $\mathbf{z} \leftarrow D^m_{\mathbf{v},\sigma}$, output $(\mathbf{z}, v)$ with probability $\min(D^m_{\sigma}(\mathbf{z})/MD^m_{\mathbf{v},\sigma}(\mathbf{z}), 1)$.

Algorithm 2. $v \leftarrow h$, $\mathbf{z} \leftarrow D^m_{\sigma}$, output $(\mathbf{z}, v)$ with probability $1/M$.

Furthermore, the output probability of Algorithm 1 is at least $1 - 2^{-\omega(\log m)}/M$.

3. Security Model

In this section, we present our security model and define related security concepts.

3.1. LRS Definition. A LRS scheme consists of the following five PPT algorithms:

(1) $\mathrm{Setup}(1^{\lambda})$: On input a security parameter λ, it outputs system public parameters PP.

(2) $\mathrm{KeyGen}(PP)$: On input the public parameters PP, it outputs a public/private key pair (pk_i, sk_i).We denote by SK and PK the domains of possible private and public keys, respectively.

(3) $\mathrm{Sign}(PP, L, m, sk_k)$: On input the public parameters PP, a public key list L, a message $m \in \{0,1\}^*$, and private key sk_k, it outputs a signature $\sigma(m)$, which contains a linking tag I.

(4) $\mathrm{Verify}(PP, L, m, \sigma(m))$: On input the system public parameters PP, a public key list L, a message $m \in \{0,1\}^*$, and a signature $\sigma(m)$, if $\sigma(m)$ is valid, it outputs "1"; otherwise, it outputs "0."

(5) $\mathrm{Link}(\sigma(m_1), \sigma(m_2))$: On input two signatures $\sigma_1(m_1), \sigma_2(m_2)$, where $\sigma_1(m_1)$ and $\sigma_2(m_2)$ are the signatures of different messages m_1 and m_2 under the same ring, which contain linking tags I_1 and I_2, respectively. It checks whether $I_1 \stackrel{?}{=} I_2$ and outputs "Link" if $I_1 = I_2$; otherwise, it outputs "Unlink." "Link" means that the two signatures are generated by the same signer, and "Unlink" means that the two signatures are generated by different signers.

Definition 9 (correctness). Correctness for LRS contains verification correctness and linking correctness simultaneously.

(i) *Verification Correctness*: For a valid signature $\sigma(m)$, the probability of the algorithm $\mathrm{Verify}(PP, L, m, \sigma(m))$ outputting "0" is negligible.

(ii) *Linking Correctness:* For two valid signatures $\sigma_1(m_1), \sigma_2(m_2)$ generated by using the same private key, the probability of the algorithm $\mathrm{Link}(\sigma(m_1), \sigma(m_2))$ outputting "Unlink" is negligible. The formal definition of the correctness of the LRS scheme is shown in the following expressions:

$$\Pr\left[\text{"0"} \leftarrow \mathrm{Verify}(PP, L, m, \sigma(m)) \;\middle|\; \begin{array}{l} PP \leftarrow \mathrm{Setup}(1^{\lambda}) \\ (pk, sk) \leftarrow \mathrm{KeyGen}(PP) \\ \sigma(m) \leftarrow \mathrm{Sign}(PP, L, m, sk) \end{array}\right] \le negl(\lambda). \tag{8}$$

$$\Pr\left[\text{"Unlink"} \leftarrow \mathrm{Link}(\sigma(m_1), \sigma(m_2)) \;\middle|\; \begin{array}{l} PP \leftarrow \mathrm{Setup}(1^{\lambda}) \\ (pk, sk) \leftarrow \mathrm{KeyGen}(PP) \\ \sigma(m_1) \leftarrow \mathrm{Sign}(PP, L_1, m_1, sk) \\ \sigma(m_2) \leftarrow \mathrm{Sign}(PP, L_2, m_2, sk) \end{array}\right] \le negl(\lambda). \tag{9}$$

3.2. Security Model. Generally, a LRS scheme should satisfy three security properties, namely unforgeability, anonymity, and linkability. According to the security model of UALRS proposed by Liu et al. [8] in 2013, this study uses a series of games between an adversary A and a challenger S to describe the security model of LRS. Supposing there are l members in the ring, these three properties are described as follows:

Before defining unforgeability, anonymity, and linkability, we consider the following oracles, which together simulate the adversary's ability to break the security of the scheme.

JO (*Joining Oracle*): A inputs member index k, and S outputs the corresponding public key $pk_k \in PK$ to A

CO (*Corruption Oracle*): A inputs a public key $pk_k \in PK$, which is a query output of *JO*, and S returns the corresponding private key $sk_k \in SK$

SO (*Signing Oracle*): A inputs a public key list $L = \{pk_i\}_{1 \le i \le l} \in PK$, and a message $m \in \{0,1\}^*$, and S returns a valid signature $\sigma(m)$

In addition, in the random oracle model, a random oracle model *HO* is provided for users to query.

3.2.1. Unforgeability. It means that users outside the ring cannot successfully forge a legal signature under the ring. That is, if there is no private key of a member in the ring, even if the adversary obtains multiple valid message signature pairs, the probability of the adversary forging a valid signature successfully is negligible. Unforgeability for the LRS scheme is defined by the following game between an adversary A and a challenger S, in which A is given access to oracles *JO*, *CO*, *SO*, and *HO*:

(i) The system public parameters PP are generated by challenger S and given to A

(ii) A can access the oracles adaptively

(iii) A gives S a list $L = \{pk_i\}_{1 \le i \le l}$ of public keys, a message $m \in \{0,1\}^*$, and a signature $\sigma(m)$

A wins the game if

(i) $\text{Verify}(PP, L, m, \sigma(m)) = "1"$

(ii) All public keys in L are obtained by querying *JO*

(iii) Any public key in L has not been input to *CO*

(iv) $\sigma(m)$ is not obtained by querying *SO*

We express it as

$$\text{Adv}_A^{\text{Unf}} = \Pr[A \text{wins the game}]. \tag{10}$$

Definition 10 (unforgeability). If the advantage $\text{Adv}_A^{\text{Unf}}$ of any PPT adversary A to win the unforgeability game is negligible, then the LRS scheme is unforgeable.

3.2.2. Unconditional Anonymity. It means that given a ring signature, no one can guess the real signer. In other words, given the public keys of all the members of the ring, it is impossible for anyone to tell the public key of the actual signer with a probability larger than $1/l$, where l denotes the cardinality of the ring, even the adversary has unlimited computing time and resources. The unconditional anonymity of LRS is described by the following game between an adversary A and a challenger S, where A is granted access to oracle *JO*:

(i) The system public parameters PP are generated by challenger S and given to A;

(ii) A can access the oracle *JO* adaptively;

(iii) A gives S a public key list $L = \{pk_i\}_{1 \le i \le l}$, which are query outputs of *JO*, and a message $m^* \in \{0,1\}^*$. S randomly samples $b \in \{1, \cdots, l\}$, uses the signature key sk_b corresponding to pk_b to run algorithm $\text{Sign}(PP, L, m, sk_b)$, and generates and gives A the signature $\sigma(m^*)$; and

(iv) A returns the guess value $b\prime \in \{1, \cdots, l\}$.

We express it as

$$\text{Adv}_A^{\text{Anon}} = \left|\Pr[b' = b] - 1/l\right|. \tag{11}$$

Definition 11 (unconditional anonymity). If the advantage $\text{Adv}_A^{\text{Anon}}$ of any unbounded adversary A to win the anonymity game is negligible, then the LRS scheme is called to be unconditional anonymous.

It is worth noting that though only *JO* is given to A, since A has unbounded computation power, it can calculate out the solution of any NP-hard problem, such as NTRU-SIS, large integer factorization, discrete logarithm, as well as the preimage of a given hash value. Therefore, unconditional anonymity in fact requires that in this case, A is still unable to reveal the pubic key of the actual signer of a RS with a probability higher than $1/l$.

3.2.3. Linkability. It means that two signatures generated by the same ring member can be linked. That is, an adversary who has less than two members' private keys in the ring cannot generate two valid signatures determined by the linking algorithm as "Unlink." The linkability of a LRS scheme is described by the following game between an adversary A and a challenger S, where A is granted access to oracles *JO*, *CO*, *SO*, and *HO*:

(i) The system public parameters PP are generated by challenger S and given to A

(ii) A can access the oracles adaptively

(iii) A gives S two sets $L_1 = \{pk_i\}_{1 \le i \le l_1}$ and $L_2 = \{pk_i\}_{1 \le i \le l_2}$, messages $m_1, m_2 \in \{0,1\}^*$, and signatures $\sigma(m_1)$ and $\sigma(m_2)$, where $\sigma(m_1)$ and $\sigma(m_2)$ contain the corresponding linking tags I_1, I_2, respectively

A wins the game if

(i) All public keys in $L_1 \cup L_2$ are query outputs of *JO*

(ii) For $i = 1, 2$, $Verify(PP, L_i, m_i, \sigma(m_i)) = "1"$ such that $\sigma(m_i)$ is not an output of *SO*

(iii) *CO* has been queried less than two times

(iv) $Link(\sigma(m_1), \sigma(m_2)) =$ "Unlink"

We express it as

$$\text{Adv}_A^{\text{Link}} = \Pr[A \text{wins the game}]. \tag{12}$$

Definition 12 (linkability). If the advantage $\text{Adv}_A^{\text{Link}}$ of any PPT adversary A to win the linkability game is negligible, then the LRS scheme is linkable.

4. Scheme Construction

(1) Setup $(1^\lambda, 1^n)$: On input the security parameter λ and integer $n = 2^k$, where $k > 0$, a ring of $l = \omega(\log n)$, a prime $q = 1 \bmod 2n$, two parameters $\sigma = 1.17\sqrt{q/2n}$ and $s = 0.585/\pi\sqrt{q \ln(2 + 2/\eta)}$, where $\eta = 2^{-\lambda}/2n$, choose a collision-resistant hash function H: $\{0,1\}^* \longrightarrow \{0,1\}^n$, and output $PP = (q, \sigma, s, H)$.

(2) $KeyGen(PP)$: On input the system public parameters PP, the following steps should be performed:

(i) Run the trapdoor generation algorithm $\mathrm{TrapGen}(n, q, \sigma)$ to generate $\{h_i \in R_q, \mathbf{B}_i \in \mathbb{Z}_q^{2n \times 2n}\}$;

(ii) Randomly choose $t_i \in R_q$, and let $sk_i = (s_{i,0}, s_{i,1}) = \mathrm{SamplePre}(\mathbf{B}_i, s, t_i)$ such that $s_{i,0} + s_{i,1} * h_i = t_i$, $\|(s_{i,0}, s_{i,1})\| \le s\sqrt{2n}$; and

(iii) Output a public key list $L = \{h_i\}_{1 \le i \le l}$, and the private key for the member i: $sk_i = (s_{i,0}, s_{i,1})$.

(3) $\mathrm{Sign}(PP, L, m, sk_k)$: On input the system public parameters PP, the public key list $L = \{h_i\}_{1 \le i \le l}$, a message $m \in \{0,1\}^*$, and a private key $sk_k = (s_{k,0}, s_{k,1})$, the member k performs the following steps:

(i) Compute linking tag

$$I = s_{k,0} + s_{k,1} * h_k. \tag{13}$$

(ii) For $1 \le i \le l$, sample random vectors $\mathbf{r}_{i,0}, \mathbf{r}_{i,1} \leftarrow D_s^n$.

(iii) Let

$$\mathbf{v} = H\left(\sum_{1 \le i \le l} \left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right), L, m, I\right). \tag{14}$$

(iv) If $i \ne k$, compute

$$\mathbf{z}_i = \left(\mathbf{z}_{i,0}, \mathbf{z}_{i,1}\right) = \left(\mathbf{r}_{i,0}, \mathbf{r}_{i,1}\right). \tag{15}$$

if $i = k$, compute

$$\mathbf{z}_k = \left(\mathbf{z}_{k,0}, \mathbf{z}_{k,1}\right) = \left(s_{k,0} * \mathbf{v} + \mathbf{r}_{k,0}, s_{k,1} * \mathbf{v} + \mathbf{r}_{k,1}\right). \tag{16}$$

(v) Continue with probability $\min(D_s^n(z_k)/MD_{s*v,s}^n(z_k), 1)$, where $M = O(1)$; otherwise restart.

(vi) Output signature $\sigma(m) = (m, (\mathbf{z}_i)_{1 \le i \le l}, \mathbf{v}, I)$.

(4) $\mathrm{Verify}(PP, L, m, \sigma(m))$: On input the system parameters PP, the public key list $L = \{h_i\}_{1 \le i \le l}$, a message $m \in \{0,1\}^*$, and a signature $\sigma(m) = (m, (\mathbf{z}_i)_{1 \le i \le l}, \mathbf{v}, I)$, output "1" if and only if the following conditions are true; otherwise, output "0":

$$\text{(i)}\mathbf{v} = H\left(\sum_{1 \le i \le l} \left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v}, L, m, I\right). \tag{17}$$

$$\text{(ii)For } 1 \le i \le l, 0 \le \left\|\left(\mathbf{z}_{i,0}, \mathbf{z}_{i,1}\right)\right\| \le s\sqrt{2n}. \tag{18}$$

(5) $\mathrm{Link}(\sigma(m_1), \sigma(m_2))$: On input two signatures $\sigma(m_1)$ and $\sigma(m_2)$, which contains linking tags I_1 and I_2, respectively, the following steps should be performed:

Verify whether $I_1 \stackrel{?}{=} I_2$. If $I_1 = I_2$, then return "Link"; otherwise, return "Unlink."

Theorem 2 (correctness). *The proposed LRS scheme satisfies correctness.*

Proof. Assuming $\sigma(m) = (m, (\mathbf{z}_i)_{1 \le i \le l}, \mathbf{v}, I)$ is a signature generated by a member of the ring according to the algorithms under public key set $L = \{h_i\}_{1 \le i \le l}$, then the following equation holds:

$$\begin{aligned}
&\sum_{1 \le i \le l} \left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v} \\
&= \mathbf{z}_{k,0} + \mathbf{z}_{k,1} * h_k - I\mathbf{v} + \sum_{1 \le i \le l, i \ne k} \left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) \\
&= \left(s_{k,0} + s_{k,1} * h_k\right)\mathbf{v} + \mathbf{r}_{k,0} + \mathbf{r}_{k,1} * h_k - I\mathbf{v} \\
&\quad + \sum_{1 \le i \le l, i \ne k} \left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right).
\end{aligned} \tag{19}$$

Given that $s_{k,0} + s_{k,1} * h_k = I$, we have

$$\sum_{1 \le i \le l} \left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v} = \sum_{1 \le i \le l} \left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right). \tag{20}$$

Hence,

$$\mathbf{v} = H\left(\sum_{1 \le i \le l} \left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v}, L, m, I\right). \tag{21}$$

By using the rejection sampling algorithm described in Definition 8, the distribution of $(\mathbf{z}_{i,0}, \mathbf{z}_{i,1})$ is close to $D_s^n(\mathbf{z}_i)$ for $1 \le i \le l$. Thus, by Lemma 3, we have $\mathbf{z_i} = (\mathbf{z}_{i,0}, \mathbf{z}_{i,1})$ satisfies $\|\mathbf{z}_i\| \le s\sqrt{2n}$ with a probability at least $1 - 2^{-\omega(\log n)}$. Therefore, the proposed scheme satisfies verification correctness.

Assume member k calculates the linking tags of messages m_1 and m_2 as I_1 and I_2, respectively. In the proposed scheme, $I_1 = s_{k,0} + s_{k,1} * h_k$ and $I_2 = s_{k,0} + s_{k,1} * h_k$ are generated by the signer's public and private keys, and thus this scheme satisfies linking correctness. This completes the proof. □

5. Security Analysis

Theorem 3 (unforgeability). *Under the random oracle model, when the e-NTRU problem is intractable, the proposed LRS scheme is unforgeable.*

Proof. Setup Phase: To solve the e-NTRU problem, S gets an instance $(h_i)_{1 \le i \le l}$

Query Phase: Adversary A is allowed to access oracles JO, CO, SO, and HO, and S responds as follows:

(i) H: A inputs $((\mathbf{r}_{i,0}, \mathbf{r}_{i,1})_{1 \le i \le l}, L, m, I, k)$, S first checks whether there is the relevant record in the list $list_H$. If so, then the same query result is returned to A. Otherwise, S randomly picks and gives A an integer

$\mathbf{v}$, and adds the tuple $((\mathbf{r}_{i,0}, \mathbf{r}_{i,1})_{1\le i\le l}, L, m, I, \mathbf{v}, k)$ to the list $list_H$.

(ii) JO: Suppose A can only access the oracle JO l' times at most, where $l' \ge l$. S selects a subset X_l with l random indexes. S assigns $(h_i)_{1\le i\le l}$ to these l indexes as their public keys, respectively. Moreover, for these l indexes, S does not know the corresponding private keys. We use $l+1, \cdots, l'$ to denote other indexes. With regard to other $l'-l$ indexes, S obtains the public and private keys according to the algorithm KeyGen(PP). A inputs index j to query, and S outputs the corresponding public key.

(iii) CO: A inputs a public key $pk_i = h_i$, S checks whether i belongs to X_l. If so, then S stops; otherwise, S outputs the corresponding private key.

(iv) SO: A inputs a ring public key set $L = \{h_i\}_{1\le i\le l}$, a public key h_k, where $k \in \{1, \cdots, l\}$, and a message $m \in \{0,1\}^*$. S performs as follows:

(1) If h_k does not correspond to any element in the subset X_l, then S knows its private key and generates the signature according to the signature algorithm Sign(PP, L, m, sk_k). Otherwise, we assume that h_k is obtained by JO.

(2) S checks the list $list_H$ to find the record $((\mathbf{r}_{i,0}, \mathbf{r}_{i,1})_{1\le i\le l}, L, m, I, \mathbf{v}, k)$ corresponding to the index k. Then, S randomly chooses $\mathbf{z}_{i,0}, \mathbf{z}_{i,1} \leftarrow D_s^n$ and sets the output of $H(\sum_{1\le i\le l}(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i) - I\mathbf{v}, L, m, I)$ to $\mathbf{v}$.

(3) S returns a signature $\sigma(m) = (m, (\mathbf{z}_i)_{1\le i\le l}, \mathbf{v}, I)$ with probability $\min(D_s^n(z_k)/MD_{s_k * v,s}^n(z_k), 1)$, where $M = O(1)$.

Forgery Phase: After the simulation, A gives signature $\sigma(m^*) = (m^*, (\mathbf{z}_{i,0}^*, \mathbf{z}_{i,1}^*)_{1\le i\le l}, \mathbf{v}^*, I^*)$ about $\{PP, m^*, L\}^*$ to S satisfying the following conditions:

(i) Verify$(PP, L^*, m^*, \sigma(m^*)) = "1"$

(ii) All of the public keys $pk_i = h_i$ in L^* are query outputs of JO

(iii) A did not query CO about the public keys in L^*

(iv) $\sigma(m^*)$ is not a query output of SO

Analysis. Assuming the signature $\sigma(m^*)$ is a valid signature, the following shows how S can solve the e-NTRU problem using the forged results of A. We will consider the following two situations:

(i) If $\mathbf{v}^*$ appears in the SO, and assume that $\sigma(m) = (m, (z_{i,0}, z_{i,1})_{1\le i\le l}, v^*, I)$ is a query output of SO. Given that the signature is valid, it satisfies

$$\mathbf{v}^* = H\left(\sum_{1\le i\le l}\left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v}^*, L, m, I\right). \tag{22}$$

Given that A successfully forged the signature, there is

$$\mathbf{v}^* = H\left(\sum_{1\le i\le l}\left(\mathbf{z}_{i,0}^* + \mathbf{z}_{i,1}^* * h_i\right) - I^*\mathbf{v}^*, L^*, m^*, I^*\right). \tag{23}$$

When the function H collides, S aborts (Abort I). Otherwise, from (22) and (23), there is

$$L^* = L, m^* = m, I^* = I,$$
$$\sum_{1\le i\le l}\left(\mathbf{z}_{i,0} + \mathbf{z}_{i,1} * h_i\right) - I\mathbf{v}^* = \sum_{1\le i\le l}\left(\mathbf{z}_{i,0}^* + \mathbf{z}_{i,1}^* * h_i\right) - I^*\mathbf{v}^*. \tag{24}$$

$$\sum_{1\le i\le l}\left(\mathbf{z}_{i,0} - \mathbf{z}_{i,0}^*\right) + \left(\mathbf{z}_{i,1} - \mathbf{z}_{i,1}^*\right) * h_i = 0 \bmod q. \tag{25}$$

Therefore, $[(\mathbf{z}_{i,0}^* - \mathbf{z}_{i,0}), (\mathbf{z}_{i,0}^* - \mathbf{z}_{i,1})]_{1\le i\le l}$ is a solution to the e-NTRU problem.

(ii) If $\mathbf{v}^*$ appears in the H query and is stored as $((r_{i,0}, r_{i,1})_{1\le i\le l}, L, m, I, v^*, k)$ in $list_H$, then,

$$\mathbf{v}^* = H\left(\sum_{1\le i\le l}\left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right), L, m, I\right). \tag{26}$$

When the function H collides, S aborts (Abort II). Otherwise, from (23) and (26), there is

$$L^* = L, m^* = m, I^* = I,$$
$$\sum_{1\le i\le l}\left(\mathbf{z}_{i,0}^* + \mathbf{z}_{i,1}^* * h_i\right) - I^*\mathbf{v}^* = \sum_{1\le i\le l}\left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right). \tag{27}$$

S performs the following: when $i \ne k^*$, let $\mathbf{z}_{i,0} = \mathbf{r}_{i,0}$ and $\mathbf{z}_{i,1} = \mathbf{r}_{i,1}$; when $i = k^*$, let $z_{k^*,0} = r_{k^*,0} + v^* I$ and $\mathbf{z}_{k^*,1} = \mathbf{r}_{k^*,1}$. Then, we have

$$\begin{aligned}\mathbf{v}^* &= H\left(\sum_{1\le i\le l}\left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right), L, m, I\right)\\ &= H\left(\sum_{1\le i\le l, i\ne k^*}\left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right) + \mathbf{z}_{k^*,0}\right.\\ &\qquad \left. - \mathbf{v}^* I + \mathbf{z}_{k^*,1} * h_{k^*}, L, m, I\right)\\ &= H\left(\sum_{1\le i\le l}\left(\mathbf{r}_{i,0} + \mathbf{r}_{i,1} * h_i\right) - \mathbf{v}^* I, L, m, I\right).\end{aligned} \tag{28}$$

Given (23), (27), and (28), we have

$$\sum_{1\le i\le l}\left(\mathbf{z}_{i,0} - \mathbf{z}_{i,0}^*\right) + \left(\mathbf{z}_{i,1} - \mathbf{z}_{i,1}^*\right) * h_i = 0 \bmod q. \tag{29}$$

Thus, the solution to the e-NTRU problem is $[(\mathbf{z}_{i,0}^* - \mathbf{z}_{i,0}), (\mathbf{z}_{i,0}^* - \mathbf{z}_{i,1})]_{1\le i\le l}$.

Probability Analysis. The challenger S fails when Aborts I and II occur. The probability of H colliding is $1/2^n$. Assume A can successfully forge the signature with probability ξ,

then the probability of S solving the e-NTRU problem is $\xi - 1/2^n \times 2 = \xi - 1/2^{n-1}$. This completes the proof. □

Theorem 4 (unconditional anonymity). *The proposed scheme satisfies unconditional anonymity.*

Proof. The anonymity proof of the signature is completed by the following game between adversary A and challenger S. If the signature distributions of l different members in the ring are computationally indistinguishable to adversary A, then this scheme satisfies anonymity.

Query Phase: A is allowed to access JO, and S responds as follows:

JO: A inputs an index j to query. S runs the algorithm $\text{KeyGen}(PP)$ to generate the public key $pk_j = h_j$ and returns it to A.

Challenge Phase: A inputs a public key list $L = \{h_i\}_{1 \le i \le l}$, and a message $m^* \in \{0,1\}^*$. S randomly chooses $b \in \{1, \cdots, l\}$, then runs $\text{Sign}(PP, L, m^*, sk_b)$ to generate the signature $\sigma(m^*) = \text{Sign}(PP, L, m^*, sk_b)$ and gives it A, where sk_b is the private key corresponding to index b.

Guess Phase: A gives a value $b\prime \in \{1, \cdots, l\}$ as a guess for b.

Analysis. Suppose A is an adversary with unlimited computing power. Next, we will show the advantage $\text{Adv}_A^{\text{Anon}}$ of A in winning the anonymous game is negligible. We need to prove that the distributions of signatures generated with the private keys of different users are computationally indistinguishable.

First, even A is an adversary with unlimited computing power, from the JO query, or from the challenger signature (which contains a linkability tag), A still cannot deduce the private key, as well as the corresponding index. That is because the randomness of the algorithms TrapGen and SamplePre makes each public key h_b correspond to multiple pairs $(s_{b,0}, s_{b,1})$, and which one is the actual private key of member b cannot be determined. Moreover, given a linking tag $I = s_{b,0} + s_{b,1} * h_b$, to know which member generated the linking tag I, it is no better than random guessing for the adversary. In addition, it should be noticed that the signature $\sigma(m^*)$ is generated by using not only a private key $(s_{b,0}, s_{b,1})$ but also a set of random numbers. Lemma 3 guarantees that the distributions of $(\mathbf{z}_{b,0}, \mathbf{z}_{b,1})$ and $(\mathbf{z}_{i,0}, \mathbf{z}_{i,1})_{i \ne b}$ are indistinguishable, and the distribution of $(\mathbf{z}_{b,0}, \mathbf{z}_{b,1})$ is independent of $(s_{b,0}, s_{b,1})$. That is, in the view of the adversary, the signature $\sigma(m^*)$ is independent of the index b of the actual signer. Hence, we can conclude that even an unbounded adversary cannot guess the index b with a probability greater than $1/l$.

We can infer that when A is a normal adversary, that is, A has limited computing power and time, obviously it ccannot destroy the anonymity of the scheme. This completes the proof. □

Theorem 5 (linkability). *Under the random oracle model, if the proposed scheme is unforgeable, then for any PPT adversary A, the proposed scheme is linkable.*

Proof. We will show that if the proposed scheme satisfies unforgeability, then it will satisfy linkability. The linkability proof of the scheme is completed by the following game interaction between an adversary A and a challenger S.

(i) S generates the system public parameters PP and public and private keys $(pk_i, sk_i)_{1 \le i \le l}$, and then sends PP to A

(ii) A can access JO, CO, SO, and HO, and the process of accessing JO, CO, SO, and HO in the linkability game is the same as that in the unforgeability game

(iii) Suppose A outputs two signatures $\sigma_1(m_1) = (m_1, (z_{i,0}, z_{i,1})_{1 \le i \le l}, v_1, I_1)$ and $\sigma_2(m_2) = (m_2, (\mathbf{z}'_{i,0}, \mathbf{z}'_{i,1})_{1 \le i \le l}, \mathbf{v}_2, I_2)$ under public key set L, which satisfy the following conditions:

(1) All public keys in L are outputs of JO
(2) For $i = 1, 2$, $Verify(PP, L, m_i, \sigma_i(m_i)) = "1"$ such that $\sigma_i(m_i)$ is not an output of SO
(3) A accesses CO once at most

Analysis. Assume A can generate two signatures $\sigma_1(m_1)$ and $\sigma_2(m_2)$ with a nonnegligible probability η while holding only one private key sk_k, and $"1" \leftarrow \text{Verify}(PP, L, m_i, \sigma_i(m_i))$ for $i = 1, 2$. Given that the proposed LRS scheme is unforgeable, these two signatures can be validated by the *Verify* algorithm if and only if A honestly generates signatures $\sigma_1(m_1)$ and $\sigma_2(m_2)$ using his private key sk_k. In other words, we have $I_1 = s_{k,0} + s_{k,1} * h_k$ and $I_2 = s_{k,0} + s_{k,1} * h'_k$. And since there is also only one public key corresponding to this private key, that is, $h_k = h'_k$, we have $I_1 = I_2$. This indicates that the algorithm $\text{Link}(\sigma_1(m_1), \sigma_2(m_2))$ returns "Link" when given two signatures $\sigma_1(m_1)$ and $\sigma_2(m_2)$. Hence, the advantage $\text{Adv}_A^{\text{link}}$ of A is negligible. This completes the proof. □

6. Discussion

6.1. Parameter Selection. The security of the proposed scheme is based on the e-NTRU problem, which is reduced to the NTRU-SIS problem. The NTRU-SIS problem is to find two polynomials $(u, v) \in R_q^2$ that satisfies $u + v * h = 0 \bmod q$ and $\|u\|, \|v\| \le \beta$ in the NTRU lattice, which is in turn reduced to γ-Ideal-SVP problem. Similar to [34, 36], we use the "root Hermite factor γ" which measures the hardness of γ-Ideal-SVP problems to select the parameters.

If we look for a polynomial v in an n-dimensional lattice, which is greater than the n-th root of the determinant, then the associated γ is

$$\frac{\|v\|}{\det(\Lambda)^{1/n}} = \gamma^n. \tag{30}$$

According to [37], if we look for a small-size polynomial v in the NTRU lattice, the associated γ is

$$\frac{\sqrt{n/(2\pi e)} \cdot \det(\Lambda)^{1/n}}{\|v\|} = 0.4\gamma^n. \tag{31}$$

From the results in [36, 38], if the value of γ is approximately 1.007, to find the polynomial is at least 80 bits

Table 2: Parameter settings.

Parameter	Recommended choice	
λ	80	192
γ	1.0069	1.0040
n	256	512

Table 3: Comparison of time costs and difficult assumption.

Scheme	Signature cost	Verification cost	Unconditional anonymity	Difficult assumption
[23]	$nlT_{SD} + kn(2l-1)T_{Mul} + nT_{RS}$	$2knlT_{\mathrm{Mul}}$	No	MSIS, MLWE
[24]	$knlT_{SD} + k^2n(2l+1)T_{\mathrm{Mul}} + knT_{RS}$	$2k^2nlT_{\mathrm{Mul}}$	Yes	R-SIS
[26]	$knlT_{SD} + kn(2l+1)T_{Mul} + knT_{RS}$	$2knlT_{Mul}$	No	MSIS, MLWE
[27]	$vnT_{SD} + 5knT_{Mul}\log l$	$2knT_{Mul}\log l$	No	MSIS, MLWE
[30]	$2n(l+1)T_{SD} + 2n(l+1)T_{Mul}$	$2nlT_{\mathrm{Mul}}$	No	R-SIS,R-ISIS
Ours	$2nlT_{SD} + nlT_{Mul} + 2nT_{RS}$	nlT_{Mul}	Yes	e-NTRU

hard. If the value of γ is less than 1.004, to find the polynomial is at least 192 bits hard.

The methods to attack the proposed scheme are mainly to attack the ring member's public key and the signature.

The public key of the member i is a polynomial $h_i = g_i * f_i^{-1} \bmod q \in R_q$. The attack on h_i is to find two nonzero small-size polynomial $(u_i, v_i) \in R_q^2$ that satisfies $u_i + v_i * h_i = 0 \bmod q$. By Lemma 1 we know, $\|(u_i, v_i)\| \le \sigma\sqrt{2n}$. So using (32) to calculate the value of γ, we have $\gamma = (\sqrt{n}/1.368)^{1/2n}$. When $n = 256$, $\gamma \approx 1.0048$, it is at least 80 bits hard to attack the ring member's public key, and when $n = 512$, $\gamma \approx 1.0027$, it is at least 192 bits hard to attack the ring member's public key.

The attack on the signature of the member i is to find a vector $(\mathbf{z}_{i,0}, \mathbf{z}_{i,1})$ passing the verification algorithm without member i's private key. It can be seen from Lemma 3, $\|(\mathbf{z}_{i,0}, \mathbf{z}_{i,1})\| \le s\sqrt{2n}$. Since $s = 0.585/\pi\sqrt{q \ln(2 + 2/\eta)}$, where $\eta = 2^{-\lambda}/2n$, there is $s = 1.4708\sqrt{q}$ for $n = 256$ and $s = 2.2089\sqrt{q}$ for $n = 512$. So, computing the value of γ by (28), we have

$$\frac{\sigma\sqrt{2n}}{\sqrt{q}} = \gamma^{2n} \Longrightarrow \begin{cases} \gamma = (2.080\sqrt{n})^{1/2n}, & n = 256 \\ \gamma = (3.124\sqrt{n})^{1.2n} & n = 512 \end{cases}. \quad (32)$$

When $n = 256$, $\gamma \approx 1.0069$, to attack the ring member's signature is at least 80 bits hard, and when $n = 512$, $\gamma \approx 1.0041$, to attack the ring member's signature is at least 192 bits hard. The recommended choice of the parameters is shown in Table 2.

6.2. Post-Quantum Security. The proposed scheme is based on the hard assumption over lattice which is generally recognized to provide anti-quantum security. The security proof of the proposed scheme is unlikely to be extended to the Quantum Random Oracle Model [39] (QROM): in the security proof (Theorems 3 and 5), we use the adaptive programming of random oracle (RO) H, and this proof technique is inherent in the structure to some extent.

We note that other schemes built on QROM, such as [40, 41], also use the form of RO programming (even if not adaptive). In addition, although Fiat–Shamir seems unlikely to be proved in QROM, to the best of our knowledge, there are no attacks on the protocols using these proof technologies, which stems from the use of RO.

Table 4: Comparison of communication costs.

Scheme	Public key size (bits)	Private key size (bits)	Signature size (bits)
[23]	$kn\log q$	$n\log q$	$O(n \cdot l)$
[24]	$n\log q$	$kn\log q$	$O(kn \cdot l)$
[26]	$3kn\log q$	$kn\log q$	$O(\mathrm{kn} \cdot l)$
[27]	$kvn\log q$	$vn\log q$	$O(n \cdot \log l)$
[30]	$n\log q$	$9n\log q$	$O(n \cdot l)$
Ours	$n\log q$	$2n\log q$	$O(n \cdot l)$

Table 5: Parameter settings for our scheme.

Parameter	n	k	v	q	Security level
Recommended choice	256	5	4	2^{32}	80 bits

7. Performance Analysis

In this section, the proposed LRS scheme is compared with the schemes [23, 24, 26, 27, 30] in terms of efficiency. We mainly compare these schemes in terms of elapsed time and storage space.

Comparison terms in Table 3 include signature generation cost, signature verification cost, unconditional anonymity, and difficult assumption. Comparison terms in Table 4 include public and private key, as well as signature size of each user. In Tables 3 and 4, n is the degree of polynomials, $q = 1 \bmod 2n$ is a large prime number, l represents the cardinality of the ring, and k and v are integers. The time cost for the discrete Gaussian sampling algorithm and the rejection sampling algorithm running once are represented by T_{SD} and T_{RS}, respectively. In general, $T_{SD} > T_{RS}$. The time cost for polynomial-polynomial multiplication is represented by T_{Mul}, and $T_{Mul} > T_{SD}$. The time overhead of hash, matrix-matrix addition, and polynomial-

Table 6: Comparison of time costs (ms) at security level $\lambda = 80$.

Scheme	Signature time								Verification time							
	l=1	$l = 8$	$l = 64$	$l = 128$	$l = 256$	$l = 512$	$l = 1024$	$l = 2048$	$l = 1$	$l = 8$	$l = 64$	$l = 128$	$l = 256$	$l = 512$	$l = 1024$	$l = 2048$
[23]	3.42	33.44	218.09	421.31	817.84	1532.27	2953.14	5666.39	5.73	35.46	200.10	379.92	750.35	1410.44	2699.05	5189.23
[24]	32.87	154.36	1019.57	1906.38	3693.68	7084.92	14018.56	27925.31	24.32	133.12	950.27	1769.47	3440.64	6619.14	13120.31	23855.36
[26]	9.25	48.87	282.71	525.43	1002.42	1890.29	3659.71	7106.84	5.63	36.86	201.19	389.94	753.65	1428.68	2752.51	5295.31
[27]	34.97	101.14	202.98	239.61	281.36	330.24	381.64	447.12	14.02	41.56	83.32	100.15	121.06	150.38	176.86	237.63
[30]	3.78	14.88	82.87	151.91	265.57	514.81	986.62	1898.85	1.23	7.78	49.81	94.37	162.53	316.15	622.34	1172.31
Ours	1.71	10.36	59.56	109.04	199.47	364.63	688.64	1367.06	0.73	4.63	29.13	49.81	94.37	162.53	316.15	622.34

Table 7: Comparison of storage overhead (KB) at security level $\lambda = 80$.

Scheme	[23]	[24]	[26]	[27]	[30]	Ours
Size of public key	5.45	1.09	16.35	31.80	1.09	1.09
Size of private key	1.09	5.45	5.45	6.36	9.81	2.18
Signature size for $l = 1$	6.54	6.54	7.63	33.39	4.36	3.27
Signature size for $l = 8$	14.17	44.69	45.78	36.57	27.25	18.53
Signature size for $l = 64$	75.21	349.89	350.98	41.34	210.37	140.61
Signature size for $l = 128$	144.97	698.69	699.78	42.93	419.65	280.13
Signature size for $l = 256$	284.49	1396.29	1397.38	44.52	838.21	559.17
Signature size for $l = 512$	563.53	2791.49	2792.58	46.11	1675.33	1117.25

polynomial addition is ignored because these operations take less time. We mainly focus on time-consuming operations, such as matrix-matrix multiplication and polynomial-polynomial multiplication.

In terms of signature generation cost, the proposed scheme mainly uses the Gaussian sampling algorithm $2l$ times, the polynomial-polynomial multiplication l times, and the rejection sampling algorithm once, respectively. Hence, the signature generation cost is $2nlT_{SD} + nlT_{Mul} + 2nT_{RS}$. In terms of signature verification cost, since the proposed scheme primarily runs polynomial-polynomial multiplication l times, the signature generation cost is about nlT_{Mul}. From Table 3, due to $T_{Mul} > T_{SD} > T_{RS}$, compared with the four schemes of [23, 24, 26, 30], the proposed scheme has higher signature generation and verification efficiency. The signature generation and verification time of the proposed scheme is linearly related to the number of ring members l, while that of the scheme of [27] has a logarithmic relationship with l. Therefore, when l is large, the signature generation and verification efficiency of the scheme of [27] is better than that of the proposed scheme. But when l is small, the proposed scheme is more efficient by the settings of relevant parameters. In addition, only Alberto Torres et al.'s scheme [24] and our scheme can achieve unconditional anonymity, while other four schemes only have computational anonymity. And the efficiency of signature generation and verification of our scheme is obviously higher than that of Torres et al.'s scheme.

In the proposed scheme, the public key of the member in the ring is a small polynomial $h_i \in R_q$ generated by the trapdoor generation algorithm TrapGen, and the private key corresponds to two small polynomials in R_q. Therefore, the public and private key lengths of the proposed scheme are $n \log q$ and $2n \log q$, respectively. As shown in Table 4, the public and private key lengths of [23, 24, 26, 27, 30] are $(kn \log q, n \log q)$, $(n \log q, kn \log q)$, $(3kn \log q, kn \log q)$, $(kvn \log q, vn \log q)$, and $(n \log q, 9n \log q)$, respectively. Hence, in terms of public key size, the public key size of the proposed scheme is similar to that of [24, 30] and smaller than that of [23, 26, 27]. With respect to private key size, the private key size of the proposed scheme is larger than that of [23] and they are both smaller than that of [24, 26, 27, 30]. For signature size, the signature size of the scheme [27] has a logarithmic relationship with l, while that of the other five schemes including the proposed scheme has a linear relationship with l. But the growth rate of signature size of [23, 30] and the proposed scheme is obviously slower than that of [24, 26].

8. Implementation and Evaluation

We implemented and evaluated the proposed LRS scheme on a typical laptop configured with a Windows 8.1 system, an Intel(R) Core(TM) i5-4210U CPU@1.70 GHz processor, and a 4.00 GB running memory. We selected parameters to make the proposed scheme secure, and detailed parameter settings are given in Table 5. We ran the signature generation and verification algorithms for 1000 times. And at security level $\lambda = 80$, the average running time of these algorithms of the five schemes under different numbers of ring members is shown in Table 6. It can be seen from Table 6 that the signature generation and verification of [24] take the longest time among the six schemes, while the signature generation and verification time of the proposed scheme is shorter than that of [23, 24, 26, 30]. Compared with [27], when $l \leq 256$, the proposed scheme has higher signature efficiency, but when $l \geq 512$, the signature efficiency of the proposed scheme needs to be improved. On average, compared with the other five schemes, the signature generation and verification time of the proposed scheme is reduced by about 56.61% and 65.18%, respectively. Especially compared with [24], which also has unconditional anonymity as ours, the signature generation and verification time of the proposed scheme is reduced by about 94.52% and 97.18%, respectively.

At security level $\lambda = 80$, the comparison between the proposed scheme and the other five schemes on public/private key size and signature size under different numbers of ring members is shown in Table 7. As for the public key size, the public key size of the proposed scheme is equal to that of [24, 30] and smaller than that of [23, 26, 27]. With respect to private key size, the private key size of the proposed scheme is larger than that of [23] but is significantly smaller than that of [24, 26, 27, 30]. In the case of signature size, the signature size of the proposed scheme is larger than that of [23] but is significantly smaller than that of [24, 26, 30]. When $l \geq 64$, the signature size of the scheme in [27] is shorter than that of the proposed scheme. However, the scheme of [27] only has computational anonymity, while the proposed scheme has unconditional anonymity. Especially compared with [24], the signature size of the proposed scheme is reduced by 58.03% on average.

In addition, in the above experiment, we only completed the proof-of-concept work and did not consider potential

optimization algorithms, such as the polynomial-polynomial multiplication based on FFT.

9. Conclusions

Based on the e-NTRU problem, this study constructed a LRS scheme on NTRU lattice by combining preimage and rejection sampling techniques. Under the random oracle model, the security of our LRS scheme was analyzed in detail. The analysis results show that our scheme satisfies the requirements of correctness, unforgeability, and linkability based on the intractability of the e-NTRU problem in the random oracle model. In particular, our scheme can achieve unconditional anonymity. The efficiency of the proposed scheme was analyzed in detail, and the optional parameter settings of the proposed scheme that meet the security requirements are given. Finally, the proposed scheme and other five latest lattice-based LRS schemes are implemented, which shows that under the same security level, the proposed scheme has higher signature generation and verification efficiency as well as shorter signature size compared with other five LRS schemes.

Data Availability

The data that support of our findings are available at https://github.com/wang-0218/ring-signature.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 61802117), Support Plan of Scientific and Technological Innovation Team in Universities of Henan Province (Grant no. 20IRTSTHN013), the Youth Backbone Teacher Support Program of Henan Polytechnic University (Grant no. 2018XQG-10), and Key Scientific Research Project of Henan Higher Education Institutions (Grant no. 20A413005).

References

[1] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret, Advances in Cryptology - ASIACRYPT 2001," in *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, pp. 552–565, Berlin, Heidelberg, November 2001.

[2] D. Chaum and E. van Heyst, "Group Signatures," *Workshop on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 257–265, 1991.

[3] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures, Advances in Cryptology - CRYPTO 2004," in *Proceedings of the Annual International Cryptology Conference*, pp. 41–55, Santa Barbara, CA, USA, August 2004.

[4] P. P. Tsang and V. K. Wei, "Short Linkable Ring Signatures for E-Voting, E-Cash and Attestation," in *Proceedings of the International Conference on Information Security Practice and Experience*, pp. 48–60, Singapore, April 2005.

[5] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups, Information Security and Privacy," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 325–335, Sydney, Australia, July 2004.

[6] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, "A blockchain privacy protection scheme based on ring signature," *IEEE Access*, vol. 8, pp. 76765–76772, 2020.

[7] F. Tang, J. Pang, K. Cheng, and Q. Gong, "Multiauthority traceable ring signature scheme for smart grid based on blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5566430, 2021.

[8] J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Linkable ring signature with unconditional anonymity," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 1, pp. 157–165, 2013.

[9] M.-J. Qin, Y.-L. Zhao, and Z.-J. Ma, "Practical constant-size ring signature," *Journal of Computer Science and Technology*, vol. 33, no. 3, pp. 533–541, 2018.

[10] X. Zhang and C. Ye, "A Novel Privacy protection of Permissioned Blockchains with Conditionally Anonymous Ring Signature," *Cluster Computing*, vol. 25, pp. 1–15, 2022.

[11] H. Yu and W. Wang, "Certificateless Network Coding Ring Signature Scheme," *Security and Communication Networks*, vol. 2021, Article ID 8029644, 2021.

[12] F. Tang, J. Pang, K. Cheng, and Q. Gong, "Multiauthority Traceable Ring Signature Scheme for Smart Grid Based on Blockchain," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 5566430, 2021.

[13] K. Gu, X. Dong, X. Dong, and L. Wang, "Efficient traceable ring signature scheme without pairings," *Advances in Mathematics of Communications*, vol. 14, no. 2, pp. 207–232, 2020.

[14] T. X. Khuc, T. N. Nguyen, H. Q. Le et al., "Efficient unique ring signature for blockchain privacy protection," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 391–407, Australia, Nov 2021.

[15] S. Bouakkaz and F. Semchedine, "A certificateless ring signature scheme with batch verification for applications in VANET," *Journal of Information Security and Applications*, vol. 55, Article ID 102669, 2020.

[16] H. Lin and M. Wang, "Repudiable Ring Signature: Stronger Security and Logarithmic-Size," *Computer Standards & Interfaces*, vol. 80, 2022.

[17] P. W. Shor, "Polynomial Time Algorithms for Discrete Logarithms and Factoring on a Quantum Computer," in *Proceedings of the International Algorithmic Number Theory Symposium*, London, May 1994.

[18] B. Libert, S. Ling, K. Nguyen, and H. Wang, "Zero-knowledge arguments for lattice-based accumulators: logarithmic-size ring signatures and group signatures without trapdoors, Advances in Cryptology - EUROCRYPT 2016," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 1–31, Zagreb, Oct 2016.

[19] M. F. Esgin, R. Steinfeld, J. K. Liu, and D. Liu, "Lattice-based Zero-Knowledge Proofs: New Techniques for Shorter and Faster Constructions and Applications," in *Proceedings of the Annual International Cryptology Conference*, pp. 115–146, CA, USA, Aug 2019.

[20] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, "SMILE: set membership from ideal lattices with applications to ring signatures and confidential transactions, Advances in

Cryptology - CRYPTO 2021," in *Proceedings of the Annual International Cryptology Conference*, pp. 611–640, Aug 2021.

[21] C. Cao, L. You, and G. Hu, "Fuzzy Identity-Based Ring Signature from Lattices," *Security and Communication Networks*, vol. 2021, 2021.

[22] R. Yang, M. H. Au, J. Lai, Q. Xu, and Z. Yu, "Lattice-based techniques for accountable anonymity: composition of abstract stern's protocols and weak PRF with efficient protocols from LWR," *IACR Cryptol. ePrint Arch.*, p. 781, 2017.

[23] C. Baum, H. Lin, and S. Oechsner, "Towards Practical Lattice-Based One-Time Linkable Ring Signatures," in *Proceedings of the International Conference on Information and Communications Security*, pp. 303–322, Lille, France, October 2018.

[24] W. A. Alberto Torres, R. Steinfeld, A. Sakzad et al., "Post-quantum one-time linkable ring signature and application to ring confidential transactions in blockchain (lattice RingCT v1.0), Information Security and Privacy," in *Proceedings of the Australasian Conference on Information Security and Privacy*, pp. 558–576, Perth, WA, Australia, NOV 2018.

[25] H. Zhang, F. Zhang, H. Tian, and M. H. Au, "Anonymous post-quantum Cryptocash," in *Proceedings of the International Conference on Financial Cryptography and Data Security*, pp. 461–479, Nieuwpoort Curaçao, February 2018.

[26] Z. Liu, K. Nguyen, G. Yang, H. Wang, and D. S. Wong, "A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 726–746, Luxemberg, September 2019.

[27] W. Beullens, S. Katsumata, and F. Pintore, "Calamari and Falafl: Logarithmic (Linkable) Ring Signatures from Isogenies and Lattices," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 464–492, Daejeon, South Korea, December 2020.

[28] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: a ring-based public key cryptosystem," in *Proceedings of the Algorithm Number Theory (ANTS III)*, pp. 267–288, Oregon, USA, June 1998.

[29] Y. Zhang, Y. Hu, J. Xie, and M. Jiang, "Efficient ring signature schemes over NTRU Lattices," *Security and Communication Networks*, vol. 9, no. 18, pp. 5252–5261, 2016.

[30] X. Lu, M. H. Au, and Z. Zhang, "Raptor: a practical lattice-based (linkable) ring signature, Applied Cryptography and Network Security," in *Proceedings of the International Conference on Applied Cryptography and Network Security*, pp. 110–130, Bogota, Colombia, June 2019.

[31] Y. Tang, F. Xia, Q. Ye, M. Wang, R. Mu, and X. Zhang, "Identity-based Linkable Ring Signature on NTRU Lattice," *Security and Communication Networks*, vol. 2021, 2021.

[32] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267–302, 2007.

[33] D. Stehlé and R. Steinfeld, "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 27–47, Tallinn, Estonia, May 2011.

[34] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient identity-based encryption over NTRU lattices," *Lecture Notes in Computer Science*, vol. 8874, pp. 22–41, 2014.

[35] V. Lyubashevsky, "Lattice Signatures without Trapdoors," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 738–755, Cambridge, UK, April 2012.

[36] N. Gama and P. Q. Nguyen, "Predicting lattice reduction," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 31–51, Istanbul, Turkey, April 2008.

[37] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice Signatures and Bimodal Gaussians," in *Proceedings of the Annual Cryptology Conference*, pp. 40–56, Santa Barbara, CA, USA, Augest 2013.

[38] Y. Chen and P. Q. Nguyen, "Bkz 2.0: better lattice security estimates," Advances in Cryptology-ASIACRYPT 2011-," in *Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security*, pp. 1–20, Seoul, South Korea, December 2011.

[39] D. Boneh, Ö. Dagdelen, M. Fischlin, A. Lehmann, C. Schaffner, and M. Zhandry, "Random Oracles in a Quantum W," in *Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security*, pp. 41–69, Seoul, South Korea, 2011.

[40] R. Del Pino, V. Lyubashevsky, N. Gregory, and G. Seiler, "Practical quantum-safe voting from lattices," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1565–1581, New YorkNY-United State, Oct 2017.

[41] D. Leo, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals–dilithium: Digital Signatures from Module Lattices," 2017, http://eprint.iacr.org/2017/633.