Lattice-Based Ring Signature Scheme under the Random Oracle Model

Shangping Wang, Ru Zhao
(Shaanxi Key Laboratory for Network Computing and Security Technology, Xi’an University of Technology, Xi’an, 710054, China)

Abstract: On the basis of the signatures scheme without trapdoors from lattice, which is proposed by Vadim Lyubashevsky in 2012, we present a new ring signature scheme from lattice. The proposed ring signature scheme is an extension of the signatures scheme without trapdoors. We proved that our scheme is strongly unforgeable against adaptive chosen message in the random oracle model, and proved that the security of our scheme can be reduced to the hardness of the small integer solution (SIS) problem by rejection samplings. Compared with the existing lattice-based ring signature schemes, our new scheme is more efficient and with shorter signature length.

Keywords: lattice; ring signature; random oracle model; unforgeable;

Mathematics Subject Classification (2010) 94A60; 81T25

1. Introduction

Recent studies show that the cryptography schemes based on the problems of large integer factoring and discrete logarithm have been unable to resist the quantum attacks, so we must research more efficient and more secure new cryptosystems to resist the quantum attacks. In the 18th century, mathematicians Lagrange, Gauss and Minkowski began to study lattice. Because lattice is of linear structure and the operation based on the lattice is mostly linear, the hard problem on lattice can be used to build new and efficient public key cryptosystems. The lattice-based cryptosystem is assumed can resist quantum attacks, so far the quantum algorithm[1] which can solve the hard problems on the lattice has not emerged in polynomial time, therefore the lattice-based cryptography has became one of the best choice in the era of quantum computing time. Constructing new public key cryptosystems based on the hard problem in lattice has become a new research hotspot of cryptography.

1.1 Ring Signature

A digital signature is a kind of encryption technology, which has message integrity, authentication and non-repudiation. There has been a class of digital signatures which is known as the group digital signature. In the cryptosystem, the entity is a group, and the membership is a complex structure. A group-oriented digital signature contains various different types of digital signatures, such as group signature, ring signature, signature threshold.

2001, Rivest et al. proposed a new signature technique called ring signature in the context of anonymously leaked secret [2]. Ring signature can be regarded as a special group signature [3]. There is no established process group, and for those verifiers, the signer is completely anonymous. Meanwhile, ring signature provides a clever method for anonymous leaking secrets. This unconditional anonymity in long-term protection of information needs some special environment. Because of its unique nature, the ring signature technique can be widely used in anonymous electronic voting, e-government and e-currencies.

2004, Yevgeniy Dodis et al. discussed ad-hoc groups anonymous authentication issues [4], and presented a ring signature scheme based on one-way
accumulators [5]. Gan Zhi et al. used the valve channel method of embedding authentication information to construct a more efficient verifiable ring signature scheme [6]. Amit KAwasthi put forward an efficient identity-based ring signature and proxy ring signature scheme [7]. Javier Herranz et al. put forward a new identity-based ring signature scheme [8]. JiQiang Lv et al. have proposed a ring authenticated encryption scheme which is the combination of encryption and authentication signature [9] and has the verifiability. Tianjie Cao improved the group signature scheme [11]. Tony K.Chan put forward the concept of blind ring signature [12].

2005, KCLee put forward a revocable anonymous ring signature scheme [13]. Patrick P.Tsang designed an association ring signature scheme [14], which can be used for electronic voting and electronic cash systems. Lan Nguyen constructed an accumulator based on bilinear pairing identity-based ring signature scheme [15], and the signature length is fixed. Qianhong Wu et al. constructed an efficient blind ring signature scheme [16]. Qiang Lei et al. constructed an anonymous fingerprinting protocol with the ring signature scheme [17]. Joseph K.Liu et al. who focused on the key leak issues the first time described a forward security ring signature and key encapsulation ring signature scheme [18], and then extended it to the threshold scheme.

In 2006, Yiqun Chen put forward a suitable P2P network identity-based anonymous designated ring signature scheme [19]. Adam Bender analyzed the security definition of the ring signature scheme and fully taken into account the actual ability of an attacker. Eventually, he gave more reliable security definitions and proposed security in the standard model of the two ring signature schemes [20].

In 2008, Gentry, Peikert and Vaikuntanathan raised a hash-and-sign signature scheme based on the hardness of worst-case lattice problem [21]. Lyubashevsky and Micciancio built a signature scheme based on the hardness of worst-case ideal lattice problem [22]. However, the hash-and-sign signature scheme is more inefficient and with larger key length, so it has the higher storage costs.

In 2009, due to the inefficiency of the hash-and-sign signature, Lyubashevshy proposed a new digital signature scheme, which using Fiat-Shamir framework based on the hardness of worst-case ideal lattice problem [23]. The scheme was the only one using the Fiat-Shamir technique at that time. It has made a major contribution to building lattice-based signature scheme using the Fiat-Shamir technique. The first contribution of this work is adapting the ring-SIS based scheme to one based on the hardness of the regular SIS problem. The second contribution is reducing the signature length to $\widetilde{O}(n)$. The third contribution is showing that the parameters of the scheme can be set so that the resulting produces shorter signatures.

2010, Wang and others, who based Cash signature scheme, proposed a lattice-based ring signature scheme against the fixed ring attack in the standard model [24]. A disadvantage of this scheme is that the dimension of the new bonsai tree should be expanded larger than the bonsai tree in the original signature, because the ring members need to join the others’ public keys. That makes the ring signature scheme has larger key size and higher storage cost. But this scheme only uses a small integer with modular multiplication and modular addition, it has high computational efficiency.

In 2012, MiaomiaoTian, who added messaging technology based Boyen's scheme, proposed a ring signature scheme based on lattice [25] and gave formal security proof in the standard model. This scheme is security under adaptive
chosen message attack. Although the scheme has high efficiency, its public size, private size and signature length are large, and it has high storage cost.

In 2012, Vadim Lyubashevsky presented a signature scheme without trapdoor [26] based on lattice. The scheme is provably secure in the random oracle model. Its private key, public key and signature size are much smaller than the hash-and-sign signature scheme. The scheme greatly reduces the storage cost and has great efficiency improvement.

1.2 Our contribution

We present a new lattice-based ring signature scheme based on Vadim Lyubashevsky's lattice signatures without trapdoors. That is, our scheme is extension of the Lyubashevsky's lattice signatures [26], we extend it to be a ring signature scheme. The extension need elaborated, in the key generation algorithm, produce the key pair for the each user by trapdoor function. In the signature algorithm, the signer uses the others’ public keys and his secret key to generate the ring in the name of all members in the ring. In terms of security, the scheme is based on the hardness of the SIS problem on lattice. The security proof depend on the theory of rejection sampling in[26]. In the random oracle model, our scheme can be proved strongly unforgeable against adaptive chosen messages and ensure unconditional anonymity by rejection sampling. Compared with the lattice-based ring signature scheme proposed in literature [24, 25], our scheme has a very major improvement on enhancing the efficiency, such as the running time, the key size and the signature length. Compared with the traditional lattice-based ring signature scheme, our scheme in the signing process just uses the vector matrix multiplication instead of other algorithms similar to extend base algorithm. Therefore, our scheme has a small amount of operations and the running time is short. In terms of the storage space, our scheme has shorter signature length and saves the signature space consumed in the store.

2. DEFINITION

2.1 Lattice

Definition 2.1 (LATTICE[27][ DEFINITION1]). Given \( n \) linearly independent vectors \( \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \in \mathbb{R}^m \), the lattice generated by them is defined as

\[
L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}
\]

We refer to \( \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \) as a basis of the lattice. Equivalently, if we define \( \mathbf{B} \) as the \( m \times n \) matrix whose columns are \( \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n \), the lattice generated by \( \mathbf{B} \) is

\[
L(\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n) = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i \mid x_i \in \mathbb{Z} \right\}
\]

We say that the rank of the lattice is \( n \) and its dimension is \( m \). If \( n=m \), the lattice is called a full-rank lattice.
2.2 SIS problem

Definition 2.2 (l₂ - SISₚₚₚₚₚ [26, DEFINITION 3.1]). Given a random matrix \( A \leftarrow \mathcal{N}_{q \times n} \), find a vector \( v \in \mathbb{Z}^n \setminus \{0\} \) such that \( Av = 0 \) and \( \| v \| \leq \beta \).

Definition 2.3 (SISₚₚₚₚₚₚ distribution [26, DEFINITION 3.2]). Choose a matrix \( A \leftarrow \mathcal{N}_{q \times n} \) and a vector \( s \leftarrow \{-d, \ldots, 0, \ldots, d\}^m \) and output \( (A, s) \).

Definition 2.4 (SISₚₚₚₚₚₚ search [26, DEFINITION 3.3]). Given a pair \( (A, t) \) from the SISₚₚₚₚₚₚ distribution, find \( s \in \{-d, \ldots, 0, \ldots, d\}^m \) such that \( As = t \).

Definition 2.5 (SISₚₚₚₚₚₚ determination [26, DEFINITION 3.4]). Given a pair \( (A, t) \), decide, with non-negligible advantage, whether it came from the SISₚₚₚₚₚₚ distribution or it was generated uniformly at random from \( \mathcal{N}_{q \times n} \times \mathcal{N}_{q \times n} \).

2.3 The Normal Distribution

Definition 2.6 (The continuous Normal distribution [26, DEFINITION 4.1]). The continuous Normal distribution over \( \mathbb{R}^m \) centered at \( v \) with standard deviation \( \sigma \) is defined by the function \( \rho_{v, \sigma}^m(x) = \left( \frac{1}{\sqrt{2\pi\sigma^2}} \right)^m e^{-\frac{|x-v|^2}{2\sigma^2}} \). When \( v=0 \), we will just write it as \( \rho_\sigma^m(x) \).

Definition 2.7 (The discrete Normal distribution [26, DEFINITION 4.2]). The discrete Normal distribution over \( \mathbb{Z}^m \) centered at some \( v \in \mathbb{Z}^m \) with standard deviation \( \sigma \) is defined as \( D_{v, \sigma}^m(x) = \rho_{v, \sigma}^m(x) / \rho_\sigma^m(Z^m) \).

The below lemma collects some basic facts about the discrete Normal distribution over \( \mathbb{Z}^m \).

Lemma 2.1 [28-30]:
1. \( \Pr[|z| > \omega(\sigma \sqrt{\log m}); z \leftarrow \mathcal{D}_\sigma^m] = 2^{-\omega(\log m)} \)
2. For any \( z \in \mathbb{Z}^m \), and \( \sigma \geq \sqrt{\log 3m} \), \( D_{\sigma}^m(z) \leq 2^{-m+1} \)
3. \( \Pr[|z| > 2\sigma \sqrt{m}; z \leftarrow \mathcal{D}_\sigma^m] < 2^{-m} \)

3. Algorithm

3.1 Rejection Sampling

Lemma 3.1 (rejection sampling [26]). Let \( V \) be a subset of \( \mathbb{Z}^m \) in which all
elements have norms less than \( T \), \( \sigma \) be some element in \( R \) such that 
\[ \sigma = \omega(T, \sqrt{\log m}) \], and \( h : V \to R \) be a probability distribution. Then there exists a constant \( M = O(1) \) such that the distribution of the following algorithm \( A \):

1. \( v \leftarrow h \)
2. \( z \leftarrow D^m \)

3. outputs \((z, v)\) with probability with 
\[ \min \left( \frac{D^m(z)}{MD^m(\sigma, z)} \right), 1 \]

is within statistical distance \( \frac{2^{-\omega(\log m)}}{M} \) of the distribution of the following algorithm \( F \):

1. \( v \leftarrow h \)
2. \( z \leftarrow D^m \)
3. outputs \((z, v)\) with probability with \( 1/M \)

Moreover, the probability that \( A \) outputs something is at least \( \frac{1 - 2^{-\omega(\log m)}}{M} \).

3.2 Trapdoor Function

1. **TrapGen** \((1^n) [21] \). Let \( q = poly(n) \) be a prime, \( m \) be an arbitrary positive integer such that \( m > 5n \log q \). Input a security parameter \( n \), and then output the matrix \( A \in Z_q^{n \times m} \) and \( B_A \in Z_q^{m \times m} \). Here \( B_A \) is a good basis of lattice \( \Lambda_q(A) = \{ v \in Z^n : Av = 0 (\text{mod } q) \} \), and \( \| B_A \| \leq O(\sqrt{n \log q}) \).

2. **SamplePre** \((A, B_A, \sigma, y) [21] \). Input \( A \in Z_q^{n \times m} \), \( B_A \in Z_q^{m \times m} \), any \( \sigma \geq \| B_A \| \cdot \omega(\sqrt{\log n}) \) and vector \( y \in Z_q^n \). Then obtain a randomly nonzero vector \( e \in \{ e \in Z^m : \| e \| \leq \sigma \cdot \sqrt{m} \} \) such that \( Ae = y \) (mod \( q \)) with overwhelming probability.

Literature [21] proposed that the domain of the nonzero vector \( e \) can be defined as \( \{ e \in Z^m : \| e \| \leq \sigma \cdot \omega( \sqrt{\log n} ) \} \) in terms of \( l_\infty \) norm. Therefore, the **SamplePre** \((A, B_A, \sigma, y) \) algorithm can be rewritten as follows.

Input \( A \in Z_q^{n \times m} \), \( B_A \in Z_q^{m \times m} \), any \( \sigma \geq \| B_A \| \cdot \omega(\sqrt{\log n}) \) and vector \( y \in Z_q^n \). Then obtain a randomly nonzero vector \( \{ e \in Z^m : \| e \| \leq \sigma \cdot \sqrt{\log n} \} \) by the basis \( B_A \) such that \( Ae = y \) (mod \( q \)) with overwhelming probability.
4. Ring Signature

4.1 Ring Signature

We will describe a ring signature scheme by triple of algorithm (Ring-gen, Ring-sign, Ring-verify).

1. Ring-gen

The Ring-gen algorithm is a probabilistic polynomial time algorithm that takes as input a security parameter \( n \) and output a key pair \( \{ pk_i, sk_i \} \). Different key pairs may come from different public key systems.

2. Ring-sign

This algorithm is a probabilistic polynomial time algorithm that takes as input a set of parameters \( \rho \), a signing key \( sk_j \), a message \( \mu \), and a set of public keys \( L = \{ pk_1, ..., pk_l \} \), outputs a ring signature \( z \). A certain parameter of \( z \) is connected into a ring according the rules. The signer uses the others’ public keys to generate a ring with a fracture, and put his private key into the ring to make it become a complete ring.

3. Ring-verify

The algorithm is a deterministic algorithm that takes as input a set of parameters \( \rho \), a ring signature \( z \) on a message \( \mu \), and outputs True or False for accept or reject respectively.

4.2 Security of the ring signature scheme

In order to be considered secure, a ring signature scheme must satisfy the properties of both anonymity and unforgeability.

1. Anonymity

If the probability of an adversary \( \Gamma \) wins the anonymity game with the polynomial time is negligible, the ring signature scheme has the anonymity property. The anonymity game is defined as follows.

   (1) The challenger \( \Psi \) chooses the system parameter \( n \), and runs the ring-gen algorithm, then outputs a key pair \( \{ pk_i, sk_i \}_{i \in [l]} \). \( \Psi \) sends a set of public key \( \{ pk_i \}_{i \in [l]} \) to adversary \( \Gamma \).

   (2) \( \Gamma \) asks the ring signature to \( \Psi \) for a ring \( L = \{ A_i \}_{i \in [l]} \), a message \( \mu \) and an index \( j \in [l] \) of the signer. \( \Psi \) outputs a ring signature by running the ring-sign algorithm, and sends the result to the adversary \( \Gamma \).
(3) The adversary $\Gamma$ adaptability queries the private key of the user whose index is $j$. Then $\psi$ replies with $sk_j$.

(4) $\Gamma$ queries the ring signature with a message $\mu'$, the index $i_0, i_1 \in [l]$, and a ring $L = \{pk_i\}_{i \in [l]}$. $\psi$ chooses a random bit $b \in \{0,1\}$, input the private key $sk_b$ of the user $i_b$, then finishes running ring-sign algorithm and outputs a ring signature $z$.

(5) $\Gamma$ outputs a bit $b'$ as a guess of the user $i_b$. If $b' = b$, $\Gamma$ wins the anonymity game.

2. unforgeability

There is a polynomial-time reduction from the unforgeability of the ring signature scheme to the hard problem. There is a polynomial-time forger $F$, who can query the random oracle $H$ and the Ring-sign algorithm. If $F$ can forge a valid ring signature with probability $\delta$, then there exist a polynomial-time algorithm who can solve the hard problem with some probability. We can prove the unforgeability property by the hardness of the hard problem. The proof consists of the following four steps:

(1) Setup: The challenger $\psi$ designs Hybrid algorithm to replace the ring signing. The advantage that the forger $F$ distinguishes the actual Ring-sign algorithm from the one in Hybrid is negligible.

(2) Query Phase: The forger $F$, who can query the Ring-sign algorithm, inputs a message $\mu$, a ring $L = \{pk_i\}_{i \in [l]}$ and an index $i_0$ of the signer, then obtains the ring signature. Meanwhile, $F$ can also query the random oracle $H$.

(3) Forgery Phase: $F$ produces a valid ring signature $(z,c)$ with probability $\delta$, we will show that $c$ comes from query phase with large probability.

(4) Reduction: Discuss the source of $c$ in two cases. $c$ comes from the query to the ring signing or the random oracle $H$. In each case, we show that there is a polynomial-time algorithm which can solve the hard problem with some probability respect to $\delta$.

5. Lattice-Based Ring Signature Scheme under the Random Oracle Model

In this section we will give our lattice-based ring signature scheme, the scheme is as follows.

1. Setup.
(1) let \( q \geq 3 \) be a prime number, \( n \) a positive integer and large more than 64. \( m \) is a positive integer such that \( m > 5n \log q \).

\( H : \{0,1\}^t \rightarrow \{v : v \in \{-1,0,1\}^t, \|v\| \leq k\} \) is collision-resistant hash function, where \( k \) and \( K \) are positive integers. A matrix \( T \) is chosen uniformly at random from \( Z_q^{n \times m} \).

(2) In a ring \( R \) of \( l \) members, for all \( i \in [l] \), we run the algorithm \( \text{TrapGen}(1^n) \) to obtain \( A_i \in Z_q^{n \times m} \) and \( B_i \in Z_q^{m \times n} \), where \( B_i \) is a good basis of lattice \( \Lambda_q^\perp(A_i) = \{v \in Z^m : A_i v = 0 (\text{mod } q)\} \) and such that \( \|\tilde{B}_i\| \leq L \) with \( L = O(\sqrt{n \log q}) \).

(3) For all \( i \in [l] \), we run the algorithm \( \text{SamplePre}(A_i,B_i,d(\omega(\log n))^{-1}, t_j) \) \( k \) times with a positive integer \( d \geq \max_{i \in [l]} \{\|B_i\| \omega(\log n)\} \omega(\log n) \). Where vector \( t_j \in Z_q^m (j \in [k]) \) is the \( j \)-th column vector of the matrix \( T \). The algorithm outputs vector \( s_{i,j} \in Z^m (j \in [k]) \) such that \( A_i S_j = T \) and \( S_j \in \{-d, \cdots, 0, \cdots, d\}^{n \times m} \), in which \( S_j = (s_{i,1}, \cdots, s_{i,k}) \in \{-d, \cdots, 0, \cdots, d\}^{n \times m} \). Let \( A_i \in Z_q^{n \times m} \) be the public key of the \( i \)-th member, and \( S_j \in \{-d, \cdots, 0, \cdots, d\}^{n \times m} \) be the private key associated to \( A_i \in Z_q^{n \times m} \).

2. Sign.

Take as input a message \( \mu \), a ring \( R \) of \( l \) members with public keys \( L = \{A_i\}_{i \in [l]} \), and a private key \( S_j \) of the signer \( j \).

(1) For all \( i \in [l] \), sampling random vector \( y_i \xleftarrow{} D_{\sigma}^m \), \( D_{\sigma}^m \) is a discrete Normal distribution over \( Z^m \) with standard deviation \( \sigma \).

(2) set \( c \leftarrow H\left(\sum_{i \in [l]} A_i y_i, L, \mu\right) \).

(3) For all \( i \in [l] \), if \( i \neq j \), set \( z_i = y_i \); if \( i = j \), set \( z_j = S_j c + y_j \) with probability \( \min \left( \frac{D_{\sigma}^m(z_j)}{MD_{\sigma}^m(z_j)} , 1 \right) \), where \( M = O(1) \) is the same as in Lemma 3.1.

(4) Output \( (z_i : i \in [l], c) \) as the ring signature of message \( \mu \) with ring \( R \) with public keys \( L = \{A_i\}_{i \in [l]} \).
Verify.

Take as input a message \( m \), a ring \( R \) of \( l \) members with public keys \( L = \{ A_i \}_{i \in [l]} \), and the ring signature \( (z_i : i \in [l], \epsilon) \) of message \( m \) with ring \( R \). The verifier accepts the signature if and only if both of the following conditions satisfied:

1. \( \| z_i \| \leq 2\sigma \sqrt{m} \) for all \( i \in [l] \).

2. \( \epsilon = H \left( \sum_{i \in [l]} A_i z_i - Tc, L, \mu \right) \).

Otherwise, the verifier rejects.

Firstly we will claim that our scheme is correct. Let \( (z_i : i \in [l], \epsilon) \) be the signature generated by the user \( j \). We will apply the rejection sampling theorem. \( S_j, \epsilon \) in the signature algorithm is equivalent to the random vector \( v \) in Lemma 3.1. \( z_j = S_j, \epsilon + y_j \) is equivalent to \( z \) in Lemma 3.1. According to the conclusions of Lemma 3.1, the distribution of \( z_j = S_j, \epsilon + y_j \) is within statistical distance \( \frac{2^{-\omega(\log n)}}{M} \) of the Gaussian distribution \( D_a^m \). That is to say, the distribution of \( z_j = S_j, \epsilon + y_j \) is statistical close the Gaussian distribution \( D_a^m \). Moreover, in the signature, in addition to the index \( j \), \( z_i(i \in [l] \setminus \{ j \}) \) will all directly come from the Gaussian distribution. Therefore, all \( z_i(i \in [l]) \) can be applied to lemma 2.1, \( \text{Pr}[|z| > 2\sigma \sqrt{m}; z \leftarrow D_a^m] < 2^{-m} \). We have a conclusion that \( \| z_i \| \leq 2\sigma \sqrt{m}(i \in [l]) \) holds with an overwhelming probability. The first part of the verification is correct for a valid signature.

With respect to the second test, we have:

\[
\sum_{i \in [l]} A_i z_i - Tc = A_j z_j - Tc + \sum_{i \in [l] \setminus \{ j \}} A_i z_i \\
= A_j, S_j, \epsilon + A_j, y_j - Tc + \sum_{i \in [l] \setminus \{ j \}} A_i, y_i \\
= \sum_{i \in [l]} A_i, y_i
\]

Therefore, from the above argument we can conclude that our ring signature...
scheme is correct.

6. Anonymity

Theorem 6.1 (Anonymity): The probability of an adversary won the anonymity game with the polynomial time is negligible. Therefore, the ring signature scheme is of anonymity.

Proof: Given a challenger $\psi$, and an adversary $\Gamma$, consider the following game:

1. The challenger $\psi$ obtain $A_i \in \mathbb{Z}_q^{m \times n}$, and $B_i \in \mathbb{Z}_q^{m \times n}$ ($i \in [l]$) that is a good basis of lattice $\Lambda_q^\perp(A_i)$, by $l$ times of running TrapGen($l^n$), and matrix $T$ that is chosen uniformly at random from $\mathbb{Z}_q$.

2. $\psi$ answers the signing query of adversary $\Gamma$, with a ring $L = \{A_i\}_{i \in [l]}$, and a message $\mu$. $\psi$ sends the results of the ring-sign to the adversary $\Gamma$.

3. The adversary $\Gamma$ adaptability queries the private key of the index $i \in [l], \psi$ reply with $S_i$.

4. The adversary $\Gamma$ queries the ring signature with a message $\mu'$, the index $i_0, i_1 \in [l]$, and the public key $L = \{A_i\}_{i \in [l]}$ of a ring. $\psi$ chooses a random bit $b \in \{0, 1\}$, inputs the private key $S_{i_b}$ of the user $i_b$, then finishes running ring-sign and outputs a ring signature $(z_i : i \in [l], c)$.

5. $\Gamma$ outputs a bit $b'$ as a guess of the random bit $b \in \{0, 1\}$.

If we running the ring-sign algorithm by the private key $S_{i_b}$ of the index $i_b$, we will get $z_{i_b} = S_{i_b}c + y_{i_b}$ with probability $\min \left(\frac{D^w_\sigma(z_{i_b})}{MD^m_{S_{i_b}c, \sigma}(z_{i_b})}, 1\right)$, and output the sign $(z_i : i \in [l], c)$. And if we use another method to obtain $z_{i_b}$ in the ring-sign algorithm, such as that we obtain $z_{i_b}$ that are chosen uniformly at random over $D^w_\sigma$ with probability $1/M$ ($M = O(1)$), and output a ring signature.
\((z_i : i \in [l], e)\). Using the rejection sampling lemma 3.1, the statistical distance of the distribution of the signature from those two algorithms is within \(\frac{2^{-\omega(\log m)}}{M}\).

Let \(X_{i_0}\) be a distribution that represents the distribution of the signature received by the private key \(S_{i_0}\), while \(z\) is obtained uniformly at random over \(D_{m_i}\) with probability \(1/M\). And the remaining \(z_i\) \((i \in [l] \setminus i_0)\) come from \(D_{m_i}\), we use \(Y\) to denote the distribution of the signature \((z_i : i \in [l], e)\). Using the rejection sampling lemma 3.1 for \(i_0\) \([i]\), and use above analysis

\[
\Delta(X_{i_0}, X_i) \leq \Delta(X_{i_0}, Y) + \Delta(X_i, Y) \leq 2 \cdot \frac{2^{-\omega(\log m)}}{M}
\]

Therefore, the signature \(X_{i_0}\) is indistinguishable with the signature \(X_i\) with overwhelming probability. That is to say, the advantage of any adversary making a correct guess of \(b\) is negligible. This implies the ring signature scheme ensures unconditional anonymity.

7. Unforgeability

Before proving the unforgeability, we need to prove the following theorem, there exists a collision of the vector \(s\) with certain probability.

**Theorem 6.2** Given any \(A \in Z_q^{n \times m}\) where \(n \gg 64\) and \(m > 5n \log q\), randomly chosen \(s \leftarrow \{-d, \cdots, 0, \cdots, d\}^m\), then with probability \(1 - 2^{-100}\), there exists another \(s' \leftarrow \{-d, \cdots, 0, \cdots, d\}^m\) such that \(As = As'\).

**Proof:** Similar to the proof of Theorem 5.2 in the literature [26]. Notice that \(A\) can be thought of as a linear transformation whose range has size \(q^n\). This means that there are at most \(q^n\) elements \(s \leftarrow \{-d, \cdots, 0, \cdots, d\}^m\) that do not collide with any other elements in \(-d, \cdots, 0, \cdots, d\)\(^m\). Since the set \(-d, \cdots, 0, \cdots, d\)\(^m\) consists of \((2d + 1)^m\) elements, the probability of randomly selecting a non-colliding element is at most

\[
\frac{q^n}{(2d + 1)^m} \leq \frac{q^n}{(2d + 1)^{5n \log q}} \leq \frac{q^n}{(2d + 1)^{64 + 64 \log q / \log(2d + 1)}} = \frac{1}{(2d + 1)^{64}} < 2^{-100} \quad \square
\]

In the process of proving unforgeability, we will use the following algorithms Hybrid1 and Hybrid2. When the adversary asks to the signature, the challenger
can use the algorithm Hybrid1 or Hybrid2 to replace the real signature algorithm, and reply to adversary’s signature queries. The following theorem can prove that the statistical distance between the algorithm Hybrid1 or Hybrid2 and the real signature algorithm is negligible.

**Theorem 6.3.** Suppose there is a polynomial-time forger \( F \), who makes at most \( s \) queries to the signing oracle and \( h \) queries to the random oracle \( H \), succeeds in forging the ring signature scheme with non-negligible probability \( \delta \), then there is a polynomial-time algorithm who can solve the \( l_2 - \text{SIS}_{q,n,m,l,\beta} \) problem for

\[
\beta = (4\sigma + 2d\kappa)\sqrt{mli} \\
\text{with non-negligible probability } \frac{\delta^2}{2(h + s)}.
\]

Proof: The theorem is proved by theorem 6.4 and theorem 6.5. In theorem 6.4, we will show that our ring signing algorithm can be replaced by Hybrid2, and the statistical distance between the two outputs will be at most
\[ \varepsilon = s(h + s) \cdot 2^{-n+1} + s \cdot \frac{2^{-100}}{M} \]. In theorem 6.5, we will show that if a forger can produce a forgery with non-negligible probability \( \delta \) when the ring signing algorithm is replaced by one in Hybrid2, we can utilize him to recover a vector \( v \) such that \( Av = 0 \) and \( \| v \| \leq (4\sigma + 2\delta)\sqrt{ml} \), with non-negligible probability at least

\[
\left( \frac{1}{2} - 2^{-100} \right) \left( \frac{1}{|D_h|} - \frac{1}{t} \right) \left( \frac{\delta - 2^{-100}}{h} \right) \left( \frac{1}{|D_H|} \right)
\]

If we assume that the output of the hash function \( H \) is 100 bits in the ring signing scheme, the probability is \( \left( \frac{1}{2} - 2^{-100} \right) \left( \frac{\delta - 2^{-100}}{h + s} \right) \left( \frac{1}{2} \right) \).

**Theorem 6.4** Let \( D \) be a distinguisher who can query the random oracle \( H \) with \( h \) times and Hybrid2 with \( s \) times. For all but a \( e^{-\Omega(n)} \) fraction of all possible matrices \( A, i \in [L] \), the advantage that \( D \) distinguishes the actual ring signing algorithm from the one in Hybrid2 is at most \( s(h + s) \cdot 2^{-n+1} + s \cdot \frac{2^{-\omega(\log m)}}{M} \).

Proof: We first show that the Distinguisher \( D \) has advantage of at most \( s(h + s) \cdot 2^{-n+1} \) in distinguishing between the real ring signing algorithm and Hybrid1. The only difference between the two algorithm is that in Hybrid1, instead of the output from the hash function \( H \), vector \( c \) is chosen at uniformly random from \( \{v : v \in [-1,0,1]^k, \|v\| \leq \kappa\} \). And then the procedure sets the answer with \( H \left( \sum_{i \in [L]} A_i z_i - T c, L, \mu \right) = H \left( \sum_{i \in [L]} A_i y_i, L, \mu \right) \) without checking whether the value for \( \sum_{i \in [L]} A_i y_i, L, \mu \) was already set. Since \( D \) calls the random oracle \( H \) \( h \) times and the ring signing algorithm \( s \) times, at most \( s+h \) values of \( \sum_{i \in [L]} A_i y_i, L, \mu \) have ever been set. We now show that each time the Hybrid1 procedure is called, the probability of generating \( l \) vectors \( y, i \in [L] \) such that \( \sum_{i \in [L]} A_i y_i \) is equal to one of the previous queried values is at most of \( 2^{-n+1} \). With probability \( 1 - e^{-\Omega(n)} \), write the matrix \( A, i \in [L] \) as “Hermite Normal Form”,

13
such as $A_i = [\overline{A}_i \| I]$, and write the corresponding vector $y_i$ as $y_i = [y_{i,1} \| y_{i,0}]$. For any $t \in \mathbb{Z}_q^n$,

$$\begin{align*}
\Pr \left[ \sum_{i \in [t]} A_i y_i = t; y_i \leftarrow S^{-}\overline{D}_\alpha \right] \\
= \Pr \left[ \sum_{i \in [t]} y_{i,1} = \left( t - \sum_{i \in [t]} \overline{A}_i y_{i,0} \right); y_i \leftarrow S^{-}\overline{D}_\alpha \right] \\
= \Pr \left[ y_i = [y_{i,1} \cdots y_{i,1}] = \left( t - \sum_{i \in [t]} \overline{A}_i y_{i,0} \right); y_i \leftarrow S^{-}\overline{D}_\alpha \right] \\
= \max_{t \in \mathbb{Z}_q^n} \Pr \left[ y_i = t'; y_i \leftarrow S^{-}\overline{D}_\alpha \right] \\
\leq 2^{-n^{t+1}}
\end{align*}$$

Where the last inequality follows Lemma 2.1. Thus if Hybrid1 is accessed $s$ times, and the probability of getting a collision each time is at most $(h + s) \cdot 2^{-n^{t+1}}$, the probability that a collision occurs after $s$ queries is at most $s(h + s) \cdot 2^{-n^{t+1}}$.

Using rejection sampling lemma 3.1, Hybrid1 plays the role of the algorithm $A$ in lemma 3.1, and Hybrid2 corresponds to $F$, the statistical distance between the output of Hybrid1 and the output of Hybrid2 is within $\frac{2^{\omega(\log m)}}{M}$. Since the ring signing is called at most $s$ times, the statistical distance is at most $s \cdot \frac{2^{\omega(\log m)}}{M}$.

In conclusion, the statistical distance between the real ring signing algorithm and Hybrid2 is within

$$s(h + s) \cdot 2^{-n^{t+1}} + s \cdot \frac{2^{\omega(\log m)}}{M}$$

That is the advantage of distinguishing between the real ring signing algorithm and Hybrid2.

**Theorem 6.5** Suppose there exists a polynomial-time forger $F$, who makes at most $s$ queries to the signing oracle and $h$ queries to the random oracle $H$, succeeds in forging the ring signature with non-negligible probability $\delta$, then there exists an algorithm of the same time-complexity as $F$, given $A = [A_i \| \cdots \| A_i] \leftarrow S^{-}\overline{Z}_q^{\text{conv}}$, the algorithm can find a non-zero $v \in \mathbb{Z}_m^n$ such that $Av = 0$ and $\| v \| \leq (4\sigma + 2d\kappa)\sqrt{m}$, with non-negligible probability at least...
\[
\left(\frac{1}{2} - 2^{-100}\right) \left(\delta - 2^{-100}\right) \left(\frac{\delta - 2^{-100}}{h + s} - 2^{-100}\right)
\]

Proof: Let \( D_H = \{ c : c \in \{-1,0,1\}^k, \| c \| \leq \kappa \} \) denotes the range of the random oracle \( H \). Given a randomly matrix \( T \) over \( \mathbb{Z}_q^{n \times k} \), let \( t = h + s \) be the number of times the random oracle \( H \) is called or programmed during \( F \) 's attack. We note \( r_1, \ldots, r_t \leftarrow^s D_h \) as the responses of the random oracle \( H \).

We now consider a subroutine \( A \), which takes as input \( \{\{A_i\}_{i \in [l]} \mid T, i_0, r_1, \ldots, r_t\} \), where \( i_0 \in [l] \) is an index of the signer. We will initialize the forger \( F \) by giving the parameter \( \left(\{A_i\}_{i \in [l]} \mid T, i_0\right) \). When \( F \) wants to get a signature of the message \( \mu \), \( A \) runs the ring signing algorithm in Hybrid2 \( \left(\mu, L = \{A_i\}_{i \in [l]}, i_0\right) \) to produce the signature. During signing, the random oracle \( H \) will have to be programmed, and the response of \( H \) will be first \( r_{i}^t \) (\( i \in [t] \)) in the list \( (r_1, \ldots, r_t) \) that hasn’t been used yet. Therefore, \( A \) will have to keep a table of all the queries to \( H \). In case the same query is made twice, it will have to reply with the previously answer \( r_{i}^t \).

The forger \( F \) can also make queries to the random oracle \( H \), in which case the reply will similarly be the first unused \( r_i^t \) in the list \( (r_1, \ldots, r_t) \). Once \( F \) finishes running and outputs a forgery with non-negligible probability \( \delta \), our subroutine \( A \) simply outputs \( F \)'s output.

With probability \( \delta \), \( F \) will output a valid ring signature \( (z_i : i \in [l], c) \) for \( \left(\mu, L = \{A_i\}_{i \in [l]}, i_0\right) \), then we have \( \| z_i \| \leq 2\sigma\sqrt{m} \) and \( c = H \left( \sum_{i \in [l]} A_i z_i - Tc, L, \mu \right) \) for all \( i \in [l] \). Notice that if the random oracle \( H \) was not queried or programmed on some input \( w = \sum_{i \in [l]} A_i z_i - Tc \) during forging, then \( F \) only has a \( 1/|D_H| \) chance to produce vector \( c \) such that \( c = H(w, L, \mu) \). To ensure the validity of the ring signature, with probability \( 1 - 1/|D_H| \), the vector \( c \) must be one of the list \( (r_1, \ldots, r_t) \) that is the responses of the random oracle \( H \). In conclusion, the probability that \( F \) succeeds in a forgery and \( c \) is one of the list \( (r_1, \ldots, r_t) \) is at least

\[
\delta \left(1 - 1/|D_H|\right) = \delta - \delta / |D_H| \geq \delta - 1/|D_H|
\]

Let \( j \) be some index such that \( c = r_j \). There are two possibilities: \( r_j \) was a
response to a random oracle $H$ query made by $F$, or was programmed during signing.

Case 1: $r_j$ was programmed during signing

The signer programmed the random oracle $H\left(\sum_{i \in [l]} A_i z'_i - \text{Te}, L, \mu'\right) = c$ for signing a message $\mu'$. If the forger outputs a valid forgery $(z_i : i \in [l], c)$ for the message $\mu$, we have

$$H\left(\sum_{i \in [l]} A_i z'_i - \text{Te}, L, \mu'\right) = H\left(\sum_{i \in [l]} A_i z_i - \text{Te}, L, \mu\right)$$

If $\sum_{i \in [l]} A_i z'_i - \text{Te} \neq \sum_{i \in [l]} A_i z_i - \text{Te}$ or $\mu' \neq \mu$, it means that $F$ has found a pre-image of $r_j$. Therefore, we have $\sum_{i \in [l]} A_i z'_i - \text{Te} = \sum_{i \in [l]} A_i z_i - \text{Te}$ and $\mu' = \mu$.

$\sum_{i \in [l]} A_i z'_i - \text{Te} = \sum_{i \in [l]} A_i z_i - \text{Te}$, so $\sum_{i \in [l]} A_i (z'_i - z_i) = 0$. By concatenating each $A_i, z_i (i \in [l])$, we have $Av = 0$, where $A = [A_1 \| \cdots \| A_l] \in \mathbb{Z}_q^{n \times m}$, $v = [(z'_i - z_i) \| \cdots \| (z'_i - z_i)]$. According to the conditions in the verification algorithm, we have $\| z'_i \|, \| z_i \| \leq 2\sigma \sqrt{m}$, hence $\| v \| \leq 4\sigma \sqrt{m l}$.

Case 2: $r_j$ was a response to a random oracle $H$

We record the signature $(z_i : i \in [l], r_j)$ of $F$ on the message $\mu$, and generate fresh random elements $(r'_j, \ldots, r'_l) \leftarrow D_H$. We then run the subroutine $A$ again with input $(\{A_i\}_{i \in [l]}, T_0, r_i, r_{i-1}, r'_j, \ldots, r'_l)$. By the General Forking Lemma, we obtain that the probability that $r'_j \neq r_j$ and the forger uses the random oracle response $r'_j$ in its forgery is at least

$$\left(\frac{\delta - 1}{|D_H|} \left(\frac{\delta - 1/|D_H|}{t} - \frac{1}{|D_H|}\right)\right)$$

Thus with the above probability, the forger $F$ outputs a valid ring signature $(z'_i : i \in [l], r'_j)$ of the message $\mu$, and

$$\sum_{i \in [l]} A_i z'_i - \text{Te} = \sum_{i \in [l]} A_i z_i - \text{Te}$$

where $c = r_j$ and $c' = r'_j$. By rearranging, we obtain
$$\sum_{i\in[l]} A_i [z'_i - z_i + S_i c' - S_i c] = 0.$$  

Let $A = [A_i \| \cdots \| A_i] \in Z_q^{m \times l}$.  

Now all we need is to prove $v \neq 0$. For any index $z'_i - z_i + S_i c' - S_i c (i_0 \in [l])$, let $k$ be a position in which $c[k] \neq c'[k]$. By theorem 6.2, we know that there is at least a $1-2^{-100}$ chance that there exists another secret key $S'_{i_0}$ such that all the columns of $S'_{i_0}$ are the same as $S_{i_0}$ except for column $k$, and $AS'_{i_0} = AS_{i_0}$. If $z'_i - z_i + S_i c' - S_i c = 0$, then $z'_i - z_i + S'_i c' - S'_i c \neq 0$. But to forge F, he does not know whether we use the secret key $S'_{i_0}$ or $S_{i_0}$, the probability that we obtain $z'_i - z_i + S_i c' - S_i c \neq 0$ is at least 1/2, and so we will find a non-zero vector $v$ with probability at least

$$\left( \frac{1}{2} - 2^{-100} \right) \left( 1 - \frac{1}{|D_H|} \right) \left( \frac{1}{|D_H|} \right) - \frac{1}{|D_H|}$$

### 8. Efficiency Analysis

The proposed scheme required just a few matrix-vector multiplications in signing algorithm, which is different from the others who use the ExtBasis algorithm. Therefore, our new scheme is more simple, more efficient, and with shorter signature length. In terms of the storage space, the signature is composed of $l+1$ vectors. Among these, $l$ vectors’ length is $m$, so the length of the signature is $lm+k$. Compared to the other schemes, we have made great progress.

Here in table 8.1 we have compared the efficiency of our scheme with other schemes based on lattices [24, 25] in time and space. Where $T_{Sam}$ and $T_{Ext}$ represent the time cost by algorithm SamplePre and ExtBasis every step, respectively. $T_{mul}$ represents the time cost by scalar multiplication computation $n$ times.

| scheme      | Sign time       | Verify time     | Signature length |
|-------------|-----------------|-----------------|------------------|
| 2010W [24]  | $m(l+d)T_{Ext} + m(l+d+1)T_{Sam}$ | $m(l+d+1)T_{mul}$ | $(l+d+1)m$        |
| 2012T [25]  | $mT_{Sam} + m(l+1)T_{mul}$  | $m(l+2)T_{mul}$  | $(l+2)m$          |
| Our scheme  | $m(l+1)T_{mul}$  | $m(l+1)T_{mul}$  | $lm+k$            |
9. Conclusion

We present a high efficient lattice-based ring signature scheme, and prove its security of unforgeability in the random oracle model. Our scheme has made a great progress in time efficiency. The length of the signature is also relative improved comparing with others. However, both the length of the public key and private key are longer than the scheme which was presented by Carlos Aguilar-Melchor in 2013. So the storage cost of the public key and private key is relatively high. Therefore, our work in the future is to transform our scheme to polynomial rings in order to improve the length of the public key and private key.

Acknowledgements

This work is supported by the National Natural Science Foundation of China under grants 61173192, Research Foundation of Education Department of Shaanxi Province of China under grants 12JK0740. Thanks also go to the anonymous reviewers for their useful comments.

References

[1] D. Micciancio, O. Regev. Lattice-based cryptography. Post-quantum Cryptography [J]. In: Springer Berlin Heidelberg, 147-191.
[2] RIVEST R L, SHAMIR A, TA UMAN Y. How to leak a secret[A]. Proc ASIACRYPT’01[C]. Springer-Verlag, 2001. 552-565.
[3] CHAUM D, HEYST V E. Group signatures[A]. Proc CRYPTO’91[C]. Springer-Verlag, 1991. 257-265.
[4] DODIS Y, KIAYIAS A, NICOLOSI A, et al. Anonymous identification in ad hoc groups[A]. Proc EUROCRYPT’04[C]. Springer-Verlag, 2004. 609-626.
[5] BENALOH J, MARE M D. One-way accumulators: a decentralized alternative to digital signat- ures[A]. Advances in Cryptology-EUROCRYPT’93[C]. Springer-Verlag, 1993. 274-285.
[6] GAN Z, CHEN K F. A new verifiable ring signature scheme[J]. Acta Scientiarum Naturalium Universitatis Sunyatsenii, 2004, 43(2): 132-134.
[7] AWASTHI A K, SUNDER L. ID-based ring signature and proxy ring signature schemes from bilinear pairings[EB/OL]. http://eprint.iacr.org/2004/242, 2004.
[8] HERRANZ J, S’AEZ G. New identity-based ring signature schemes[A]. ICICS 2004 [C]. Springer-Verlag, 2004. 27-39.
[9] LV J Q, REN K, CHEN X, et al. Ring authenticated encryption: a new type of authenticated encryption[A]. The 2004 Symposium on Cryptography and Information Security[C]. Sendai, Japan: 2004. 1179-1184.
[10] CAO T, LIN D, XUE R. Improved ring authenticated encryption scheme[A]. Proceedings of Tenth Joint International Computer Conference[C]. 2004. 341-346.
[11] WANG Ji-in, ZHANG Jian-hong, WANG Yu-min. A Group Signature Scheme Based on Ring Signature idea [J]. ACTA ELECTRONICA SINICA, 2004, 32(3): 408-410.
[12] CHAN T K, FUNG K, LIU J K, et al. Blind spontaneous anonymous group signatures for ad hoc groups[A]. ESAS 2004[C]. Springer-Verlag, 2005. 82-94.
[13] LEE K C, WEI H, HWANG T. Convertible ring signature[A]. IEEE Proc Commum 2005 [C]. 2005. 411-414.
[14] TSANG P P, WEI V K. Short linkable ring signatures for Evoting, E-cash and attestation[A]. ISPEC 2005 [C]. Springer-Verlag 2005. 48-60.
[15] NGUYEN L. Accumulator from bilinear pairings and application to ID-based ring signatures and group membership revocation[A]. CT-RSA 2005[C]. San Francisco, CA USA. Springer-Verlag, 2005. 275-292.
[16] WU Q H, ZHANG F G, SUSILO W, et al. An efficient static blind ring signature scheme[A]. ICISC 2005 [C]. Springer-Verlag, 2006. 410-423.
[17] LEI Q, JIANG Z T, WANG Y M. Ring-based anonymous fingerprinting scheme[A]. CIS 2005[C]. Springer-Verlag, 2005. 1080-1085.
[18] LIU J K, WONG D S. Solutions to key exposure problem in ring signature [EB/OL]. http://eprint.iacr.org/2005/477, 2005.
[19] CHEN Y Q, SUSILO W, MU Y. Identity-based anonymous designated ring signatures[A].
[20] BENDER A, KATZ J, MORSELLI R. Ring signatures: stronger definitions, and constructions without random oracles[A]. Proc TCC2006[C]. Springer-Verlag, 2006.60-79.
[21] Craig Gentry, Chris Peikert, Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions[C]. STOC, 2008:31-51.
[22] Vadim Lyubashevsky, Daniele Micciancio. Asymptotically efficient lattice-based digital signatures[C]. TCC, 2008:37-54.
[23] Vadim Lyubashevsky. Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures[C]. ASIACRYPT, 2009:598-616.
[24] Wang Feng-he, Hu Yu-pu, Wang Chun-xiao. A Lattice-based Ring Signature Scheme from Bonsai Trees [J]. Journal of Electronics & Information Technology, 2010, 32(2): 2400-2403.
[25] Tiao Miao Miao, Huang Liu Sheng, Yang We. Efficient Lattice-Based Ring Signature Scheme[J]. Chinese Journal of Computers, 2012, 35(4): 713-717.
[26] Vadim Lyubashevsky. Lattice Signatures Without Trapdoors[C]. Lecture Notes in Computer Science, 2012:738-755.
[27] D. Sieradzki, V. Bronstein. Introduction[R]. Tel Aviv University: Lattices in Computer Science, 2004.
[28] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers[J]. Mathematische Annalen, 1993:296:625-635.
[29] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measures[J]. EUROSIAM J. Comput, 2007, 37(1):267-302.
[30] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices[C], 2006:145-166.
[31] Bener A, Katz J, MorSELLI R. Ring signatures: Stronger definitions, and constructions without random oracles[J]. Journal of Cryptology, 2009, 22(1):114-138.
[32] Jin Wang. Identity-Based Ring Signature from Lattice Basis Delegation[D]. Beijing: Tsinghua University, 2008.
[33] Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma[C]. ACM Conference on Computer and Communications Security, 2006:390-399.
[34] R. Markus. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles[C]. In Proceedings of the 3rd International Conference on Post-Quantum Cryptography, 2010: 234-257.
[35] Carlos Aguilar Melchor, Slim Bettaieb, Xavier Boyen, Laurent Fousse, Philippe Gaborit. Adapting Lyubashevsky’s Signature Schemes to the Ring Signature Setting[C]. AFRICACRYPT, 2013: 1-25.