Hindawi Publishing Corporation
Journal of Applied Mathematics
Volume 2014, Article ID 371924, 12 pages
http://dx.doi.org/10.1155/2014/371924

Research Article

Strongly Unforgeable Ring Signature Scheme from Lattices in the Standard Model

Geontae Noh, Ji Young Chun, and Ik Rae Jeong

CIST (Center for Information Security Technologies), Korea University, Anam-dong, Seongbuk-gu, Seoul 136-713, Republic of Korea

Correspondence should be addressed to Ik Rae Jeong; irjeong@korea.ac.kr

Received 14 November 2013; Accepted 21 April 2014; Published 5 May 2014

Academic Editor: Jongsung Kim

In a ring signature scheme, a user selects an arbitrary ring to be able to sign a message on behalf of the ring without revealing the signer's identity. Whistle-blowers especially find this useful. To date, various ring signature schemes have been proposed, all considered to be secure as existentially unforgeable with respect to insider corruption; that is, an adversary who chooses ring-message pairs for which he requests signatures, corrupts honest users, and obtains their signing keys can not produce forgeries for new ring-message pairs. Lattice-based ring signature schemes offer lower computational overhead and security from quantum attacks. In this paper, we offer a lattice-based scheme. We begin by showing that the existing ring signature schemes are not sufficiently secure, because existential unforgeability still permits a signer to potentially produce a new signature on previously signed messages. Furthermore, we show that existing ring signature schemes from lattices are not even existentially unforgeable with respect to insider corruption. We then improve previous schemes by applying, for the first time, the concept of strong unforgeability with respect to insider corruption to a ring signature scheme in lattices. This offers more security than any previous ring signature scheme: adversaries cannot produce new signatures for any ring-message pair, including previously signed ring-message pairs.

1. Introduction

Ring signatures were first introduced by Rivest et al. in 2001 in order to provide anonymity to signers [1]. The classic case of a signer who wishes to remain anonymous would be a whistle-blower, who wants to identify a problem without exposing himself as the source. Anyone seeking to expose wrongdoing or leak a secret would want to remain anonymous. Prior to the advent of the ring signature, group signatures were the best way to achieve this; however, group signatures have a group manager who can identify the signer and so complete anonymity is not possible. By contrast, a signer can select a ring for the signature, and no one can trace which member of the ring is the actual signer.

In 2004, Dodis et al. proposed a ring signature scheme in the random oracle model using the Fiat-Shamir transformation [2, 3]. In 2006, Bender et al. proposed new definitions of anonymity and existential unforgeability and first proposed ring signature schemes in the standard model [4]. In 2007, Shacham and Waters proposed efficient ring signature schemes in the standard model based on bilinear groups [5]. In addition to these, various ring signature schemes have been studied [6–11].

All of these early ring signatures used nonlattice based approaches. These cryptographic systems were based on integer factorization and discrete logarithmic problems based on average case problems. These nonlattice based approaches did not offer security against quantum computing attacks [12]. These early ring signatures also entailed more computational overhead because they require exponentiation, although they did offer existential unforgeability with respect to insider corruption and anonymity against full key exposure. Lattice-based cryptographic systems held promise in reducing computational overhead since they only require linear operations on matrices [13–18].

In order to try to reduce computational overhead and make ring signatures secure against quantum computing attacks, Brakerski and Kalai introduced the first lattice-based system for ring signatures in 2010, using ring trapdoor functions [19]. The lattice-based approach is based on worst-case problems, which offers the sought for security against quantum computing attacks; however, Brakerski-Kalai's ring

Table 1: Comparison of ring signature schemes.

	EU	SU	ROM/STM
[19]	×	×	STM
[20]	×	×	ROM
[21]	×	×	ROM/STM
[22]	◯	×	ROM
Ours	◯	◯	STM

EU means the ring signature scheme is existentially unforgeable with respect to insider corruption, SU means the ring signature scheme is strongly unforgeable with respect to insider corruption, ROM means the ring signature scheme is secure in the random oracle model, and STM means the ring signature scheme is secure in the standard model.

signature scheme did not satisfy existential unforgeability with respect to insider corruption. In 2010, Cayrel et al. proposed a threshold ring signature scheme over ideal lattices (ideal lattices are described as ideals of certain polynomial rings; that is, ideal lattices are a special case of lattices) in the random oracle model; however, Cayrel et al.'s threshold ring signature scheme did not satisfy existential unforgeability with respect to insider corruption [20]. In 2011, Wang and Sun proposed two ring signature schemes, one in the random oracle model and one in the standard model, using lattice-based delegation techniques [21]. They claimed their ring signature schemes offered the existential unforgeability that had been lacking in Brakerski-Kalia's ring signature scheme, but they in fact did not (see Section 3). In 2013, Aguilar Melchor et al. proposed a new ring signature scheme over ideal lattices; however, Aguilar Melchor et al.'s ring signature scheme is only existentially unforgeable with respect to insider corruption in the random oracle model [22]. Table 1 shows the comparison of ring signature schemes.

In addition to showing that Wang and Sun's ring signature scheme does not offer existential unforgeability, we introduce a novel lattice-based ring signature scheme that reduces the computational overhead inherent in nonlattice based schemes while successfully offering existential unforgeability with respect to insider corruption. Indeed, we are the first to suggest strong unforgeability for ring signatures, which is stronger than existential unforgeability.

Before the work on strong unforgeability [23–25], if a signature scheme is existentially unforgeable, it has been considered to be secure. In other words, an adversary who chooses messages for which she requests signatures should not be able to produce signatures for new messages. However, in an existentially unforgeable signature scheme, the adversary could potentially produce a new signature on one or more of the previously signed messages. By contrast, if a signature scheme is strongly unforgeable, the adversary cannot ever produce a new signature for any message, including previously signed messages. Strongly unforgeable signature schemes can be especially useful in constructing chosen ciphertext secure encryption schemes and group signature schemes.

Similarly, existentially unforgeable ring signature schemes have been considered to be secure. In other words, an adversary who chooses ring-message pairs for which she requests signatures is not able to produce signatures for new ring-message pairs. In this paper, we are the first to design a securer ring signature scheme, implementing the concept of strong unforgeability and ensuring that the adversary cannot ever produce a new signature for any ring-message pair, including previously signed ring-message pairs. That is, suppose an adversary chooses some ring-message pairs, requests their signatures, and obtains a tuple of ring, message, and signature $(\mathsf{R}, \mathsf{m}, \sigma)$ along with other tuples of rings, messages, and signatures. If the adversary cannot ever produce a new signature σ' for (R, m), or any signatures for any of the ring-message pairs, we say that the ring signature scheme is strongly unforgeable.

We accomplish this strong unforgeability using lattices in the standard model. Our ring signature scheme uses new trapdoor algorithms for lattices proposed by Micciancio and Peikert in 2012 [18]. They are much simpler, tighter, faster, and smaller than the existing algorithms. More concretely, their trapdoor algorithms do not run any expensive operation such as matrix inverse computations; their new trapdoor algorithms improved the quality s from $s \approx 20\sqrt{n \lg q}$ to $s \approx 1.6\sqrt{n \lg q}$ for some small $q = \text{poly}(n)$ and a security parameter n; using their new trapdoor algorithms reduces the lattice dimension m from $m > 5n \lg q$ to $m \approx 2n \lg q$. Therefore, our ring signature scheme is also much simpler, tighter, faster, and smaller than the existing lattice-based ring signature schemes. In fact, the lattice dimension of our ring signature scheme is $m \approx 2(1 + l)n \lg q$ for the number of ring users instead of $m > 5(1 + l)n \lg q$. Our ring signature scheme not only maintains anonymity against full key exposure but also offers strong unforgeability with respect to insider corruption in the standard model.

1.1. Our Contribution. Our work makes three significant contributions. First, we show that all of Wang-Sun's ring signature schemes are insecure with respect to existential unforgeability. Second, we suggest the concept of strong unforgeability, which is a stronger notion than existential unforgeability, for ring signatures. None of the existing lattice-based ring signature schemes satisfy the conditions of strong unforgeability. Third, based on our new model, we construct a new ring signature scheme from lattices that is both anonymous against full key exposure and strongly unforgeable with respect to insider corruption in the standard model.

1.2. Our Approach. As with most existing ring signature schemes for lattices, we design our ring signature scheme using trapdoor delegation techniques for lattices, which afford anonymity against full key exposure. In addition, in our ring signature scheme, like most of the existing signature schemes from lattices, the "hash-and-sign" paradigm is used. Wang and Sun also used the "hash-and-sign" paradigm, but they did so in a way that failed to ensure the security of their schemes. Both of Wang-Sun's ring signature schemes only hash the message, so that anyone can add a ring member and add another message, making it possible for anyone to produce a forgery. We address this problem in our ring signature scheme by hashing the message along with the ring and a random number. Because the ring is included in the

hash value, an adversary cannot change the ring. We have drawn on the concept of strong unforgeability in signature schemes from lattices to extend strong unforgeability to a ring signature scheme. One of the features of the existing strongly unforgeable signature schemes is that the signature algorithm samples a signature in a coset of the lattice (not in the original lattice). Our ring signature scheme uses this signature algorithm. This is the defining feature that makes our ring signature scheme strongly unforgeable with respect to insider corruption in the standard model.

1.3. Organization of the Paper. The remainder of our paper is organized as follows. In Section 2, we describe related work and preliminaries. We will describe early ring signature schemes, existing lattice-based schemes, and chameleon hash functions. In Section 3, we analyze Wang-Sun's ring signature schemes and show that they do not provide existential unforgeability as they purport to do. In Section 4, we address our security model for ring signatures, describing anonymity against full key exposure and our new concept of strong unforgeability. In Section 5, we construct our ring signature scheme and demonstrate that it is secure in both of these respects. In Section 6, we will make our concluding comments.

2. Preliminaries

The security parameter in this paper is n. We denote the real numbers and integers by $\mathbb{R}$ and $\mathbb{Z}$, respectively. For a positive integer k, we let $[1,k] = \{1,\ldots,k\}$. We denote vectors by lower-case bold letters (e.g., $\mathbf{v}$) and assume that $\mathbf{v}$ is a column vector. $\|\mathbf{v}\|$ means the Euclidean norm of $\mathbf{v}$. We denote matrices by upper-case bold letters (e.g., $\mathbf{A}$) and represent the n-by-n identity matrix as $\mathbf{I}_n$. We use standard big-O notation, and, if $f(k) = O(g(k)\cdot \log^c k)$ for any fixed integer c, then we denote $f(k) = \widetilde{O}(g(k))$. $q = \mathrm{poly}(k)$ means $q \in \Theta(k^c)$ for some positive integer c. If $|f(k)| < 1/k^c$ for sufficiently large k and any $c > 0$, then a function $f : \mathbb{R} \to \mathbb{R}$ is negligible. We denote any negligible function by $\mathrm{negl}(n)$. An overwhelming probability is greater than or equal to $1 - f(k)$, where $f(k)$ is a negligible function. When $\mathbf{v}$ is randomly chosen from a set R, we use the notation $\mathbf{v} \leftarrow \mathsf{R}$. The statistical distance between two distributions X and Y over a countable domain $\mathscr{D}$ is denoted by $\Delta(X,Y) = 1/2 \cdot \sum_{i\in\mathscr{D}} |X(i) - Y(i)|$.

2.1. Lattices. In this paper, we consider m-dimensional integer lattices. An m-dimensional integer lattice Λ is defined as follows:

$$\Lambda = \left\{ \mathbf{Bz} = \sum_{i=1}^{m} z_i \mathbf{b}_i : \mathbf{z} \in \mathbb{Z}^m \right\} \subseteq \mathbb{Z}^m, \tag{1}$$

where $\mathbf{B} = \{\mathbf{b}_1,\ldots,\mathbf{b}_m\} \subset \mathbb{Z}^m$ is a basis. The dual lattice Λ^* of Λ is defined as follows:

$$\Lambda^* = \left\{ \mathbf{x} \in \mathbb{Z}^m : {}^{\forall}\mathbf{y} \in \Lambda, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z} \right\} \subseteq \mathbb{Z}^m. \tag{2}$$

We use a q-ary lattice, which is one of m-dimensional integer lattices. For a parity-check matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a q-ary lattice $\Lambda^{\perp}(\mathbf{A})$ is defined as follows:

$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{Az} = \mathbf{0} \,(\mathrm{mod}\, q)\} \subseteq \mathbb{Z}^m, \tag{3}$$

where n and q are positive integers and $\mathbf{0} \in \mathbb{Z}_q^n$ is a zero vector. Next, we define a coset of $\Lambda^{\perp}(\mathbf{A})$. For a syndrome $\mathbf{u} \in \mathbb{Z}_q^n$, a coset $\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A})$ of $\Lambda^{\perp}(\mathbf{A})$ is defined as follows:

$$\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{Az} = \mathbf{u} \,(\mathrm{mod}\, q)\} = \Lambda^{\perp}(\mathbf{A}) + \bar{\mathbf{z}}, \tag{4}$$

where $\mathbf{A}\bar{\mathbf{z}} = \mathbf{u} (\mathrm{mod}\, q)$ for $\bar{\mathbf{z}} \in \mathbb{Z}^m$.

The SIS (short integer solution) problem in lattices is defined as follows.

Definition 1. Given a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ for any desired $m = \mathrm{poly}(n)$, the $\mathrm{SIS}_{q,\beta}$ problem is to find a nonzero vector $\mathbf{v} \in \mathbb{Z}^m$ such that $\mathbf{Av} = \mathbf{0} (\mathrm{mod}\, q)$ and $\|\mathbf{v}\| \le \beta$.

The hardness of the SIS problem follows from [13, 26, 27]. For $q \ge \beta\cdot\sqrt{n}\cdot\omega(\sqrt{\log n})$, the SIS problem in the average case is known to be as hard as approximating the SIVP (shortest independent vectors problem) under quantum reductions to within $\widetilde{O}(\beta\cdot\sqrt{n})$ factors in the worst case.

We now review Gaussian distributions over lattices. First, we recall the Gaussian function as follows:

$$\rho_{\mathscr{H},s,\mathbf{c}}(\mathbf{x}) = \exp\left(-\frac{\pi\|\mathbf{x}-\mathbf{c}\|^2}{s^2}\right), \tag{5}$$

where $\mathscr{H}$ is a d-dimensional subspace of $\mathbb{R}^m$, $m \ge 1$, $s > 0$, $\mathbf{x} \in \mathscr{H}$, and the Gaussian function centered at $\mathbf{c} \in \mathscr{H}$. The continuous distribution with density function is defined as follows:

$$\mathscr{D}_{\mathscr{H},s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{\mathscr{H},s,\mathbf{c}}(\mathbf{x})}{s^d}, \quad \text{where } s^d = \int_{\mathbf{x}\in\mathscr{H}} \rho_{s,\mathbf{c}}(\mathbf{x})\, d\mathbf{x}. \tag{6}$$

Then, the discrete distribution with density function over a lattice Λ is defined as follows:

$$\mathscr{D}_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\mathscr{D}_{\mathscr{H},s,\mathbf{c}}(\mathbf{x})}{\mathscr{D}_{\mathscr{H},s,\mathbf{c}}(\Lambda)}, \tag{7}$$

where $\Lambda \subset \mathscr{H}$ spans $\mathscr{H}$ and $\mathbf{x} \in \Lambda$. Next, we define the Gaussian parameter which is a lattice quantity.

Definition 2 (see [27, 28]). For an m-dimensional integer lattice Λ and a real number $\epsilon > 0$, the Gaussian parameter $\eta_\epsilon(\Lambda)$ is the smallest s such that $\rho_{\mathscr{H},1/s}(\Lambda^* \setminus \{\mathbf{0}\}) \le \epsilon$, where $\rho_{\mathscr{H},1/s}(\cdot)$ is the Gaussian function (centered at $\mathbf{0}$) for $1/s$, $\Lambda \subset \mathscr{H}$ spans $\mathscr{H}$, and Λ^* is the dual lattice of Λ.

In this paper, we also use the following fact.

Lemma 3 (see [18, 29]). *For $\epsilon \in (0,1)$, $s \ge \eta_\epsilon(\Lambda)$, and $\mathbf{c} \in \mathrm{span}(\Lambda)$:*

$$\Pr\left[\left\|\mathscr{D}_{\Lambda,s,\mathbf{c}}\right\| \ge s\cdot\sqrt{m}\right] \le 2^{-m}\cdot\frac{1+\epsilon}{1-\epsilon}, \tag{8}$$

where $\Lambda \subset \mathbb{R}^m$ is a lattice.

2.2. Basic Algorithms for Lattices. The trapdoor generation algorithm $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{H})$ proposed by Micciancio and Peikert in 2012 [18] has the following properties.

Lemma 4 (see [18]). *There exists a probabilistic polynomial time algorithm* $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{H})$ *that takes a parity-check matrix* $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n\times\overline{m}}$, *an invertible matrix* $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$, $n \geq 1$, $m = O(n\log q)$, $q \geq 2$, *and outputs a parity-check matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *with its trapdoor* $\mathbf{T}$ *such that*

(i) $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{H})$ *uses some fixed primitive matrix* $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ *whose columns generate all of* $\mathbb{Z}_q^n$;

(ii) $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{H})$ *chooses a matrix* $\mathbf{T} \leftarrow \mathcal{D}^{\overline{m}\times nk}_{\mathbb{Z},\omega(\sqrt{\log n})}$, *where* $m = \overline{m} + nk$ *and* $k = O(\log n)$;

(iii) $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{H})$ *computes* $\mathbf{A} = [\overline{\mathbf{A}} \parallel \mathbf{HG} - \overline{\mathbf{A}}\mathbf{T}] \in \mathbb{Z}_q^{n\times m}$;

(iv) *the statistical distance between the distribution of* $\mathbf{A}$ *and the uniform distribution is negligible;*

(v) $s_1(\mathbf{T}) = s_T \cdot O(\sqrt{\overline{m}} + \sqrt{nk})$ *holds with an overwhelming probability, where* $s_1(\mathbf{T})$ *is the maximal singular value of* $\mathbf{T}$ *and* $s_T > 0$;

(vi) $\mathsf{GenTrap}(\overline{\mathbf{A}})$ *means* $\mathsf{GenTrap}(\overline{\mathbf{A}}, \mathbf{I}_n)$.

The trapdoor Gaussian sampling algorithm $\mathsf{SampleD}(\mathbf{A}, \mathbf{T}, \mathbf{H}, \mathbf{u}, s)$ *proposed by Micciancio and Peikert in 2012 [18] has the following properties.*

Lemma 5 (see [18]). *There exists a probabilistic polynomial time algorithm* $\mathsf{SampleD}(\mathbf{A}, \mathbf{T}, \mathbf{H}, \mathbf{u}, s)$ *that takes a parity-check matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *with its trapdoor* $\mathbf{T}$, *an invertible matrix* $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$, *a syndrome* $\mathbf{u} \in \mathbb{Z}_q^n$, $s = O(\sqrt{n\log q}) \geq s_G \cdot s_1(\mathbf{T})$ *(where* $s_G = 2$ *if* q *is a power of* 2, *or* $s_G = \sqrt{5}$ *otherwise),* $n \geq 1$, $m = O(n\log q)$, $q \geq 2$, *and outputs a vector* $\mathbf{v}$ *such that*

(i) $\mathsf{SampleD}(\mathbf{A}, \mathbf{T}, \mathbf{H}, \mathbf{u}, s)$ *uses some fixed primitive matrix* $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ *whose columns generate all of* $\mathbb{Z}_q^n$;

(ii) *the statistical distance between the distribution of* $\mathbf{v}$ *and the distribution of* $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}),s\cdot\omega(\sqrt{\log n})}$ *is negligiblel;*

(iii) $\mathsf{SampleD}(\mathbf{A}, \mathbf{T}, \mathbf{u}, s)$ *means* $\mathsf{SampleD}(\mathbf{A}, \mathbf{T}, \mathbf{I}_n, \mathbf{u}, s)$.

The trapdoor delegation algorithm $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1], \mathbf{T}, \mathbf{H}', s')$ *proposed by Micciancio and Peikert in 2012 [18] has the following properties.*

Lemma 6 (see [18]). *There exists a probabilistic polynomial time algorithm* $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1], \mathbf{T}, \mathbf{H}', s')$ *that takes a parity-check matrix* $\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1] \in \mathbb{Z}_q^{n\times(m+nk)}$, *a trapdoor* $\mathbf{T}$ *corresponding to* $\mathbf{A}$, *an invertible matrix* $\mathbf{H}' \in \mathbb{Z}_q^{n\times n}$, *and* $s' \geq \eta_\epsilon(\Lambda^{\perp}(\mathbf{A}))$, *where* $n \geq 1$, $m = O(n\log q)$, $q \geq 2$, $k = O(\log n)$, *and outputs a trapdoor* $\mathbf{T}'$ *corresponding to* $\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1]$ *such that*

(i) $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1], \mathbf{T}, \mathbf{H}', s')$ *uses some fixed primitive matrix* $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ *whose columns generate all of* $\mathbb{Z}_q^n$;

(ii) *the statistical distance between the distribution of* $\mathbf{T}'$ *and the Gaussian distribution with* s' *is negligible;*

(iii) $s_1(\mathbf{T}') \leq s' \cdot O(\sqrt{m} + \sqrt{nk})$ *holds with an overwhelming probability;*

(iv) $\mathsf{DelTrap}$ *works even if the columns of* $\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1]$ *are randomly permuted;*

(v) $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1], \mathbf{T}, s')$ *means* $\mathsf{DelTrap}(\mathbf{A}' = [\mathbf{A} \parallel \mathbf{A}_1], \mathbf{T}, \mathbf{I}_n, s')$.

2.3. Properties of $\mathcal{R}^*$. We use a set of invertible elements in a certain ring $\mathcal{R} = \mathbb{Z}_q/f(x)$ introduced by Micciancio and Peikert in 2012 [18].

Lemma 7 (see [18]). *Let* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathbb{Z}[x]$ *be a monic* n*-degree polynomial. Then, one defines* $\mathcal{R}^*$ *as a set of invertible elements in the ring* $\mathcal{R} = \mathbb{Z}_q[x]/f(x)$ *with the following properties:*

(i) *an arbitrary subset-sum in* $\mathcal{R}^*$ *is also an invertible element in* $\mathcal{R}^*$;

(ii) *there exists a ring homomorphism* $h(\cdot) : \mathcal{R}^* \to \mathbb{Z}_q^{n\times n}$ *that maps from* $a \in \mathcal{R}^*$ *to an invertible matrix* $\mathbf{H} = h(a)$;

(iii) *the number of elements in* $\mathcal{R}^*$ *is at most* $(p-1)\cdot n$, *where* p *is the smallest prime dividing* q.

2.4. Chameleon Hash Function. A family of chameleon hash functions $\mathsf{H}(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^m \to \{0,1\}^h$ was proposed by Cash et al. in 2010 [15].

Lemma 8 (see [15]). *If the* $SIS_{q,\beta}$ *problem for* $q \geq \sqrt{|\mathsf{m}| + 4\cdot s^2\cdot m}\cdot\sqrt{n}\cdot\omega(\sqrt{\log n})$ *and* $\beta = \sqrt{|\mathsf{m}| + 4\cdot s^2\cdot m}$ *is hard, the hash function* $\mathsf{H}(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^m \to \{0,1\}^h$ *has the trapdoor property and the collision resistance property, where* $|\mathsf{m}|$ *is the bit length of the message,* h *is the bit length of the hash value,* s *is a Gaussian parameter,* $n \geq 1$, $m = O(n\log q)$, *and* $q \geq 2$. *The properties of* $\mathsf{H}(\cdot,\cdot)$ *are as follows.*

(i) *The trapdoor property. For any* $\mathsf{H}(\mathsf{m}, \mathbf{r})$ *and* m', *we can sample* $\mathbf{r}'$ *with trapdoor information such that* $\mathsf{H}(\mathsf{m}, \mathbf{r}) = \mathsf{H}(\mathsf{m}', \mathbf{r}')$.

(ii) *The collision resistance property. It is hard to find* $(\mathsf{m}, \mathbf{r})$ *and* $(\mathsf{m}', \mathbf{r}')$ *without trapdoor information such that* $\mathsf{H}(\mathsf{m}, \mathbf{r}) = \mathsf{H}(\mathsf{m}', \mathbf{r}')$ *and* $(\mathsf{m}, \mathbf{r}) \neq (\mathsf{m}', \mathbf{r}')$.

2.5. Ring Signatures. A ring signature scheme RS is a triple set of algorithms $\{\mathsf{RS.Gen}, \mathsf{RS.Sign}, \mathsf{RS.Vrfy}\}$.

(i) $\mathsf{RS.Gen}(1^n)$: on input of a security parameter n, this algorithm outputs a signing key sk_i and verification key vk_i pair.

(ii) $\mathsf{RS.Sign}(sk_i, \mathsf{R}, \mathsf{m})$: on input of a signing key sk_i, a ring R, and a message m, this algorithm outputs a ring signature σ, where R is an ordered set of verification keys.

(iii) $\mathsf{RS.Vrfy}(\mathsf{R}, \mathsf{m}, \sigma)$: on input of a ring R, a message m, and a ring signature σ, this algorithm outputs 1 if the ring signature is valid and 0 otherwise.

Correctness. A ring signature scheme RS is correct if, for any valid ring signature σ corresponding to (R, m), the $\mathsf{RS.Vrfy}(\mathsf{R}, \mathsf{m}, \sigma)$ algorithm outputs 1 with an overwhelming probability.

Generally, ring signatures should be required to satisfy conditions of anonymity and unforgeability. Definitions of anonymity against full key exposure and existential unforgeability with respect to insider corruption were proposed by Bender et al. [4].

3. Related Work

In this section, we review the existing ring signature schemes from lattices. In 2010, Brakerski and Kalai proposed the first ring signature scheme from lattices, using ring trapdoor functions [19]. However, the Brakerski-Kalai's ring signature scheme is only existentially unforgeable under chosen subring attacks; that is, the Brakerski-Kalai's ring signature scheme does not guarantee that their scheme is existentially unforgeable with respect to insider corruption, because existential unforgeability under chosen subring attacks is a weaker security notion than the existential unforgeability with respect to insider corruption.

In 2011, Wang and Sun proposed two ring signature schemes in the random oracle model and in the standard model, using lattice-based delegation techniques [21]. They claimed that Wang-Sun's ring signature schemes offered existential unforgeability with respect to insider corruption, but Wang-Sun's ring signature schemes in fact did not. In this section, we discuss the definition of existential unforgeability with respect to insider corruption and show that all of Wang-Sun's ring signature schemes are not existentially unforgeable with respect to insider corruption.

3.1. Existential Unforgeability with respect to Insider Corruption. In 2006, Bender et al. developed the definitions of anonymity and existential unforgeability for ring signatures [4]. Bender et al. developed four kinds of anonymity and three kinds of existential unforgeability, with anonymity against full key exposure and existential unforgeability with respect to insider corruption being the securest of these. The insider corruption means that an adversary can corrupt honest users and obtain their signing keys. Since then, most existing ring signature schemes are based on Bender et al.'s definitions. In 2011, Wang and Sun proposed two ring signature schemes and claimed that these two ring signature schemes were existentially unforgeable with respect to insider corruption, so we now discuss existential unforgeability with respect to insider corruption, before concluding that their ring signature schemes are not existentially unforgeable.

Existential unforgeability with respect to insider corruption for a ring signature scheme $\mathsf{RS} = \{\mathsf{RS.Gen}, \mathsf{RS.Sign}, \mathsf{RS.Vrfy}\}$ is defined by the game $\mathsf{Game}^{\mathsf{eu}}_{\mathsf{RS},\mathcal{F}}(n)$ between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$ as follows.

(i) *Setup.* $\mathcal{C}$ runs $\mathsf{RS.Gen}(1^n)$ t times to obtain $\{(sk_1, vk_1), \ldots, (sk_t, vk_t)\}$. $\mathcal{C}$ sends an ordered set $\mathsf{S} = \{vk_1, \ldots, vk_t\}$ of verification keys to $\mathcal{F}$. $\mathcal{C}$ sets $\mathsf{CU} \leftarrow \emptyset$, where CU is a set of corrupted users.

(ii) *Signing Queries.* $\mathcal{F}$ sends $(e, \mathsf{R}, \mathsf{m})$ such that $vk_e \in \mathsf{R} \cap \mathsf{S}$ to $\mathcal{C}$. We note that R may not be a subset of S. $\mathcal{C}$ runs $\mathsf{RS.Sign}(sk_e, \mathsf{R}, \mathsf{m})$ to obtain σ and returns it to $\mathcal{F}$.

(iii) *Corruption Queries.* $\mathcal{F}$ sends i such that $vk_i \in \mathsf{S}$ to $\mathcal{C}$. $\mathcal{C}$ returns sk_i to $\mathcal{F}$ and adds vk_i to CU.

(iv) *Output.* $\mathcal{F}$ outputs $(\mathsf{R}^*, \mathsf{m}^*, \sigma^*)$. If $\mathsf{RS.Vrfy}(\mathsf{R}^*, \mathsf{m}^*, \sigma^*) = 1$, $\mathcal{F}$ did not send $(\cdot, \mathsf{R}^*, \mathsf{m}^*)$ to $\mathcal{C}$, and $\mathsf{R}^* \subseteq \mathsf{S} \setminus \mathsf{CU}$, then $\mathcal{F}$ wins the game $\mathsf{Game}^{\mathsf{eu}}_{\mathsf{RS},\mathcal{F}}(n)$.

The advantage of $\mathcal{F}$ in the above game is defined as follows:

$$\mathsf{Adv}^{\mathsf{eu}}_{\mathsf{RS},\mathcal{F}}(n) = \Pr\left[\mathcal{F} \text{ wins the game } \mathsf{Game}^{\mathsf{eu}}_{\mathsf{RS},\mathcal{F}}(n)\right]. \quad (9)$$

3.2. Analysis of Wang-Sun's Ring Signature Schemes. Here, we show that Wang-Sun's ring signature schemes are not existentially unforgeable with respect to insider corruption. Wang-Sun's ring signature scheme $\mathsf{WS.RS} = \{\mathsf{WS.Gen}, \mathsf{WS.Sign}, \mathsf{WS.Vrfy}\}$ in the random oracle model consists of the following algorithms.

(i) $\mathsf{WS.Gen}(1^n)$: this algorithm runs the trapdoor generation algorithm $\mathsf{DelTrap}$ to obtain $(\mathbf{A}_i, \mathbf{T}_i)$. The signing key is $sk_i = \mathbf{T}_i \in \mathbb{Z}^{m \times m}$ and the verification key is $vk_i = \mathbf{A}_i \in \mathbb{Z}_q^{n \times m}$.

(ii) $\mathsf{WS.Sign}(sk_i, \mathsf{R}, \mathsf{m})$: on input of $sk_i = \mathbf{T}_i$, $\mathsf{R} = \{vk_1, \ldots, vk_l\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_l\}$, and m, this algorithm computes $\mathbf{u} = \mathsf{H}(\mathsf{m}) \in \mathbb{Z}_q^n$ and constructs $\mathbf{A}_{\mathsf{R}} = [\mathbf{A}_1 \| \cdots \| \mathbf{A}_l] \in \mathbb{Z}_q^{n \times lm}$, where $\mathsf{H}(\cdot)$ is a hash function. The algorithm samples and outputs $\mathbf{v} \in \mathbb{Z}^{lm}$ from $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}_{\mathsf{R}}),s}$ using the Gaussian sampling algorithm $\mathsf{SampleD}$ and the trapdoor delegation algorithm $\mathsf{DelTrap}$ with $sk_i = \mathbf{T}_i$, where s is a Gaussian parameter.

(iii) $\mathsf{WS.Vrfy}(\mathsf{R}, \mathsf{m}, \mathbf{v})$: on input of $\mathsf{R} = \{vk_1, \ldots, vk_l\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_l\}$, m, and $\mathbf{v}$, this algorithm constructs $\mathbf{A}_{\mathsf{R}} = [\mathbf{A}_1 \| \cdots \| \mathbf{A}_l] \in \mathbb{Z}_q^{n \times lm}$. Then, the algorithm outputs 1 if

(i) $\|\mathbf{v}\| \leq s \cdot \sqrt{lm}$;

(ii) $\mathbf{A}_{\mathsf{R}} \cdot \mathbf{v} = \mathsf{H}(\mathsf{m}) (\mathrm{mod}\ q)$.

Otherwise, the algorithm outputs 0.

We now show that we can construct a forger $\mathcal{F}$ mounting an existential forgery attack with a nonnegligible success probability. Let $\mathcal{C}$ be a challenger in the game of existential unforgeability. $\mathcal{F}$ sends $(e, \mathsf{R}, \mathsf{m}^*)$ to $\mathcal{C}$ in the *Signing Queries* phase and receives a ring signature $\mathbf{v}$ corresponding to $(e, \mathsf{R}, \mathsf{m}^*)$. Then, $\mathcal{F}$ makes a forgery $(\mathsf{R}^*, \mathsf{m}^*, \mathbf{v}^*)$ such that R^* is a proper (or strict) superset of R (i.e.; $\mathsf{R} \subsetneq \mathsf{R}^*$).

For example, $\mathcal{F}$ chooses $\mathsf{R} = (vk_1, vk_3)$ in the *Signing Queries* phase. In this case, $\mathbf{A}_{\mathsf{R}} = [\mathbf{A}_1 \parallel \mathbf{A}_3] \in \mathbb{Z}^{n\times 2m}$. $\mathcal{F}$ chooses $\mathsf{R}^* = (vk_1, vk_3, vk_4)$ in the *Output* phase. In this case, $\mathbf{A}_{\mathsf{R}^*} = [\mathbf{A}_1 \| \mathbf{A}_3 \| \mathbf{A}_4] \in \mathbb{Z}^{n\times 3m}$. Then, $\mathcal{F}$ constructs $\mathbf{v}^* = \begin{bmatrix} \mathbf{v} \\ \mathbf{0} \end{bmatrix}$ by inserting zeros into $\mathbf{v}$, where $\mathbf{v} \in \mathbb{Z}^{2m}$ and $\mathbf{0} \in \mathbb{Z}^m$. Note that the following equation holds:

$$\begin{aligned} [\mathbf{A}_1 \| \mathbf{A}_3 \| \mathbf{A}_4] \cdot \mathbf{v}^* &= [\mathbf{A}_1 \| \mathbf{A}_3 \| \mathbf{A}_4] \cdot \begin{bmatrix} \mathbf{v} \\ \mathbf{0} \end{bmatrix} \\ &= [\mathbf{A}_1 \parallel \mathbf{A}_3] \cdot \mathbf{v} \\ &= \mathsf{H}(\mathsf{m}^*) \pmod q. \end{aligned} \tag{10}$$

Clearly, the Euclidean norms of $\mathbf{v}$ and $\mathbf{v}^*$ are the same, and the tuple $(\mathsf{R}^*, \mathsf{m}^*, \mathbf{v}^*)$ satisfies the verification algorithm (i.e.; $\mathsf{WS.Vrfy}(\mathsf{R}^*, \mathsf{m}^*, \mathbf{v}^*) = 1$). Therefore, Wang-Sun's ring signature scheme in the random oracle model is not existentially unforgeable with respect to insider corruption. Wang-Sun's ring signature scheme in the standard model can similarly be broken.

4. Security Model of Ring Signatures

4.1. Anonymity against Full Key Exposure. We first recall the definition of anonymity against full key exposure in [4]. Anonymity against full key exposure for a ring signature scheme $\mathsf{RS} = \{\mathsf{RS.Gen}, \mathsf{RS.Sign}, \mathsf{RS.Vrfy}\}$ is defined by the following game $\mathsf{Game}^{\mathsf{an}}_{\mathsf{RS},\mathcal{A}}(n)$ between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

(i) *Setup*. $\mathcal{C}$ runs $\mathsf{RS.Gen}(1^n)$ t times to obtain $\{(sk_1, vk_1), \ldots, (sk_t, vk_t)\}$. $\mathcal{C}$ sends an ordered set $\mathsf{S} = \{vk_1, \ldots, vk_t\}$ of verification keys to $\mathcal{A}$. $\mathcal{C}$ sets $\mathsf{CU} \leftarrow \emptyset$, where CU is a set of corrupted users.

(ii) *Signing Queries*. $\mathcal{A}$ sends $(e, \mathsf{R}, \mathsf{m})$ such that $vk_e \in \mathsf{R} \cap \mathsf{S}$ to $\mathcal{C}$. We note that R may not be a subset of S. $\mathcal{C}$ runs $\mathsf{RS.Sign}(sk_e, \mathsf{R}, \mathsf{m})$ to obtain σ and returns σ to $\mathcal{A}$.

(iii) *Corruption Queries*. $\mathcal{A}$ sends i such that $vk_i \in \mathsf{S}$ to $\mathcal{C}$. $\mathcal{C}$ returns sk_i to $\mathcal{A}$ and adds vk_i to CU.

(iv) *Challenge*. $\mathcal{A}$ sends $(e_0, e_1, \mathsf{R}, \mathsf{m})$ such that $vk_{e_0} \in \mathsf{R} \cap \mathsf{S}$ and $vk_{e_1} \in \mathsf{R} \cap \mathsf{S}$ to $\mathcal{C}$. We note that R may not be a subset of S. $\mathcal{C}$ randomly chooses a bit b and returns $\sigma \leftarrow \mathsf{RS.Sign}(sk_{e_b}, \mathsf{R}, \mathsf{m})$ to $\mathcal{A}$.

(v) *Output*. $\mathcal{A}$ guesses and outputs b'. If $b = b'$, then $\mathcal{A}$ wins the game $\mathsf{Game}^{\mathsf{an}}_{\mathsf{RS},\mathcal{A}}(n)$. We note that vk_{e_0} or vk_{e_1} may be in CU.

The advantage of $\mathcal{A}$ in the above game is defined as follows:

$$\mathsf{Adv}^{\mathsf{an}}_{\mathsf{RS},\mathcal{A}}(n) = \Pr\left[\mathcal{F} \text{ wins the game } \mathsf{Game}^{\mathsf{an}}_{\mathsf{RS},\mathcal{A}}(n)\right] - \frac{1}{2}. \tag{11}$$

4.2. Strong Unforgeability with respect to Insider Corruption. We propose strong unforgeability with respect to insider corruption for ring signatures. This is a stronger condition than existential unforgeability. The strong unforgeability of ring signatures is based on the existential unforgeability defined in [4].

Strong unforgeability with respect to insider corruption for a ring signature scheme $\mathsf{RS} = \{\mathsf{RS.Gen}, \mathsf{RS.Sign}, \mathsf{RS.Vrfy}\}$ is defined by the following game $\mathsf{Game}^{\mathsf{su}}_{\mathsf{RS},\mathcal{F}}$ between a challenger $\mathcal{C}$ and a forger $\mathcal{F}$.

(i) *Setup*. $\mathcal{C}$ runs $\mathsf{RS.Gen}(1^n)$ t times to obtain $\{(sk_1, vk_1), \ldots, (sk_t, vk_t)\}$. $\mathcal{C}$ sends an ordered set $\mathsf{S} = \{vk_1, \ldots, vk_t\}$ of verification keys to $\mathcal{F}$. $\mathcal{C}$ sets a set of corrupted users $\mathsf{CU} \leftarrow \emptyset$.

(ii) *Signing Queries*. For $1 \le i \le q_s$, $\mathcal{F}$ sends $(e_i, \mathsf{R}_i, \mathsf{m}_i)$ such that $vk_{e_i} \in \mathsf{R}_i \cap \mathsf{S}$ to $\mathcal{C}$. We note that R_i may not be a subset of S. $\mathcal{C}$ runs $\mathsf{RS.Sign}(sk_{e_i}, \mathsf{R}_i, \mathsf{m}_i)$ to obtain σ_i and returns σ_i to $\mathcal{F}$.

(iii) *Corruption Queries*. For $1 \le j \le t$, $\mathcal{F}$ sends j such that $vk_j \in \mathsf{S}$ to $\mathcal{C}$. $\mathcal{C}$ returns sk_j to $\mathcal{F}$ and adds vk_j to CU.

(iv) *Output*. $\mathcal{F}$ outputs $(\mathsf{R}^*, \mathsf{m}^*, \sigma^*)$. If $\mathsf{RS.Vrfy}(\mathsf{R}^*, \mathsf{m}^*, \sigma^*) = 1$, σ^* is not made for $(\mathsf{R}^*, \mathsf{m}^*)$ through signing queries, and $\mathsf{R}^* \subseteq \mathsf{S} \setminus \mathsf{CU}$, then $\mathcal{F}$ wins the game $\mathsf{Game}^{\mathsf{su}}_{\mathsf{RS},\mathcal{F}}(n)$.

The advantage of $\mathcal{F}$ in the above game is defined as follows:

$$\mathsf{Adv}^{\mathsf{su}}_{\mathsf{RS},\mathcal{F}}(n) = \Pr\left[\mathcal{F} \text{ wins the game } \mathsf{Game}^{\mathsf{su}}_{\mathsf{RS},\mathcal{F}}(n)\right]. \tag{12}$$

Note that $\mathcal{F}$ can send $(\cdot, \mathsf{R}^*, \mathsf{m}^*)$ in the *Signing Queries* phase of the game, whereas $\mathcal{F}$ cannot send $(\cdot, \mathsf{R}^*, \mathsf{m}^*)$ in the existential unforgeability game.

5. Our Construction

5.1. Sets and Parameters. In this section, we propose our ring signature scheme $\mathsf{SRS} = \{\mathsf{SRS.Gen}, \mathsf{SRS.Sign}, \mathsf{SRS.Vrfy}\}$ in the standard model. First, we define the following parameters.

(i) n is a security parameter.

(ii) $m = \overline{m} + (l+1) \cdot nk$ is the dimension of the ring signature, where $\overline{m} = O(nk)$, $k = O(\log n)$, and l is the number of ring users.

(iii) $h \le (p-1) \cdot n$ is the bit length of a hash value, where p is the smallest prime dividing q. That is, a hash value space is $\{0,1\}^h$.

(iv) $s = O(nk \cdot \sqrt{hl}) \cdot \omega(\sqrt{\log n})^3$ is a parameter used in the $\mathsf{SampleD}$ algorithm and $s' = O(\sqrt{hnk}) \cdot \omega(\sqrt{\log n})^2$ is a parameter used in the $\mathsf{DelTrap}$ algorithm.

(v) $q = O(h \cdot l \cdot n^{5/2} \cdot k^2) \cdot \omega(\sqrt{\log n})^5$ and $\beta = O(h \cdot l \cdot n^2 \cdot k^2) \cdot \omega(\sqrt{\log n})^4$ are parameters for the SIS problem and SIVP.

(vi) $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$ is a primitive matrix whose columns generate all of $\mathbb{Z}_q^n$.

(vii) $\mathsf{params} = \{\mathbf{G}, \overline{\mathbf{A}}, \mathbf{C}_0, \ldots, \mathbf{C}_h, \mathbf{u}, \mathsf{H}(\cdot,\cdot)\}$ are public parameters, where $\overline{\mathbf{A}} \leftarrow \mathbb{Z}_q^{n\times\overline{m}}$, $\mathbf{C}_0, \ldots, \mathbf{C}_h \leftarrow \mathbb{Z}_q^{n\times nk}$, $\mathbf{u} \leftarrow \mathbb{Z}_q^n$, and $\mathsf{H}(\cdot,\cdot) : \{0,1\}^* \times \{0,1\}^m \to \{0,1\}^h$ is a hash function.

5.2. Our Ring Signature Scheme. Our ring signature scheme $\mathsf{SRS} = \{\mathsf{SRS.Gen}, \mathsf{SRS.Sign}, \mathsf{SRS.Vrfy}\}$ consists of the following algorithms.

(i) $\mathsf{SRS.Gen}(1^n)$: on input of the security parameter n, this algorithm chooses $\mathbf{T}_i \leftarrow \mathcal{D}^{\overline{m}\times nk}_{\mathbb{Z},\omega(\sqrt{\log n})}$ and computes $\mathbf{A}_i = [\mathbf{G} - \overline{\mathbf{A}}\mathbf{T}_i]$. The signing key is $sk_i = \mathbf{T}_i$ and the verification key is $vk_i = \mathbf{A}_i$.

(ii) $\mathsf{SRS.Sign}(sk_i, \mathsf{R}, \mathsf{m})$: on input of $sk_i = \mathbf{T}_i$, $\mathsf{R} = \{vk_1, \ldots, vk_l\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_l\}$, and m, this algorithm computes $\mathsf{H}(\mathsf{R} \parallel \mathsf{m}, \mathbf{r}) = \mu = (\mu_1, \ldots, \mu_h) \in \{0,1\}^h$ and $\mathbf{C}_\mu = \mathbf{C}_0 + \sum_{j=1}^{h} \mu_j \mathbf{C}_j \in \mathbb{Z}_q^{n\times nk}$, where $\mathbf{r} \leftarrow \{0,1\}^m$ and μ_j is the jth element in μ. The algorithm constructs $\mathbf{A}_{\mathsf{R},\mu} = [\overline{\mathbf{A}} \| \mathbf{A}_\mathsf{R} \| \mathbf{C}_\mu] \in \mathbb{Z}_q^{n\times m}$, where $\mathbf{A}_\mathsf{R} = [\mathbf{A}_1 \| \cdots \| \mathbf{A}_l]$ is the ordered concatenation of matrices in R. The algorithm samples $\mathbf{v} \in \mathbb{Z}^m$ from $\mathcal{D}_{\Lambda^\perp_\mathbf{u}(\mathbf{A}_{\mathsf{R},\mu}),s}$ using the $\mathsf{SampleD}$ and $\mathsf{DelTrap}$ algorithms with $sk_i = \mathbf{T}_i$. The algorithm outputs a ring signature $\sigma = (\mathbf{v}, \mathbf{r})$.

(iii) $\mathsf{SRS.Vrfy}(\mathsf{R}, \mathsf{m}, \sigma)$: on input of $\mathsf{R} = \{vk_1, \ldots, vk_l\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_l\}$, m, and $\sigma = (\mathbf{v}, \mathbf{r})$, this algorithm computes $\mathsf{H}(\mathsf{R} \parallel \mathsf{m}, \mathbf{r}) = \mu = (\mu_1, \ldots, \mu_h) \in \{0,1\}^h$ and $\mathbf{C}_\mu = \mathbf{C}_0 + \sum_{j=1}^{h} \mu_j \mathbf{C}_j \in \mathbb{Z}_q^{n\times nk}$, where μ_j is the jth element in μ. The algorithm constructs $\mathbf{A}_{\mathsf{R},\mu} = [\overline{\mathbf{A}} \| \mathbf{A}_\mathsf{R} \| \mathbf{C}_\mu] \in \mathbb{Z}_q^{n\times m}$, where $\mathbf{A}_\mathsf{R} = [\mathbf{A}_1 \| \cdots \| \mathbf{A}_l]$ is the ordered concatenation of matrices in R. Then, the algorithm outputs 1 if

(i) $\mathbf{A}_{\mathsf{R},\mu} \cdot \mathbf{v} = \mathbf{u} (\mathrm{mod}\, q)$;

(ii) $\|\mathbf{v}\| \le s \cdot \sqrt{m}$.

Otherwise, the algorithm outputs 0.

Correctness. We show that our ring signature scheme SRS is correct. The $\mathsf{SRS.Sign}(sk_i, \mathsf{R}, \mathsf{m})$ algorithm can sample $\mathbf{v}$ from a distribution whose statistical distance from $\mathcal{D}_{\Lambda^\perp_\mathbf{u}(\mathbf{A}_{\mathsf{R},\mu}),s}$ is negligible using the $\mathsf{SampleD}$ and $\mathsf{DelTrap}$ algorithms with $\mathbf{T}_i$ such that $\mathbf{A}_{\mathsf{R},\mu} \cdot \mathbf{v} = \mathbf{u} (\mathrm{mod}\, q)$ and $\|\mathbf{v}\| \le s \cdot \sqrt{m}$ with an overwhelming probability [15, 18, 27]. Therefore, our ring signature scheme SRS is correct.

5.3. Anonymity against Full Key Exposure of Our Construction. We now show that our ring signature scheme SRS is anonymous against full key exposure in the standard model.

Theorem 9. $\mathsf{SRS} = \{\mathsf{SRS.Gen}, \mathsf{SRS.Sign}, \mathsf{SRS.Vrfy}\}$ *is anonymous against full key exposure in the standard model.*

Proof of Theorem 9. Recall that $(e_0, e_1, \mathsf{R}, \mathsf{m})$ is sent by $\mathcal{A}$ in the *Challenge* phase of the game of anonymity. A challenge signature $\sigma_b = (\mathbf{v}_b, \mathbf{r}_b) \leftarrow \mathsf{RS.Sign}(sk_{e_b}, \mathsf{R}, \mathsf{m})$ is then returned to $\mathcal{A}$.

The signing algorithm with $sk_{e_i} = \mathbf{T}_i$ samples $\mathbf{v}_i$ from a distribution whose statistical distance from $\mathcal{D}_{\Lambda^\perp_\mathbf{u}(\mathbf{A}_{\mathsf{R},\mu}),s}$ is negligible. Therefore, the statistical distance between the distribution of $\mathbf{v}_0$ and the distribution of $\mathbf{v}_1$ is negligible. We also note that the distributions of $\mathbf{r}_0$ and $\mathbf{r}_1$ are the same. Therefore, the advantage $\mathsf{Adv}^{\mathsf{an}}_{\mathsf{SRS},\mathcal{A}}$ of $\mathcal{A}$ is negligible. □

5.4. Strong Unforgeability with respect to Insider Corruption of Our Construction. We now show that our ring signature scheme SRS is strongly unforgeable with respect to insider corruption in the standard model.

Theorem 10. *If the* $SIS_{q,\beta}$ *problem for* $q \ge \sqrt{|\mathsf{R}| + |\mathsf{m}| + 4 \cdot s^2 \cdot m} \cdot \sqrt{n} \cdot \omega(\sqrt{\log n})$ *and* $\beta = \sqrt{|\mathsf{R}| + |\mathsf{m}| + 4 \cdot s^2 \cdot m}$ *and* $q \ge O(h \cdot l \cdot n^{5/2} \cdot k^2) \cdot \omega(\sqrt{\log n})^5$ *and* $\beta = O(h \cdot l \cdot n^2 \cdot k^2) \cdot \omega(\sqrt{\log n})^4$ *is hard, the ring signature scheme* $\mathsf{SRS} = \{\mathsf{SRS.Gen}, \mathsf{SRS.Sign}, \mathsf{SRS.Vrfy}\}$ *proposed here is strongly unforgeable with respect to insider corruption in the standard model, where* $|\mathsf{R}|$ *is the ring size and* $|\mathsf{m}|$ *is the message bit length.*

Proof of Theorem 10. We show that, if a forger exists $\mathcal{F}$ with a nonnegligible probability, we can construct an algorithm $\mathcal{A}$ solving the $\mathrm{SIS}_{q,\beta}$ problem.

Assume that $\mathcal{F}$ outputs a forgery $(\mathsf{R}^*, \mathsf{m}^*, \sigma^* = (\mathbf{v}^*, \mathbf{r}^*))$ in the game of strong unforgeability. Then, there exist three cases.

(1) $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*) = \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)$ for some $i \in [1, q_s]$ such that $\mathsf{R}^* \ne \mathsf{R}_i$, $\mathsf{m}^* \ne \mathsf{m}_i$, or $\mathbf{r}^* \ne \mathbf{r}_i$.

(2) $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*) = \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)$ for some $i \in [1, q_s]$ such that $\mathsf{R}^* = \mathsf{R}_i$, $\mathsf{m}^* = \mathsf{m}_i$, and $\mathbf{r}^* = \mathbf{r}_i$.

(3) $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*) \ne \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)$ for all $i \in [1, q_s]$.

Note that the number of signing queries is at most q_s, and $(\mathsf{R}_i, \mathsf{m}_i, \mathbf{r}_i)$ are used in the ith signing queries.

For the first case, we can construct $\mathcal{A}$ conducting a collision attack on $\mathsf{H}(\cdot,\cdot)$ using $\mathcal{F}$. $\mathcal{A}$ simulates the game of strong unforgeability with $\mathcal{F}$ as follows.

(i) *Setup.* $\mathcal{A}$ takes a hash function $\mathsf{H}(\cdot,\cdot)$ as input and chooses $\{\mathbf{G}, \overline{\mathbf{A}}, \mathbf{C}_0, \ldots, \mathbf{C}_h, \mathbf{u}\}$ at random. For $1 \le i \le t$, $\mathcal{A}$ chooses $\mathbf{T}_i \leftarrow \mathcal{D}^{\overline{m}\times nk}_{\mathbb{Z},\omega(\sqrt{\log n})}$ and computes $\mathbf{A}_i = [\mathbf{G} - \overline{\mathbf{A}}\mathbf{T}_i]$. $\mathcal{A}$ sends $\{\mathsf{params}, \mathsf{S}\}$ to $\mathcal{F}$, where $\mathsf{params} = \{\mathbf{G}, \overline{\mathbf{A}}, \mathbf{C}_0, \ldots, \mathbf{C}_h, \mathbf{u}, \mathsf{H}(\cdot,\cdot)\}$ and $\mathsf{S} = \{vk_1, \ldots, vk_t\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_t\}$. $\mathcal{A}$ sets $\mathsf{CU} \leftarrow \emptyset$, where CU is a set of corrupted users.

(ii) *Signing Queries.* $\mathcal{F}$ sends $(e, \mathsf{R}, \mathsf{m})$ such that $vk_e \in \mathsf{R} \cap \mathsf{S}$ to $\mathcal{A}$. $\mathcal{A}$ chooses $\mathbf{r} \leftarrow \{0,1\}^m$ and computes $\mathsf{H}(\mathsf{R} \parallel \mathsf{m}, \mathbf{r}) = \mu = (\mu_1, \ldots, \mu_h) \in \{0,1\}^h$. $\mathbf{A}_{\mathsf{R},\mu}$ is represented as $[\overline{\mathbf{A}} \| \mathbf{A}_\mathsf{R} \| \mathbf{C}_\mu]$, where $\mathbf{A}_\mathsf{R}$ is the ordered concatenation of matrices in R, $\mathbf{C}_\mu = \mathbf{C}_0 + \sum_{j=1}^{h} \mu_j \mathbf{C}_j \in \mathbb{Z}_q^{n\times nk}$, and μ_j is the jth element in μ.

The maximal singular value of $sk_e = \mathbf{T}_e$ (where $s_T > 0$) is as follows:

$$\begin{aligned} s_1(\mathbf{T}_e) &= s_T \cdot O\left(\sqrt{\overline{m}} + \sqrt{nk}\right) \\ &= s_T \cdot O\left(\sqrt{nk} + \sqrt{nk}\right) \\ &= s_T \cdot O\left(\sqrt{nk}\right). \end{aligned} \tag{13}$$

$\mathcal{A}$ calculates $\mathbf{T} \leftarrow \mathsf{DelTrap}(\mathbf{A}_{\mathsf{R},\mu}, \mathbf{T}_e, s')$, where $s' = O(\sqrt{hnk}) \cdot \omega(\sqrt{\log n})^2$.

Then, the maximal singular value of $\mathbf{T}$ is as follows:

$$\begin{aligned} s_1(\mathbf{T}) &\le s' \cdot O\left(\sqrt{\overline{m}+nk}+\sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right)\cdot\omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk+nk}+\sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right)\cdot\omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk}+\sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right)\cdot\omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{lnk}\right) \\ &= O\left(nk\cdot\sqrt{hl}\right)\cdot\omega\left(\sqrt{\log n}\right)^2. \end{aligned} \tag{14}$$

$\mathcal{A}$ calculates $\mathbf{v} \leftarrow \mathsf{SampleD}(\mathbf{A}_{\mathsf{R},\mu}, \mathbf{T}, \mathbf{u}, O(nk\cdot\sqrt{hl})\cdot\omega(\sqrt{\log n})^2)$ from a distribution whose statistical distance from $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}_{\mathsf{R},\mu}),s}$ is negligible, where $s = O(nk\cdot\sqrt{hl})\cdot\omega(\sqrt{\log n})^3$. $\mathcal{A}$ returns $\sigma = (\mathbf{v}, \mathbf{r})$ to $\mathcal{F}$.

(iii) *Corruption Queries*. $\mathcal{F}$ sends i such that $vk_i \in \mathsf{S}$ to $\mathcal{A}$. $\mathcal{A}$ returns $sk_i = \mathbf{T}_i$ to $\mathcal{F}$ and adds $vk_i = \mathbf{A}_i$ to CU.

(iv) *Output*. $\mathcal{A}$ outputs $(\mathsf{R}^*, \mathsf{m}^*, \sigma^* = (\mathbf{v}^*, \mathbf{r}^*))$. For any i, $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*) = \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i) \in \{\mathsf{H}(\mathsf{R}_1 \parallel \mathsf{m}_1, \mathbf{r}_1), \ldots, \mathsf{H}(\mathsf{R}_{q_s} \parallel \mathsf{m}_{q_s}, \mathbf{r}_{q_s})\}$, where $\mathsf{R}^* \neq \mathsf{R}_i$, $\mathsf{m}^* \neq \mathsf{m}_i$, or $\mathbf{r}^* \neq \mathbf{r}_i$. $\mathcal{A}$ outputs two pairs $\{(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*), (\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)\}$ as a collision on $\mathsf{H}(\cdot,\cdot)$.

To reduce the average-case SIS problem to the worst-case SIVP in lattices, $q \ge \beta\cdot\sqrt{n}\cdot\omega(\sqrt{\log n})$ should hold. Therefore,

$$\begin{aligned} q &\ge \beta\cdot\sqrt{n}\cdot\omega\left(\sqrt{\log n}\right) \\ &= \sqrt{|\mathsf{R}|+|\mathsf{m}|+4\cdot s^2\cdot m}\cdot\sqrt{n}\cdot\omega\left(\sqrt{\log n}\right). \end{aligned} \tag{15}$$

Naturally,

$$\mathsf{Adv}^{\mathsf{SIS}}_{\mathcal{A}} \ge \mathsf{Adv}^{\mathsf{cr}}_{\mathsf{H}(\cdot,\cdot),\mathcal{A}} \ge \mathsf{Adv}^{\mathsf{su}}_{\mathsf{SRS},\mathcal{F}}. \tag{16}$$

For the second case, we can construct $\mathcal{A}$ attacking the $\mathrm{SIS}_{q,\beta}$ problem using $\mathcal{F}$. Assume that the number of corrupted users is at most l. $\mathcal{A}$ simulates the game of strong unforgeability with $\mathcal{F}$ as follows.

(i) *Setup*. $\mathcal{A}$ chooses a primitive matrix $\mathbf{G} \in \mathbb{Z}_q^{n\times nk}$. $\mathcal{A}$ takes as input $\mathbf{A}' \in \mathbb{Z}_q^{n\times(\overline{m}+lnk+1)}$ as an SIS instance and parses $\mathbf{A}'$ as $[\mathbf{A} \parallel \mathbf{u}'] = [\overline{\mathbf{A}}\|\mathbf{A}_1^*\|\cdots\|\mathbf{A}_l^*\|\mathbf{u}']$, where $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n\times\overline{m}}$, $\mathbf{A}_1^*, \ldots, \mathbf{A}_l^* \in \mathbb{Z}_q^{n\times nk}$, and $\mathbf{u}' \in \mathbb{Z}_q^n$. $\mathcal{A}$ chooses a chameleon hash function $\mathsf{H}(\cdot,\cdot)$ with trapdoor information and distinct hash values $\{\mu_1, \ldots, \mu_{q_s}\}$, where $\mu_i \leftarrow \{0,1\}^h$ for $1 \le i \le q_s$. $\mathcal{A}$ randomly selects $\mu' \in \{\mu_1, \ldots, \mu_{q_s}\}$.

For $0 \le j \le h$, $\mathcal{A}$ computes $\mathbf{H}_j$ as follows:

$$\mathbf{H}_j = \begin{cases} (-1)^{\mu'_j}\cdot h(u_j) & j \in \{1,\ldots,h\} \\ -\sum_{k=1}^{h}\mu'_k\cdot\mathbf{H}_k & j = 0, \end{cases} \tag{17}$$

where μ'_j is the jth element in μ' and $h(\cdot)$ is a ring homomorphism.

For $0 \le j \le h$, $\mathcal{A}$ chooses $\mathbf{R}_j \leftarrow \mathcal{D}^{\overline{m}\times nk}_{\mathbb{Z},\omega(\sqrt{\log n})}$ and computes the following:

$$\mathbf{C}_j = \mathbf{H}_j\mathbf{G} - \overline{\mathbf{A}}\mathbf{R}_j. \tag{18}$$

If $\mu_i = \mu'$, $\mathbf{H}_0 + \sum_{j=1}^{h}\mu_{i,j}\mathbf{H}_j = \mathbf{0} \in \mathbb{Z}^{n\times n}$, where $\mu_{i,j}$ is the jth element in μ_i. Otherwise, $\mathbf{H}_0 + \sum_{j=1}^{h}\mu_{i,j}\mathbf{H}_j \neq \mathbf{0} \in \mathbb{Z}^{n\times n}$ is an invertible matrix.

$\mathcal{A}$ chooses $\mathbf{v} \leftarrow \mathcal{D}_{\mathbb{Z}^{\overline{m}+(l+1)nk},s}$ and computes $\mathbf{u} = [\mathbf{A} \parallel \mathbf{C}_{\mu'}]\cdot\mathbf{v}$, where $\mathbf{C}_{\mu'} = \mathbf{C}_0 + \sum_{j=1}^{h}\mu'_j\mathbf{C}_j$ and μ'_j is the jth element in μ'.

$\mathcal{A}$ randomly chooses $\mathbf{t} = (t_1, \ldots, t_t) \leftarrow \{0,1\}^t$ such that the number of 1s in $\mathbf{t}$ is l. If $t_k = 1$ for $1 \le k \le t$, $\mathcal{A}$ sets $\mathbf{A}_k = \mathbf{A}_i^*$ for $1 \le i \le l$ in turn. Otherwise, $\mathcal{A}$ chooses $\mathbf{T}_k \leftarrow \mathcal{D}^{\overline{m}\times nk}_{\mathbb{Z},\omega(\sqrt{\log n})}$ and computes $\mathbf{A}_k = [\mathbf{G} - \overline{\mathbf{A}}\mathbf{T}_k]$.

$\mathcal{A}$ sends $\{\mathsf{params}, \mathsf{S}\}$ to $\mathcal{F}$, where $\mathsf{params} = \{\mathbf{G}, \overline{\mathbf{A}}, \mathbf{C}_0, \ldots, \mathbf{C}_h, \mathbf{u}, \mathsf{H}(\cdot,\cdot)\}$ and $\mathsf{S} = \{vk_1, \ldots, vk_t\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_t\}$. $\mathcal{A}$ sets $\mathsf{CU} \leftarrow \emptyset$, where CU is a set of corrupted users.

(ii) *Signing Queries*. For $1 \le i \le q_s$, $\mathcal{F}$ sends $(e_i, \mathsf{R}_i, \mathsf{m}_i)$ such that $vk_{e_i} \in \mathsf{R}_i \cap \mathsf{S}$ to $\mathcal{A}$. $\mathcal{A}$ samples $\mathbf{r}_i$ with trapdoor information such that $\mu_i = \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)$.

(1) For $\mu_i = \mu'$: if $\mathbf{A} \neq [\overline{\mathbf{A}} \parallel \mathbf{A}_{\mathsf{R}_i}]$, $\mathcal{A}$ aborts. Otherwise, $\mathcal{A}$ returns $\sigma_i = (\mathbf{v}, \mathbf{r}_i)$ to $\mathcal{F}$. Note that the distributions of $\mathbf{v}$ and $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}\|\mathbf{C}_{\mu'}),s}$ are the same.

(2) For $\mu_i \neq \mu'$: $\mathbf{A}_{\mathsf{R}_i,\mu_i}$ is represented as $[\overline{\mathbf{A}}\|\mathbf{A}_{\mathsf{R}_i}\|\mathbf{H}\mathbf{G} - \overline{\mathbf{A}}\mathbf{R}]$, where $\mathbf{H} = \mathbf{H}_0 + \sum_{j=1}^{h}\mu_{i,j}\mathbf{H}_j \neq \mathbf{0} \in \mathbb{Z}^{n\times n}$ and $\mathbf{R} = \mathbf{R}_0 + \sum_{j=1}^{h}\mu_{i,j}\mathbf{R}_j$.

The maximal singular value of $\mathbf{R}$ is as follows:

$$\begin{aligned} s_1(\mathbf{R}) &= \sqrt{h+1}\cdot O\left(\sqrt{\overline{m}}+\sqrt{nk}\right)\cdot\omega\left(\sqrt{\log n}\right) \\ &= \sqrt{h+1}\cdot O\left(\sqrt{nk}+\sqrt{nk}\right)\cdot\omega\left(\sqrt{\log n}\right) \end{aligned}$$

$$= \sqrt{h+1} \cdot O\left(\sqrt{nk}\right) \cdot \omega\left(\sqrt{\log n}\right)$$
$$= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right). \tag{19}$$

$\mathcal{A}$ calculates $\mathbf{R}' \leftarrow \mathsf{DelTrap}(\mathbf{A}_{\mathsf{R}_i,\mu_i}, \mathbf{R}, s')$, where $s' = O(\sqrt{hnk}) \cdot \omega(\sqrt{\log n})^2$.

Then, the maximal singular value of $\mathbf{R}'$ is as follows:

$$\begin{aligned} s_1\left(\mathbf{R}'\right) &\le s' \cdot O\left(\sqrt{m} + nk + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk + nk} + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk} + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{lnk}\right) \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^2. \end{aligned} \tag{20}$$

$\mathcal{A}$ calculates $\mathbf{v}_i \leftarrow \mathsf{SampleD}(\mathbf{A}_{\mathsf{R}_i,\mu_i}, \mathbf{R}', \mathbf{u}, O(nk \cdot \sqrt{hl}) \cdot \omega(\sqrt{\log n})^2)$ from a distribution whose statistical distance from $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}_{\mathsf{R}_i,\mu_i}),s}$ is negligible, where $s = O(nk \cdot \sqrt{hl}) \cdot \omega(\sqrt{\log n})^3$. $\mathcal{A}$ returns $\sigma_i = (\mathbf{v}_i, \mathbf{r}_i)$ to $\mathcal{F}$.

(iii) *Corruption Queries*. If $\mathcal{F}$ asks for sk_j, where $t_j = 1$, $\mathcal{A}$ aborts. Otherwise, $\mathcal{A}$ returns $sk_j = \mathbf{T}_j$ and adds $vk_j = \mathbf{A}_j$ to CU.

(iv) *Output*. $\mathcal{F}$ outputs $(\mathsf{R}^*, \mathsf{m}^*, \sigma^* = (\mathbf{v}^*, \mathbf{r}^*))$. If $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*) \neq \mu'$, $\mathcal{A}$ aborts. Otherwise, $\mathbf{A}_{\mathsf{R}^*,\mu^*} = [\mathbf{A} \parallel \mathbf{C}_{\mu'}] = [\overline{\mathbf{A}} \| \mathbf{A}_1^* \| \cdots \| \mathbf{A}_l^* \| - \overline{\mathbf{A}}\mathbf{R}^*]$, where $\mathbf{H}^* = \mathbf{H}_0 + \sum_{j=1}^{h} \mu_j^* \mathbf{H}_j = \mathbf{0} \in \mathbb{Z}^{n \times n}$ and $\mathbf{R}^* = \mathbf{R}_0 + \sum_{j=1}^{h} \mu_j^* \mathbf{R}_j$. Therefore, we obtain the following equation:

$$\left[\mathbf{A} \parallel \mathbf{C}_{\mu'}\right] \cdot \mathbf{v} = \left[\mathbf{A} \parallel \mathbf{C}_{\mu'}\right] \cdot \mathbf{v}^* = \mathbf{u} \left(\mathrm{mod}\, q\right). \tag{21}$$

From the above equation, we have that

$$\begin{aligned} &\left[\mathbf{A} \parallel \mathbf{C}_{\mu'}\right] \cdot (\mathbf{v}^* - \mathbf{v}) \\ &= \left[\overline{\mathbf{A}} \| \mathbf{A}_1^* \| \cdots \| \mathbf{A}_l^* \| - \overline{\mathbf{A}}\mathbf{R}^*\right] \cdot (\mathbf{v}^* - \mathbf{v}) \\ &= \mathbf{A} \begin{bmatrix} \mathbf{I}_{\overline{m}} & & -\mathbf{R}^* \\ & \mathbf{I}_{lnk} & \end{bmatrix} \cdot (\mathbf{v}^* - \mathbf{v}) = \mathbf{0} \left(\mathrm{mod}\, q\right). \end{aligned} \tag{22}$$

Let $\mathbf{z} \in \mathbb{Z}^{\overline{m}+lnk}$ be $\begin{bmatrix} \mathbf{I}_{\overline{m}} & & -\mathbf{R}^* \\ & \mathbf{I}_{lnk} & \end{bmatrix} \cdot (\mathbf{v}^* - \mathbf{v})$ and let $\mathbf{z}' \in \mathbb{Z}^{\overline{m}+lnk+1}$ be $\begin{bmatrix} \mathbf{z} \\ 0 \end{bmatrix}$. Then, $\mathbf{A}\mathbf{z} = \mathbf{0} (\mathrm{mod}\, q)$ and

$$\mathbf{A}'\mathbf{z}' = \left[\mathbf{A} \parallel \mathbf{u}'\right] \begin{bmatrix} \mathbf{z} \\ 0 \end{bmatrix} = \mathbf{0} \left(\mathrm{mod}\, q\right). \tag{23}$$

$\mathcal{A}$ outputs $\mathbf{z}'$ as a SIS solution to $\mathbf{A}'$.

The Euclidean norm of $\mathbf{v}^*$ is as follows:

$$\begin{aligned} \left\|\mathbf{v}^*\right\| &\le s \cdot \sqrt{m} \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot \sqrt{\overline{m} + (l+1) \cdot nk} \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot O\left(\sqrt{nk + (l+1) \cdot nk}\right) \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot O\left(\sqrt{lnk}\right) \\ &= O\left(h^{1/2} \cdot l \cdot n^{3/2} \cdot k^{3/2}\right) \cdot \omega\left(\sqrt{\log n}\right)^3. \end{aligned} \tag{24}$$

Because $\|\mathbf{v}\| = \|\mathbf{v}^*\| = O(h^{1/2} \cdot l \cdot n^{3/2} \cdot k^{3/2}) \cdot \omega(\sqrt{\log n})^3$ and $\mathbf{v}^* - \mathbf{v} \neq \mathbf{0}$, $\|\mathbf{z}'\| = \|\mathbf{z}\| = O(h \cdot l \cdot n^2 \cdot k^2) \cdot \omega(\sqrt{\log n})^4 = \beta$.

To reduce the average-case SIS problem to the worst-case SIVP in lattices, $q \ge \beta \cdot \sqrt{n} \cdot \omega(\sqrt{\log n})$ should hold. Therefore,

$$\begin{aligned} q &\ge \beta \cdot \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right) \\ &= O\left(h \cdot l \cdot n^2 \cdot k^2\right) \cdot \omega\left(\sqrt{\log n}\right)^4 \cdot \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right) \\ &= O\left(h \cdot l \cdot n^{5/2} \cdot k^2\right) \cdot \omega\left(\sqrt{\log n}\right)^5. \end{aligned} \tag{25}$$

We note that $\mathcal{A}$ succeeds in its forgery if it correctly guesses μ' and $\mathbf{t}$. The probability of $\mathcal{A}$ correctly guessing μ' is $1/q_s$, and the probability of correctly guessing $\mathbf{t}$ is $1/{}_tC_l$. Therefore,

$$\mathsf{Adv}^{\mathsf{SIS}}_{\mathcal{A}} \ge \frac{1}{{}_tC_l \cdot q_s} \cdot \mathsf{Adv}^{\mathsf{su}}_{\mathsf{SRS},\mathcal{F}}, \tag{26}$$

where t is the number of users and l is the upper bound of the number of corrupted users.

For the third case, we can construct $\mathcal{A}$ attacking the $\mathrm{SIS}_{q,\beta}$ problem using $\mathcal{F}$. Assume that the number of corrupted users is at most l. $\mathcal{A}$ simulates the game of strong unforgeability with $\mathcal{F}$ as follows.

(i) *Setup*. $\mathcal{A}$ chooses a primitive matrix $\mathbf{G} \in \mathbb{Z}_q^{n \times nk}$. $\mathcal{A}$ takes as input $\mathbf{A}' \in \mathbb{Z}_q^{n \times (\overline{m}+lnk+1)}$ as a SIS instance and parses $\mathbf{A}'$ as $[\mathbf{A} \parallel \mathbf{u}] = [\overline{\mathbf{A}} \| \mathbf{A}_1^* \| \cdots \| \mathbf{A}_l^* \| \mathbf{u}]$, where $\overline{\mathbf{A}} \in \mathbb{Z}_q^{n \times \overline{m}}$, $\mathbf{A}_1^*, \ldots, \mathbf{A}_l^* \in \mathbb{Z}_q^{n \times nk}$, and $\mathbf{u} \in \mathbb{Z}_q^n$. $\mathcal{A}$ chooses a chameleon hash function $\mathsf{H}(\cdot,\cdot)$ with trapdoor information and distinct hash values $\{\mu_1, \ldots, \mu_{q_s}\}$, where $\mu_i \leftarrow \{0,1\}^h$ for $1 \le i \le q_s$. $\mathcal{A}$ constructs a set P of all shortest strings $p \in \{0,1\}^{\le h}$ such that each element of $\{\mu_1, \ldots, \mu_{q_s}\}$ has no p as a prefix. There exists an efficient algorithm for computing P, and the number of elements in P is at most $(h-1) \cdot q_s + 1$ [15, 17, 18]. $\mathcal{A}$ chooses p from P at random. $|p| \le h$, where $|p|$ is the bit length of p.

For $0 \le j \le h$, $\mathcal{A}$ computes $\mathbf{H}_j$ as follows:

$$\mathbf{H}_j = \begin{cases} h(0) = \mathbf{0} & j > |p| \\ (-1)^{p_j} \cdot h(u_j) & j \in \{1, \ldots, |p|\} \\ -\sum_{k=1}^{|p|} p_k \cdot \mathbf{H}_k & j = 0, \end{cases} \tag{27}$$

where p_j is the jth element in p and $h(\cdot)$ is a ring homomorphism.

For $0 \le j \le h$, $\mathcal{A}$ chooses $\mathbf{R}_j \leftarrow \mathcal{D}^{\overline{m} \times nk}_{\mathbb{Z}, \omega(\sqrt{\log n})}$ and computes the following:

$$\mathbf{C}_j = \mathbf{H}_j \mathbf{G} - \overline{\mathbf{A}} \mathbf{R}_j. \tag{28}$$

If any μ_i has p as a prefix, $\mathbf{H}_0 + \sum_{j=1}^{h} \mu_{i,j} \mathbf{H}_j = \mathbf{0} \in \mathbb{Z}^{n \times n}$, where $\mu_{i,j}$ is the jth element in μ_i. Otherwise, $\mathbf{H}_0 + \sum_{j=1}^{h} \mu_{i,j} \mathbf{H}_j \neq \mathbf{0} \in \mathbb{Z}^{n \times n}$ is an invertible matrix.

$\mathcal{A}$ randomly chooses $\mathbf{t} = (t_1, \ldots, t_t) \leftarrow \{0,1\}^t$ such that the number of 1s in $\mathbf{t}$ is l. If $t_k = 1$ for $1 \le k \le t$, $\mathcal{A}$ sets $\mathbf{A}_k = \mathbf{A}^*_i$ for $1 \le i \le l$ in turn. Otherwise, $\mathcal{A}$ chooses $\mathbf{T}_k \leftarrow \mathcal{D}^{\overline{m} \times nk}_{\mathbb{Z}, \omega(\sqrt{\log n})}$ and computes $\mathbf{A}_k = [\mathbf{G} - \overline{\mathbf{A}} \mathbf{T}_k]$.

$\mathcal{A}$ sends $\{\mathsf{params}, \mathsf{S}\}$ to $\mathcal{F}$, where $\mathsf{params} = \{\mathbf{G}, \overline{\mathbf{A}}, \mathbf{C}_0, \ldots, \mathbf{C}_h, \mathbf{u}, \mathsf{H}(\cdot,\cdot)\}$ and $\mathsf{S} = \{vk_1, \ldots, vk_t\} = \{\mathbf{A}_1, \ldots, \mathbf{A}_t\}$. $\mathcal{A}$ sets $\mathsf{CU} \leftarrow \emptyset$, where CU is a set of corrupted users.

(ii) *Signing Queries*. For $1 \le i \le q_s$, $\mathcal{F}$ sends $(e_i, \mathsf{R}_i, \mathsf{m}_i)$ such that $vk_{e_i} \in \mathsf{R}_i \cap \mathsf{S}$ to $\mathcal{A}$. $\mathcal{A}$ samples $\mathbf{r}_i$ with trapdoor information such that $\mu_i = \mathsf{H}(\mathsf{R}_i \parallel \mathsf{m}_i, \mathbf{r}_i)$. $\mathbf{A}_{\mathsf{R}_i, \mu_i}$ is represented as $[\overline{\mathbf{A}} \| \mathbf{A}_{\mathsf{R}_i} \| \mathbf{H}\mathbf{G} - \overline{\mathbf{A}}\mathbf{R}]$, where $\mathbf{H} = \mathbf{H}_0 + \sum_{j=1}^{h} \mu_{i,j} \mathbf{H}_j \neq \mathbf{0} \in \mathbb{Z}^{n \times n}$ and $\mathbf{R} = \mathbf{R}_0 + \sum_{j=1}^{h} \mu_{i,j} \mathbf{R}_j$.

The maximal singular value of $\mathbf{R}$ is as follows:

$$\begin{aligned} s_1(\mathbf{R}) &= \sqrt{h+1} \cdot O\left(\sqrt{\overline{m}} + \sqrt{nk}\right) \cdot \omega\left(\sqrt{\log n}\right) \\ &= \sqrt{h+1} \cdot O\left(\sqrt{nk} + \sqrt{nk}\right) \cdot \omega\left(\sqrt{\log n}\right) \\ &= \sqrt{h+1} \cdot O\left(\sqrt{nk}\right) \cdot \omega\left(\sqrt{\log n}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right). \end{aligned} \tag{29}$$

$\mathcal{A}$ calculates $\mathbf{R}' \leftarrow \mathsf{DelTrap}(\mathbf{A}_{\mathsf{R}_i, \mu_i}, \mathbf{R}, s')$, where $s' = O(\sqrt{hnk}) \cdot \omega(\sqrt{\log n})^2$.

Then, the maximal singular value of $\mathbf{R}'$ is as follows:

$$\begin{aligned} s_1(\mathbf{R}') &\le s' \cdot O\left(\sqrt{\overline{m} + nk} + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk + nk} + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{nk} + \sqrt{lnk}\right) \\ &= O\left(\sqrt{hnk}\right) \cdot \omega\left(\sqrt{\log n}\right)^2 \cdot O\left(\sqrt{lnk}\right) \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^2. \end{aligned} \tag{30}$$

$\mathcal{A}$ calculates $\mathbf{v}_i \leftarrow \mathsf{SampleD}(\mathbf{A}_{\mathsf{R}_i, \mu_i}, \mathbf{R}', \mathbf{u}, O(nk \cdot \sqrt{hl}) \cdot \omega(\sqrt{\log n})^2)$ from a distribution whose statistical distance from $\mathcal{D}_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}_{\mathsf{R}_i, \mu_i}), s}$ is negligible, where $s = O(nk \cdot \sqrt{hl}) \cdot \omega(\sqrt{\log n})^3$. $\mathcal{A}$ returns $\sigma_i = (\mathbf{v}_i, \mathbf{r}_i)$ to $\mathcal{F}$.

(iii) *Corruption Queries*. If $\mathcal{F}$ asks for sk_i, where $t_i = 1$, $\mathcal{A}$ aborts. Otherwise, $\mathcal{A}$ returns $sk_i = \mathbf{T}_i$ and adds $vk_i = \mathbf{A}_i$ to CU.

(iv) *Output*. $\mathcal{F}$ outputs $(\mathsf{R}^*, \mathsf{m}^*, \sigma^* = (\mathbf{v}^*, \mathbf{r}^*))$. If $\mu^* = \mathsf{H}(\mathsf{R}^* \parallel \mathsf{m}^*, \mathbf{r}^*)$ has no p as a prefix or $\mathbf{A} \neq [\overline{\mathbf{A}} \parallel \mathbf{A}_{\mathsf{R}^*}]$, $\mathcal{A}$ aborts. Otherwise, $\mathbf{A}_{\mathsf{R}^*, \mu^*}$ is represented as $[\overline{\mathbf{A}} \| \mathbf{A}_{\mathsf{R}^*} \| - \overline{\mathbf{A}}\mathbf{R}^*]$, where $\mathbf{H}^* = \mathbf{H}_0 + \sum_{j=1}^{h} \mu^*_j \mathbf{H}_j = \mathbf{0} \in \mathbb{Z}^{n \times n}$ and $\mathbf{R}^* = \mathbf{R}_0 + \sum_{j=1}^{h} \mu^*_j \mathbf{R}_j$. Therefore, we obtain the following equation:

$$\begin{aligned} \mathbf{A}_{\mathsf{R}^*, \mu^*} \cdot \mathbf{v}^* &= \left[\overline{\mathbf{A}} \middle\| \mathbf{A}_{\mathsf{R}^*} \middle\| - \overline{\mathbf{A}}\mathbf{R}^*\right] \cdot \mathbf{v}^* \\ &= \left[\overline{\mathbf{A}} \parallel \mathbf{A}_{\mathsf{R}^*}\right] \begin{bmatrix} \mathbf{I}_{\overline{m}} & -\mathbf{R}^* \\ & \mathbf{I}_{lnk} \end{bmatrix} \cdot \mathbf{v}^* \\ &= \mathbf{A} \cdot \begin{bmatrix} \mathbf{I}_{\overline{m}} & -\mathbf{R}^* \\ & \mathbf{I}_{lnk} \end{bmatrix} \cdot \mathbf{v}^* \\ &= \mathbf{u} \pmod q. \end{aligned} \tag{31}$$

Let $\mathbf{z} \in \mathbb{Z}^{\overline{m}+lnk}$ be $\begin{bmatrix} \mathbf{I}_{\overline{m}} & -\mathbf{R}^* \\ & \mathbf{I}_{lnk} \end{bmatrix} \cdot \mathbf{v}^*$ and let $\mathbf{z}' \in \mathbb{Z}^{\overline{m}+lnk+1}$ be $\begin{bmatrix} \mathbf{z} \\ -1 \end{bmatrix}$. Then, $\mathbf{A}\mathbf{z} = \mathbf{u} \pmod q$ and

$$\mathbf{A}'\mathbf{z}' = [\mathbf{A} \parallel \mathbf{u}] \begin{bmatrix} \mathbf{z} \\ -1 \end{bmatrix} = \mathbf{u} - \mathbf{u} = \mathbf{0} \pmod q. \tag{32}$$

$\mathcal{A}$ outputs $\mathbf{z}'$ as a SIS solution to $\mathbf{A}'$.

The Euclidean norm of $\mathbf{v}^*$ is as follows:

$$\begin{aligned} \|\mathbf{v}^*\| &\le s \cdot \sqrt{m} \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot \sqrt{\overline{m} + (l+1) \cdot nk} \\ &= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot O\left(\sqrt{nk + (l+1) \cdot nk}\right) \end{aligned}$$

$$= O\left(nk \cdot \sqrt{hl}\right) \cdot \omega\left(\sqrt{\log n}\right)^3 \cdot O\left(\sqrt{lnk}\right)$$
$$= O\left(h^{1/2} \cdot l \cdot n^{3/2} \cdot k^{3/2}\right) \cdot \omega\left(\sqrt{\log n}\right)^3. \quad (33)$$

Because $\|\mathbf{v}^*\| \le s \cdot \sqrt{m} = O(h^{1/2} \cdot l \cdot n^{3/2} \cdot k^{3/2}) \cdot \omega(\sqrt{\log n})^3$, $\|\mathbf{z}'\| \approx \|\mathbf{z}\| = O(h \cdot l \cdot n^2 \cdot k^2) \cdot \omega(\sqrt{\log n})^4 = \beta$.

To reduce the average-case SIS problem to the worst-case SIVP in lattices, $q \ge \beta \cdot \sqrt{n} \cdot \omega(\sqrt{\log n})$ should hold. Therefore,

$$q \ge \beta \cdot \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right)$$
$$= O\left(h \cdot l \cdot n^2 \cdot k^2\right) \cdot \omega\left(\sqrt{\log n}\right)^4 \cdot \sqrt{n} \cdot \omega\left(\sqrt{\log n}\right) \quad (34)$$
$$= O\left(h \cdot l \cdot n^{5/2} \cdot k^2\right) \cdot \omega\left(\sqrt{\log n}\right)^5.$$

We note that $\mathscr{A}$ succeeds in its forgery if $\mathscr{A}$ correctly guesses μ^* and $\mathbf{t}$ such that μ^* has p as a prefix. The probability of $\mathscr{A}$ correctly guessing μ^* such that μ^* has p as a prefix is $1/((h-1) \cdot q_s + 1)$. The probability that $\mathscr{A}$ correctly guesses $\mathbf{t}$ is $1/{}_tC_l$. Therefore,

$$\mathsf{Adv}^{\mathrm{SIS}}_{\mathscr{A}} \ge \frac{1}{{}_tC_l \cdot \{(h-1) \cdot q_s + 1\}} \cdot \mathsf{Adv}^{\mathsf{su}}_{\mathsf{SRS},\mathscr{F}}, \quad (35)$$

where t is the number of users and l is the upper bound of the number of corrupted users.

Our ring signature scheme has the property that the upper bound of the number of corrupted users should be constant. In proving strong unforgeability with respect to insider corruption for our ring signature scheme, the advantage of a forger is limited by the advantage of the SIS problem solver factored by ${}_tC_l$, where t is the number of users and l is the upper bound of the number of corrupted users. The lower and upper bounds of ${}_tC_l$ are as follows [30]:

$$\left(\frac{t}{l}\right)^l \le {}_tC_l \le \left(\frac{et}{l}\right)^l. \quad (36)$$

If $l = t/2$ (i.e., the maximal value of ${}_tC_l$), the lower and upper bounds on ${}_tC_l$ are as follows:

$$2^{t/2} \le {}_tC_{t/2} \le (2e)^{t/2}. \quad (37)$$

Thus, the value of ${}_tC_{t/2}$ grows exponentially if l grows polynomially; that is, the upper bound of corrupted users, l, in our ring signature scheme needs to be some constant.

Therefore, our ring signature scheme SRS is strongly unforgeable with respect to insider corruption in the standard model. □

6. Conclusion

In this paper, we have shown that all of Wang-Sun's ring signature schemes are not in fact existentially unforgeable. We then have developed the more secure concept of strong unforgeability for ring signatures and have suggested a new ring signature scheme from lattices in the standard model that satisfies strong unforgeability. Our ring signature scheme is anonymous against full key exposure and is strongly unforgeable with respect to insider corruption in the standard model.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was partly supported by Basic Science Research Programs through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (NRF-2012R1A1A3005550, 2013R1A2A2A01068200).

References

[1] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT 2001*, C. Boyd, Ed., vol. 2248 of *Lecture Notes in Computer Science*, pp. 552–565, Springer, Berlin, Germany, 2001.

[2] Y. Dodis, A. Kiayias, A. Nicolosi, and V. Shoup, "Anonymous identification in ad hoc groups," in *Advances in Cryptology—EUROCRYPT 2004*, C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science*, pp. 609–626, Springer, Berlin, Germany, 2004.

[3] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," in *Advances in Cryptology—CRYPTO '86*, A. M. Odlyzko, Ed., vol. 263 of *Lecture Notes in Computer Science*, pp. 186–194, Springer, Berlin, Germany, 1987.

[4] A. Bender, J. Katz, and R. Morselli, "Ring signatures: stronger definitions, and constructions without random oracles," *Journal of Cryptology*, vol. 22, no. 1, pp. 114–138, 2009.

[5] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Public Key Cryptography—PKC 2007*, T. Okamoto and X. Wang, Eds., vol. 4450 of *Lecture Notes in Computer Science*, pp. 166–180, Springer, Berlin, Germany, 2007.

[6] C.-H. Wang and C.-Y. Liu, "A new ring signature scheme with signer-admission property," *Information Sciences*, vol. 177, no. 3, pp. 747–754, 2007.

[7] I. R. Jeong, J. O. Kwon, and D. H. Lee, "Ring signature with weak linkability and its applications," *IEEE Transactions on Knowledge and Data Engineering*, vol. 20, no. 8, pp. 1145–1148, 2008.

[8] S. S. M. Chow, "Blind signature and ring signature schemes: rehabilitation and attack," *Computer Standards & Interfaces*, vol. 31, no. 4, pp. 707–712, 2009.

[9] J. Y. Hwang, "A note on an identity-based ring signature scheme with signer verifiability," *Theoretical Computer Science*, vol. 412, no. 8–10, pp. 796–804, 2011.

[10] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.

[11] S. Zeng, S. Jiang, and Z. Qin, "An efficient conditionally anonymous ring signature in the random oracle model," *Theoretical Computer Science*, vol. 461, pp. 106–114, 2012.

[12] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[13] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing (STOC '08)*, C. Dwork, Ed., pp. 197–206, May 2008.

[14] J. Buchmann, R. Lindner, M. Rückert, and M. Schneider, "Post-quantum cryptography: lattice signatures," *Computing*, vol. 85, no. 1-2, pp. 105–125, 2009.

[15] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Journal of Cryptology*, vol. 25, no. 4, pp. 601–639, 2012.

[16] X. Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Public Key Cryptography—PKC 2010*, P. Q. Nguyen and D. Pointcheval, Eds., vol. 6056 of *Lecture Notes in Computer Science*, pp. 499–517, Springer, Berlin, Germany, 2010.

[17] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *Post-Quantum Cryptography*, N. Sendrier, Ed., vol. 6061 of *Lecture Notes in Computer Science*, pp. 182–200, Springer, Berlin, Germany, 2010.

[18] D. Micciancio and C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Advances in Cryptology—EUROCRYPT 2012*, D. Pointcheval and T. Johansson, Eds., vol. 7237 of *Lecture Notes in Computer Science*, pp. 700–718, Springer, Berlin, Germany, 2012.

[19] Z. Brakerski and Y. T. Kalai, "A framework for efficient signatures, ring signatures and identity based encryption in the standard model," Cryptology ePrint Archive, report 2010/086, 2010http://eprint.iacr.org/2010/086.

[20] P. Cayrel, R. Lindner, M. Rückert, and R. Silva, "A lattice-based thresh-old ring signature scheme," in *Progress in Cryptology—LATINCRYPT 2010*, M. Abdalla and P. S. L. M. Barreto, Eds., vol. 6212 of *Lecture Notes in Computer Science*, pp. 255–272, Springer, Berlin, Germany, 2010.

[21] J. Wang and B. Sun, "Ring signature schemes from lattice basis delegation," in *Information and Communications Security*, S. Qing, W. Susilo, G. Wang, and D. Liu, Eds., vol. 7043 of *Lecture Notes in Computer Science*, pp. 15–28, Springer, Berlin, Germany, 2011.

[22] C. Aguilar Melchor, S. Bettaieb, X. Boyen, L. Fousse, and P. Gaborit, "Adapting Lyubashevsky's signature schemes to the ring signature setting," in *Progress in Cryptology—AFRICACRYPT 2013*, A. Youssef, A. Nitaj, and A. E. Hassanien, Eds., vol. 7918 of *Lecture Notes in Computer Science*, pp. 1–25, Springer, Berlin, Germany, 2013.

[23] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," in *Advances in Cryptology—EUROCRYPT 2002*, L. R. Knudsen, Ed., vol. 2332 of *Lecture Notes in Computer Science*, pp. 83–107, Springer, Berlin, Germany, 2002.

[24] D. Boneh and X. Boyen, "Short signatures without random oracles," in *Advances in Cryptology—EUROCRYPT 2004*, C. Cachin and J. Camenisch, Eds., vol. 3027 of *Lecture Notes in Computer Science*, pp. 56–73, Springer, Berlin, Germany, 2004.

[25] D. Boneh, E. Shen, and B. Waters, "Strongly unforgeable signatures based on computational Diffie-Hellman," in *Public Key Cryptography—PKC 2006*, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds., vol. 3958 of *Lecture Notes in Computer Science*, pp. 229–240, Springer, Berlin, Germany, 2006.

[26] M. Ajtai, "Generating hard instances of lattice problems," in *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC '96)*, G. L. Miller, Ed., pp. 99–108, May 1996.

[27] 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.

[28] C. Peikert and A. Rosen, "Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices," in *Theory of Cryptography*, S. Halevi and T. Rabin, Eds., vol. 3876 of *Lecture Notes in Computer Science*, pp. 145–166, Springer, Berlin, Germany, 2006.

[29] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Mathematische Annalen*, vol. 296, no. 1, pp. 625–635, 1993.

[30] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, The MIT Press, London, UK, 3rd edition, 2009.