Hindawi
Security and Communication Networks
Volume 2018, Article ID 8525163, 13 pages
https://doi.org/10.1155/2018/8525163

Research Article

Key Substitution Attacks on Lattice Signature Schemes Based on SIS Problem

Youngjoo An,[1] **Hyang-Sook Lee**,[1] **Juhee Lee**,[2] **and Seongan Lim**[2]

[1]*Department of Mathematics, Ewha Womans University, Seoul 120-750, Republic of Korea*
[2]*Institute of Mathematical Sciences, Ewha Womans University, Seoul 120-750, Republic of Korea*

Correspondence should be addressed to Youngjoo An; hello.joo@hotmail.com

Received 12 June 2018; Revised 3 August 2018; Accepted 30 August 2018; Published 23 September 2018

Academic Editor: Salvatore D'Antonio

The notion of key substitution security on digital signatures in the multiuser setting has been proposed by Menezes and Smart in 2004. Along with the unforgeability of signature, the key substitution security is very important since it is a critical requirement for the nonrepudiation and the authentication of the signature. Lattice-based signature is a promising candidate for post-quantum cryptography, and the unforgeability of each scheme has been relatively well studied. In this paper, we present key substitution attacks on BLISS, Lyubashevsky's signature scheme, and GPV and thus show that these signature schemes do not provide nonrepudiation. We also suggest how to avoid key substitution attack on these schemes.

1. Introduction

The classical cryptography based on factoring or discrete-logarithm problem is vulnerable to cryptanalysis by quantum computers. To prepare for a security plan after the emergence of quantum computing, NIST [1] and ETSI [2] currently try to standardize public key algorithms of three categories, namely, digital signature, public key encryption, and key exchange protocol. Among them, digital signatures are commonly used for authenticated key exchange protocol, software distribution, financial transactions, and contract management software and in other cases where it is important to detect forgery or tampering.

The established security notion for digital signature schemes is *existentially unforgeable against adaptive chosen-message attacks* introduced by Goldwasser, Micali, and Rivest [3]. Although a signature scheme secure in this scenario offers rather strong security guarantees, further requirements can be crucial in certain applications. For example, Koblitz, Menezes, and Smart [4, 5] indicate that the GMR security is not sufficient in a multiuser setting by proposing a new type of attack on digital signature scheme, which is called a key substitution attack. In the key substitution attack, an adversary is given a public key pk and a signature sig on a message m under pk, and then he tries to produce a new public key pk' different from pk, which validates the same signature sig on the same message m under the new public key pk'.

A serious practical danger of key substitution attacks is that they not only undermine nonrepudiation but are disable to authenticate the signer who signed the message. These are core functionalities the digital signature can offer. Nonrepudiation refers to the ability to ensure that a sender who signed a message or document cannot later deny having sign it. The US government standard for digital signatures states that nonrepudiation and authentication are main characteristics of a signature scheme [6]. In the key substitution attack, a successful attacker obtains a new public key pk', which validates a given signature signed by the signer. As a result, one signature is valid under two different public keys which affects these functionalities of the signature scheme. In other words, the threat of the key substitution attack is that there are two (or more) different valid public keys for the same given signature.

A typical scenario where the key substitution attack has damaging consequences is the following. Suppose that Bob has signed an important contract with Alice. When the contract was nullified by Bob, he cannot claim that he did not sign the contract with Alice if the nonrepudiation property of the digital signature scheme works properly, because Alice

presents the contract signed by Bob's signature corresponding to his public key $\mathsf{pk}_{\mathrm{Bob}}$ as an evidence of his lying. However, if the signature scheme is attacked by the key substitution attack, the scheme loses its function of nonrepudiation. Then Bob insists that he has not signed the contract with Alice and the signature on the contract presented by Alice is not what he has signed. As a proof of his claim, he mounts a key substitution attack to obtain a new public key pk' different from $\mathsf{pk}_{\mathrm{Bob}}$ and shows that the contract signed by the same signature can be validated by using the public key pk'. It means that it is hard to prove that Bob has signed a contract with Alice by using $\mathsf{pk}_{\mathrm{Bob}}$. It is serious issue to weaken the usability of the digital signature scheme in the real world. Therefore, it is crucial for the digital signature scheme to prevent the key substitution attack. It is noteworthy that the legal signer, Bob, could be a potential attacker in the key substitution attacks. For more real-world impact of the key substitution attack, we refer to [4].

In this paper, we present key substitution attacks on the lattice signature schemes based on SIS problem such as GPV signature scheme [7], Lyubashevsky's signature scheme [8], and BLISS [9]. Note that lattice-based cryptography is a most promising candidate for post-quantum cryptography, and BLISS (Bimodal Lattice Signature Scheme) is currently one of the most compact and efficient lattice-based signature schemes that is provably secure under lattice assumptions.

We present two kinds of key substitution attacks. The first one is weak key substitution attack in which the adversary who may be a legal signer wants to ruin the properties of the digital signature schemes by obtaining new public and private key pairs. This type of attack is considered in [10, 11], and e-coupon and e-lottery were presented as concrete examples of these attacks. For instance, an electronic coupon (e-coupon) system works as follows. When issuing the e-coupon for a customer, in order to prevent illegal use of the e-coupon, it requires the customer to sign the e-coupon. Then the e-coupon is signed by the issuer and it will be issued to the customer as a legitimate buyer. Before he redeems the e-coupon at the store, he needs to show the ownership of the e-coupon by zero-knowledge proof of his secret key. Assume that a successful weak key substitution attacker Alice has a valid e-coupon and duplicates the e-coupon with the same signature under pk' and sk'. Then she can use the e-coupon multiple times to buy the goods because she is able to prove that she owns the e-coupons by using sk'. Moreover, if Alice sells the copies of e-coupon with pk' and sk' to unauthorized users, she gets the financial benefits from it and illegal users obtain the goods using the e-coupon with sk' at the shop.

The other is strong key substitution attack in which an adversary, not necessary to be a signer, wants to compute a new public key validating a given signature. In this case the attacker may interfere with the communication between a signer and a verifier in order to achieve his malicious goal, like the unknown key share attack proposed in [12].

In our attacks on these signature schemes, we solve linear equations for a valid new public key pk' to pass the verification algorithm. One of the important requirements is to check if a hash value for given sig and pk' is correct. On SIS-based signature schemes mentioned above, we succeed in substituting a new public key pk' using algebraic structures depending on each signature scheme without finding the collision of hash function on the same message.

This paper is organized as follows. In Section 2, we introduce some necessary cryptographic and mathematical backgrounds, including the definitions of SIS problem and key substitution attack. In Section 3, we recall three lattice-based signature schemes, namely, GPV signature [7], Lyubashevsky's signature [8], and BLISS [9], and present key substitution attacks on these schemes. In Section 4, we examine the effectiveness of the proposed attacks and explain how to avoid key substitution attacks on these schemes. In Section 5, we conclude our paper.

2. Preliminaries

2.1. Notations. We assume that all vectors are column vectors and vectors will be written in bold lower case letters. Matrices will be written in upper case letters. For vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$, let $[\mathbf{b}_1, \ldots, \mathbf{b}_m]$ denote a matrix whose i-th column is $\mathbf{b}_i$.

The ℓ_p norm of a vector $\mathbf{v}$ is denoted by $\|\mathbf{v}\|_p$ and we will usually avoid writing the p for the ℓ_2 norm. For a distribution $\mathscr{D}$, we use the notation $x \longleftarrow \mathscr{D}$ to mean that x is chosen according to the distribution $\mathscr{D}$. If S is a set, then $x \xleftarrow{\$} S$ means that x is chosen uniformly at random from S. For integers $a \geq b$, let $[a, b]$ denote the set of integers $\{a, a+1, \ldots, b\}$.

2.2. Some Basics on Lattices. Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$ consist of n linearly independent vectors. The n-dimensional lattice $\mathscr{L}$ generated by the basis $\mathbf{B}$ is $\mathscr{L} = \{\sum_{1 \leq i \leq n} c_i \mathbf{b}_i : c_i \in \mathbb{Z}\}$. A lattice $\mathscr{L} \subseteq \mathbb{R}^m$ is a discrete additive subgroup of $\mathbb{R}^m$. If $n = m$, we say that $\mathscr{L}$ is full-rank.

The minimum distance $\lambda_1(\mathscr{L})$ of a lattice $\mathscr{L}$ is the length of its shortest nonzero vector in the ℓ_2 norm: $\lambda_1(\mathscr{L}) = \min_{\mathbf{x} \in \mathscr{L} \setminus \{\mathbf{0}\}} \|\mathbf{x}\|$. We write $\lambda_1^{\infty}(\mathscr{L})$ to denote the minimum distance of a lattice $\mathscr{L}$ in the ℓ_∞ norm. More generally, the k-th minimum $\lambda_k(\mathscr{L})$ for $k \leq n$ is defined as the smallest r such that $\mathscr{L}$ contains $\geq k$ linearly independent vectors of norm $\leq r$. If $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ is a basis matrix of $\mathscr{L}$, the fundamental parallelepiped of B is the set $\mathscr{P}(B) = \{\sum_{1 \leq i \leq n} c_i \mathbf{b}_i : c_i \in [0, 1)\}$. The volume $\det(B^T B)$ of $\mathscr{P}(B)$ is an invariant of the lattice $\mathscr{L}$ which is denoted by $\det(\mathscr{L})$. Minkowski's theorem states that $\lambda_1(\mathscr{L}) \leq \sqrt{n} \det(\mathscr{L})^{1/n}$. The dual lattice of $\mathscr{L}$, denoted by $\mathscr{L}^*$, is defined as $\mathscr{L}^* = \{\mathbf{x} \in \mathbb{R}^n : \forall \mathbf{v} \in \mathscr{L}, \langle \mathbf{x}, \mathbf{v} \rangle \in \mathbb{Z}\}$.

The following background results are borrowed from [13, Section 2]. Let n a power of 2, $\Phi(x) = x^n + 1$, and $\mathscr{R} = \mathbb{Z}[x]/\Phi(x)$. An ideal I of $\mathscr{R}$ is a subset of $\mathscr{R}$ which is closed under addition and multiplication by arbitrary elements of $\mathscr{R}$. By mapping polynomials to the vectors of their coefficients, we can see that an ideal $I \neq 0$ corresponds to a full-rank sublattice of $\mathbb{Z}^n$. An ideal lattice for $\Phi(x)$ is a sublattice of $\mathbb{Z}^n$ that corresponds to a nonzero ideal I of $\mathscr{R}$. The algebraic norm $\mathscr{N}(I)$ is the cardinality of $\mathscr{R}/I$ and it is equal to $\det(I)$ where I is regarded as a lattice. Any nonzero ideal I of $\mathscr{R}$ satisfies $\lambda_n(I) = \lambda_1(I)$.

For an integer q, the elements in $\mathbb{Z}_q$ are represented by integers in the range $[-(q-1)/2, (q-1)/2)$. Let $A \in \mathbb{Z}_q^{n \times m}$ for

some positive integers n, m, q. We consider two kinds of full-rank m-dimensional integer lattices defined by A. The first consists of those integer vectors that are orthogonal (modulo q) to the rows of A, and it is defined as $\mathscr{L}^{\perp}(A) = \{\mathbf{e} \in \mathbb{Z}^m : A\mathbf{e} \equiv \mathbf{0} \bmod q\}$. The second lattice is generated by the transposed rows of A, and it is defined as $\mathscr{L}(A) = \{\mathbf{y} \in \mathbb{Z}^m : \mathbf{y} \equiv A^T\mathbf{s} \bmod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$. In terminology of coding theory, A is the parity check matrix for the linear code $\{\mathbf{e} \in \mathbb{Z}^m : A\mathbf{e} \equiv \mathbf{0} \bmod q\}$ over $\mathbb{Z}_q$, and A^T is the generator matrix for the lattice $\{\mathbf{y} \in \mathbb{Z}_q^m : \mathbf{y} \equiv A^T\mathbf{s} \bmod q\}$ over $\mathbb{Z}_q$. When A is clear in the context, we can omit it and just write $\mathscr{L}$ and $\mathscr{L}^{\perp}$.

Micciancio and Regev [14] introduced a lattice quantity called the smoothing parameter.

Definition 1 (see [14]). For any n-dimensional lattice $\mathscr{L}$ and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\mathscr{L})$ is the smallest real $s > 0$ such that $\rho_{1/s}(\mathscr{L}^* \setminus \{\mathbf{0}\}) \leq \epsilon$.

The following lemma shows that a Gaussian sample over $\mathscr{L}$ is distributed almost-uniformly modulo a sublattice $\mathscr{L}'$, if $s \geq \eta_\epsilon(\mathscr{L}')$.

Lemma 2 (see [14]). *Let $\mathscr{L}, \mathscr{L}'$ be n-dimensional lattices, with $\mathscr{L}' \subseteq \mathscr{L}$. Then for any $\epsilon \in (0, 1/2)$, any $s \geq \eta_\epsilon(\mathscr{L}')$, and any $\mathbf{c} \in \mathbb{R}^n$, the distribution of $(D_{\Lambda,s,\mathbf{c}} \bmod \mathscr{L}')$ is within statistical distance at most 2ϵ of uniform over $(\mathscr{L} \bmod \mathscr{L}')$.*

The following lemma also shows that the smoothing parameter of a lattice is related to the minimum distance of its dual lattice in the ℓ_∞ norm or to the n-th minimum of the lattice.

Lemma 3 (see [15]). *For any n-dimensional lattice $\mathscr{L}$ and real $\epsilon > 0$, we have*

$$\eta_\epsilon(\mathscr{L}) \leq \frac{\sqrt{\ln(2n(1+1/\epsilon))/\pi}}{\lambda_1^\infty(\mathscr{L}^*)}. \tag{1}$$

Lemma 4 (see [14]). *For any n-dimensional lattice $\mathscr{L}$ and real $\epsilon > 0$, we have*

$$\eta_\epsilon(\mathscr{L}) \leq \sqrt{\frac{\ln(2n(1+1/\epsilon))}{\pi}} \cdot \lambda_n(\mathscr{L}). \tag{2}$$

2.3. SIS Problems on Lattices. We recall the definition of the generalized Short Integer Solution (SIS) problem. This average case problem proposed by Ajtai [16] is to find a short nonzero integer solution $\mathbf{e} \in \mathbb{Z}^m$ to the homogeneous linear system $A\mathbf{e} \equiv \mathbf{0} \bmod q$ for uniformly random $A \in \mathbb{Z}_q^{n\times m}$. This is syntactically equivalent to finding an approximately short nonzero vector in $\mathscr{L}^{\perp}(A)$. The problem was formalized as follows in [14].

Definition 5 (ℓ_2-$\mathbf{SIS}_{q,n,m,\beta}$ problem). The small integer solution problem SIS (in the ℓ_2 norm) is defined as follows: given an integer q, a random matrix $A \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, and a positive real number β, find a nonzero vector $\mathbf{e} \in \mathbb{Z}^m$ such that $A\mathbf{e} \equiv \mathbf{0} \bmod q$ and $\|\mathbf{e}\| \leq \beta$.

By the pigeonhole principle, if $\beta \geq \sqrt{m}q^{n/m}$, then the SIS instances are guaranteed to have a solution. We now recall a variant problem, which is to find a short solution to a random inhomogeneous system, specifically, $A\mathbf{e} \equiv \mathbf{u} \bmod q$ (where both A and $\mathbf{u}$ are uniformly random).

Definition 6 (ℓ_2-$\mathbf{ISIS}_{q,n,m,\beta}$ problem). The inhomogeneous small integer solution problem ISIS (in the ℓ_2 norm) is as follows: given an integer q, a matrix $A \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, a syndrome $\mathbf{u} \in \mathbb{Z}_q^n$, and a real β, find an integer vector $\mathbf{e} \in \mathbb{Z}^m$ such that $A\mathbf{e} \equiv \mathbf{u} \bmod q$ and $\|\mathbf{e}\| \leq \beta$.

2.4. Probability Distributions. The continuous normal distribution over $\mathbb{R}^m$ centered at $\mathbf{v}$ with standard deviation σ is defined by the function $\rho_{\mathbf{v},\sigma}^m(\mathbf{x}) = (1/\sqrt{2\pi\sigma^2})^m \exp(-\|\mathbf{x} - \mathbf{v}\|^2/2\sigma^2)$. When $\mathbf{v} = 0$, we write $\rho_\sigma^m(\mathbf{x})$. The discrete normal distribution over an m-dimensional lattice $\mathscr{L}$ centered at some $\mathbf{v} \in \mathscr{L}$ with standard deviation σ is defined as $D_{\mathscr{L},\mathbf{v},\sigma}^m(\mathbf{x}) = \rho_{\mathbf{v},\sigma}^m(\mathbf{x})/\rho_\sigma^m(\mathscr{L})$ where the quantity $\rho_\sigma^m(\mathscr{L}) = \sum_{\mathbf{z}\in\mathscr{L}} \rho_\sigma^m(\mathbf{z})$ is just a scaling quantity needed to make the function into a probability distribution. When $\mathscr{L} = \mathbb{Z}^m$, we write $D_{\mathscr{L},\mathbf{v},\sigma}^m$ as $D_{\mathbf{v},\sigma}^m$, and D_σ^m denotes $D_{\mathbf{v}=\mathbf{0},\sigma}^m$. When $m = 1$, we write D_σ^1 as D_σ.

The following lemma shows the equivalence of two distributions which is used in the construction of Lyubashevsky's signature scheme [8] and BLISS [9].

Lemma 7 (rejection sampling [9]). *Let V be an arbitrary set, and let $h : V \longrightarrow \mathbb{R}$ and $f : \mathbb{Z}^m \longrightarrow \mathbb{R}$ be probability distributions. If $g_v : \mathbb{Z}^m \longrightarrow \mathbb{R}$ is a family of probability distributions indexed by $v \in V$ with property that there exists a $M \in \mathbb{R}$ such that $\forall v \in V, \forall \mathbf{z} \in \mathbb{Z}^m, M \cdot g_v(\mathbf{z}) \geq f(\mathbf{z})$, then the output distributions of the following two algorithms are identical:*

(1) *$v \longleftarrow h$, $\mathbf{z} \longleftarrow g_v$, output $(\mathbf{z}, v)$ with probability $f(\mathbf{z})/(M \cdot g_v(\mathbf{z}))$.*

(2) *$v \longleftarrow h$, $\mathbf{z} \longleftarrow f$, output $(\mathbf{z}, v)$ with probability $1/M$.*

2.5. Signatures and Key Substitution Attack. In this section we recall the definition of digital signature schemes and introduce the key substitution attack against it.

Definition 8 (signature scheme [11]). A signature scheme $\mathcal{S}$ is a triple of algorithms $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$, where, for security parameter κ,

(i) $\mathsf{KeyGen}(1^\kappa)$, the key pair generation algorithm, is a probabilistic polynomial-time algorithm which outputs a private/public key pair $(\mathsf{sk}, \mathsf{pk})$ on input of domain parameters pp which is an output of the setup algorithm taking a security parameter κ as an input;

(ii) $\mathsf{Sign}(\mathsf{pp}, \mathsf{sk}, \mu)$, the signature generation algorithm, is a probabilistic polynomial-time algorithm which on input of message μ and a private key sk associated with domain parameters pp outputs a digital signature sig;

(iii) $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig})$, the signature verification algorithm, is a deterministic algorithm which on input of

a message μ, signature sig, valid domain parameters pp, and a public key pk outputs 1 (= valid) or 0 (= invalid).

A digital signature scheme is *secure* if it is *correct* and *existentially unforgeable* under adaptive chosen-message attack (EUF-CMA). These properties are defined below. For simplicity, we omit the input pp in Sign and Verify and just write it as $\mathsf{Sign}(\mathsf{sk}, \mu)$ and $\mathsf{Verify}(\mathsf{pk}, \mu, \mathsf{sig})$.

Definition 9 (correctness). A digital signature scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is correct if for all $\kappa \in \mathbb{N}$, all key pairs $(\mathsf{sk}, \mathsf{pk}) \in \mathsf{KeyGen}(1^\kappa)$, and all messages μ we have

$$\Pr\left[\mathsf{Verify}\left(\mathsf{pk}, \mu, \mathsf{Sign}\left(\mathsf{sk}, \mu\right)\right) = 1\right] = 1. \tag{3}$$

Definition 10 (EUF-CMA). A digital signature scheme $(\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Verify})$ is existentially unforgeable under adaptive chosen-message attacks if for all probabilistic polynomial-time algorithms $\mathscr{A}$ with access to a signing oracle $\mathsf{Sign}(\mathsf{sk}, \cdot)$ there is a negligible function $\epsilon(\cdot)$ such that

$$\Pr\left[\begin{array}{l}\left\{\begin{array}{ll}(\mathsf{sk}, \mathsf{pk}) \longleftarrow \mathsf{KeyGen}\left(1^\kappa\right) & \\ \left(\mu^*, \mathsf{sig}^*\right) \longleftarrow \mathscr{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}\left(\mathsf{pk}\right) & : \left(\mu^* \notin Q\right)\end{array}\right. \\ \wedge \left(\mathsf{Verify}\left(\mathsf{pk}, \mu^*, \mathsf{sig}^*\right) = 1\right)\end{array}\right] \leq \epsilon\left(\kappa\right), \tag{4}$$

where Q is the set of queries which $\mathscr{A}$ has accessed to the signing oracle.

We consider an additional checking algorithm Check to check the validity of a public key pk. Given the domain parameters pp and a candidate public key pk, the checking algorithm $\mathsf{Check}(\mathsf{pp}, \mathsf{pk})$ returns 1 if and only if the pk is valid under the domain parameters pp.

Definition 11 (key substitution attack [11]). Given a signature scheme $\mathcal{S}$, a key substitution attack (with malicious signer) is a probabilistic polynomial-time algorithm $\mathscr{A}$ which on input of valid domain parameters pp outputs two valid public keys pk and pk' (passing the tests for $\mathsf{KeyGen}(\mathsf{pp}, \mathsf{pk})$ and $\mathsf{Check}(\mathsf{pp}, \mathsf{pk}')$) and a message/signature pair (μ, sig) where $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig}) = 1$ and $\mathsf{Verify}(\mathsf{pp}, \mathsf{pk}', \mu, \mathsf{sig}) = 1$. When taking into account certificates, key substitution attack has access to a certification oracle.

A key substitution attack is called *weak* if an adversary also needs to output private keys sk and sk' corresponding to pk and pk', respectively; otherwise key substitution attack is called *strong*. A digital signature scheme is *strong* (resp., *weak*) key substitution secure if it is secure against *strong* (resp., *weak*) key substitution attacks.

Remark 12. When considering the nonrepudiation property of signature schemes, it is important to note that the legal signers can be considered as attackers since the repudiation of a signature is a malicious goal of legal signers.

Remark 13. A more general version of key substitution attack, which is called *message and key substitution* (MKS) attack by Menezes and Smart [5], states that the adversary has generated a valid public key $\mathsf{pk}' \neq \mathsf{pk}$ and a message $m' \neq m$ such that the same signature sig is valid under public key pk' for given valid signature sig on a message m under the public key pk. In [5], Menezes and Smart regarded MKS as an attack with little meaning, since signatures by themselves have no meaning and so they cannot envision a realistic scenario where this ability can have damaging consequence.

3. Key Substitution Attacks on SIS-Based Signature Schemes

In this section, we describe three SIS-based signature schemes: GPV signature scheme [7], Lyubashevsky's signature scheme [8], and BLISS [9]. We present strong key substitution attacks on these schemes. We also provide weak key substitution attacks on these schemes where a legal signer acts as an attacker, and this implies that these signature schemes have a problem in providing nonrepudiation property, even if the certificate authority requires users to prove possession of user's private key before issuing certificates. We note that even though our weak key substitution attack is not successful when the attacker is not the original signer, at least it can be said that there may be a problem in providing nonrepudiation with these signature schemes.

3.1. Attacks on GPV Signature Scheme

Description of GPV Signature Scheme. First, we present key substitution attacks on GPV signature scheme designed by Gentry, Peikert, and Vaikuntanathan [7]. Before continuing, we briefly describe the key generation algorithm $\mathsf{KeyGen.GPV}$, signature generation algorithm $\mathsf{Sign.GPV}$, and signature verification algorithm $\mathsf{Verify.GPV}$ of the GPV signature scheme.

$\mathsf{KeyGen.GPV}(1^\kappa)$: On the given input 1^κ, the algorithm samples a pair of matrices (A, T), where $A \in \mathbb{Z}_q^{n \times m}$ is a matrix of rank n over $\mathbb{Z}_q$ and $T \in \mathbb{Z}^{m \times m}$ is a matrix of rank m over $\mathbb{R}$ satisfying $AT \equiv \mathbf{0} \bmod q$, and $\max_{1 \leq i \leq m} \|\mathbf{t}_i\| \leq \beta$, where $\mathbf{t}_i$ denotes i-th column vector of T. The key generation algorithm also sets a collision resistant function $H : \{0,1\}^* \longrightarrow \mathbb{Z}_q^n$ and outputs public parameters $\mathsf{pp} = H$ and a pair of public key and private key $(\mathsf{pk} = A, \mathsf{sk} = T)$.

$\mathsf{Sign.GPV}(\mathsf{pp}, \mathsf{sk}, \mu \in \{0,1\}^*)$: On the given inputs pp, sk, and a message μ, the algorithm computes $\mathbf{y} = H(\mu) \in \mathbb{Z}_q^n$ and finds $\mathbf{c} \in \mathbb{Z}^m$ such that $A\mathbf{c} \equiv \mathbf{y} \bmod q$. The signing algorithm also samples $\mathbf{z} \longleftarrow D_{\mathscr{L}_{A^\perp}, \beta, -\mathbf{c}}$ satisfying $A\mathbf{z} \equiv \mathbf{0} \bmod q$ and $\|\mathbf{z} + \mathbf{c}\| \leq \sqrt{m}\beta$, using the short basis of $\mathscr{L}_{A^\perp}$ induced from $\mathsf{sk} = T$. The signing algorithm finally outputs $\mathsf{sig}_\mu = \mathbf{z} + \mathbf{c} \in \mathbb{Z}^m$ as a signature of the message μ.

Verify.GPV($\mathsf{pk}, \mathsf{pp}, \mu, \mathsf{sig}_\mu$): On the given inputs $\mathsf{pk}, \mathsf{pp}, \mu, \mathsf{sig}_\mu$, the algorithm outputs 1 (= valid) if and only if

$$\begin{aligned} \left\|\mathsf{sig}_\mu\right\| &\leq \sqrt{m}\beta \text{ and} \\ A \cdot \mathsf{sig}_\mu &\equiv H(\mu) \mod q. \end{aligned} \tag{5}$$

Strong Key Substitution Attack. We present a strong key substitution attacks on the GPV signature scheme.

Suppose that a valid signature $\mathsf{sig}_\mu \in \mathbb{Z}^m$ on a message $\mu \in \{0,1\}^*$ under the public key $\mathsf{pk} = A \in \mathbb{Z}_q^{n\times m}$ is given. One proceeds as follows to obtain a new public key pk' where sig_μ is a valid signature on the message μ under this new public key pk'.

(1) Compute a matrix $B \in \mathbb{Z}_q^{n\times m}$ such that $B \cdot \mathsf{sig}_\mu \equiv 0 \bmod q$ and the rank of the matrix $A + B$ is n.

(a) Let $\mathsf{sig}_\mu = (s_1, \ldots, s_m)^T$. In the construction of B, the vector $\{\mathbf{b}_2, \ldots, \mathbf{b}_m\}$ can be chosen arbitrarily such that $s_2\mathbf{b}_2 + \cdots + s_m\mathbf{b}_m \neq \mathbf{0}$. In particular, we select n column vectors of A which are linearly independent over $\mathbb{Z}_q$, namely, $\mathbf{a}_{i_1}, \ldots, \mathbf{a}_{i_n}$ (we may assume that $i_1 > 1$). And we set $\mathbf{b}_{i_j} = \mathbf{0}$ for $j = 1, \ldots, n$ and choose other $\mathbf{b}_i$'s so that $s_2\mathbf{b}_2 + \cdots + s_m\mathbf{b}_m \neq 0$. Then $A + B$ has n linearly independent column vectors over $\mathbb{Z}_q$, which means the rank$(A + B) = n$.

(2) Set $A' \equiv (A + B) \bmod q$.

(3) Output $\mathsf{pk}' = A'$ and sig_μ as a signature on μ under the public key pk'.

The validity of sig_μ as a signature on the message μ under the new public key pk' follows from the facts below:

(i) $\|\mathsf{sig}_\mu\| < \sqrt{m}\beta$ since sig_μ is a valid signature.

(ii) $A' \cdot \mathsf{sig}_\mu \equiv H(\mu) \bmod q$ since we have

$$A' \cdot \mathsf{sig}_\mu \equiv (A + B) \cdot \mathsf{sig}_\mu \equiv A \cdot \mathsf{sig}_\mu \equiv H(\mu) \mod q. \tag{6}$$

Weak Key Substitution Attack. We now present a weak key substitution attack on the GPV signature scheme. In the proposed attack, we assume that the signer acts as an attacker to undermine the nonrepudiation property of the signature scheme and so the attacker knows $\mathsf{sk} = T$.

Suppose that a valid signature $\mathsf{sig}_\mu \in \mathbb{Z}^m$ on a message $\mu \in \{0,1\}^*$ under the public key $\mathsf{pk} = A \in \mathbb{Z}_q^{n\times m}$ is given. The attacker proceeds as follows to obtain a new public key pk' and the corresponding private key sk' such that sig_μ is a valid signature on the message μ under this new public key pk'.

(1) Compute a matrix $M \in \mathbb{Z}_q^{n\times n}$ such that $H(\mu) \in \mathbb{Z}_q^n$ is an eigenvector of M with eigenvalue 1; that is, $M \cdot H(\mu) \equiv H(\mu) \bmod q$.

(a) M is chosen as an invertible matrix over $\mathbb{Z}_q$ with eigenvector $H(\mu)$ and eigenvalue 1 so that MA has rank n. More precisely, one can construct $M = (\delta_{i,j})$ as follows. We may assume that $H(\mu) = (h_1, \ldots, h_n)^t \neq 0$ and $h_1, h_2 \neq 0$. For any $\alpha \in \mathbb{Z}_q \setminus \{0,1\}$, we set the following.

$$\begin{aligned} &\delta_{1,1} = \alpha \\ &\delta_{1,2} = \beta = (1-\alpha)\, h_1 h_2^{-1} \mod q \\ &\delta_{i,i} = 1 \quad \text{for } i \in \{2, \ldots, n\} \\ &\delta_{i,j} = 0 \quad \text{for } (i,j) \notin \{(i,i) : i = 1, \ldots, n\} \cup \{(1,2)\} \end{aligned} \tag{7}$$

Then M is invertible, $M \cdot H(\mu) \equiv H(\mu) \bmod q$, and the rank of $MA (\neq A)$ is n.

(2) Set $A' \equiv M \cdot A \bmod q$.

(3) Output $\mathsf{pk}' = A'$ and sig_μ as a signature on the message μ under the public key pk', and output T as a private key of pk'.

Noting that the private key $\mathsf{sk} = T$ corresponding to the public key $\mathsf{pk} = A$ satisfies $A' \cdot T \equiv M \cdot A \cdot T \equiv \mathbf{0} \bmod q$, we know that T is also a private key of the new public key $\mathsf{pk}' = A'$. Thus, the attacker who knows sk also knows the private key sk' of pk'.

The validity of sig_μ as a signature on the message μ under the new public key pk' follows from the facts below:

(i) $\|\mathsf{sig}_\mu\| < \sqrt{m}\beta$ since sig_μ is a valid signature.

(ii) $A' \cdot \mathsf{sig}_\mu \equiv H(\mu) \bmod q$ since we have

$$A' \cdot \mathsf{sig}_\mu \equiv M \cdot A \cdot \mathsf{sig}_\mu \equiv M \cdot H(\mu) \equiv H(\mu) \mod q. \tag{8}$$

Therefore, the attacker, who was the original signer, has succeeded in a weak strong key substitution attack on the GPV signature scheme.

3.2. Attacks on Lyubashevsky's Signature Scheme

Description of Lyubashevsky's Signature Scheme. We describe Lyubashevsky's signature scheme based on SIS problem [8].

KeyGen.LYU(1^κ): On the given input 1^κ, the algorithm samples two matrices (A, S), where $A \in \mathbb{Z}_q^{n\times m}$ is a matrix of rank n and $S \in [-d, d]^{m\times k}$. The algorithm computes $T \in \mathbb{Z}_q^{n\times k}$ satisfying $T \equiv AS \bmod q$. The algorithm sets an integer γ such that $2^\gamma \binom{k}{\gamma} \geq 2^\kappa$ and sets $\eta \in \mathbb{R}$ so that $\Pr_{\mathbf{z}\leftarrow D_\sigma^m}[\|\mathbf{z}\| \leq \eta\sqrt{m}\sigma] \leq 1 - 2^\kappa$. The key generation algorithm also sets a hash function $H : \{0,1\}^* \longrightarrow \{\mathbf{v} : \mathbf{v} \in \{-1, 0, 1\}^k, \|\mathbf{v}\|_1 \leq \gamma\}$ and outputs public parameters $\mathsf{pp} = (A, H, B_2 := \eta\sigma\sqrt{m})$ and a pair of public key and private key ($\mathsf{pk} = T, \mathsf{sk} = S$).

$\mathsf{Sign.LYU}(\mathsf{pp}, \mathsf{sk}, \mu \in \{0,1\}^*)$: On the given inputs pp, sk, and a message μ, the algorithm samples an m-dimensional vector $\mathbf{y}$ from D_σ^m, then computes $\mathbf{c} = H(A\mathbf{y}, \mu)$, and finally obtains $\mathbf{z} \equiv S\mathbf{c} + \mathbf{y} \bmod q$ by applying the rejection sampling algorithm. The signature algorithm only outputs $(\mathbf{z}, \mathbf{c})$ as a signature with probability $\min\{\mathscr{D}_\sigma^m / M\mathscr{D}_{S\mathbf{c},\sigma}^m, 1\}$. If nothing is printed, run the algorithm again until some signature is outputted.

$\mathsf{Verify.LYU}(\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig} = (\mathbf{z}, \mathbf{c}))$: On the given inputs $\mathsf{pp}, \mathsf{sk}, \mu, \mathsf{sig}_\mu$, the algorithm outputs 1 if and only if

$$\begin{aligned} &\|\mathbf{z}\| \le B_2 \text{ and} \\ &\mathbf{c} = H\left(A\mathbf{z} - T\mathbf{c} \bmod q, \mu\right). \end{aligned} \tag{9}$$

Strong Key Substitution Attack. Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^k$ on a message $\mu \in \{0,1\}^*$ under the public key $\mathsf{pk} = T \in \mathbb{Z}_q^{n\times k}$ is given. One proceeds as follows to obtain a new public key pk' such that sig_μ is a valid signature on the message μ under the new public key pk'.

(1) Compute a matrix $B \in \mathbb{Z}_q^{n\times k}$ such that $B \cdot \mathbf{c} \equiv \mathbf{0} \bmod q$. It is easy to compute B in a similar way that is described in the strong key substitution attack on the GPV signature scheme.
(2) Set $T' \equiv (T + B) \bmod q$.
(3) Output $\mathsf{pk}' = T'$ and sig_μ as a signature on the message μ under the public key pk'.

The validity of $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^k$ as a signature on the message μ under the new public key pk' follows from the facts below:

(i) $\|\mathbf{z}\| \le \eta\sigma\sqrt{m}$ since $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ is a valid signature.
(ii) $H(A\mathbf{z} - T'\mathbf{c} \bmod q, \mu) = \mathbf{c}$ since we have

$$\begin{aligned} A\mathbf{z} - T'\mathbf{c} &\equiv A\mathbf{z} - (T + B)\,\mathbf{c} \equiv A\mathbf{z} - T\mathbf{c} \mod q, \\ \mathbf{c} &= H\left(A\mathbf{z} - T\mathbf{c} \bmod q, \mu\right). \end{aligned} \tag{10}$$

Weak Key Substitution Attack. We now present a weak key substitution attack on Lyubashevsky's signature scheme. Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^k$ on a message $\mu \in \{0,1\}^*$ under the public key $\mathsf{pk} = T \in \mathbb{Z}_q^{n\times k}$ is given. As we have commented before, the signer is an attacker and it is assumed that the attacker knows $\mathsf{sk} = S$ such that $AS \equiv T \bmod q$. The attacker proceeds as follows to obtain a new public key pk' such that sig_μ is a valid signature on the message μ under the new public key pk'.

(1) Compute a matrix $S' \in [-d, d]^{m\times k}$ satisfying $S' \cdot \mathbf{c} \equiv \mathbf{0} \bmod q$.

(i) With high probability, we may assume that $\mathbf{c} = (c_1, \ldots, c_k)^t \in \{-1, 0, 1\}^k$ has at least two nonzero components, say c_1 and c_2. Let $S = (\mathbf{s}_1, \ldots, \mathbf{s}_k)$ and $\mathbf{s}_j = (s_{1j}, \ldots, s_{mj})^t$ with $s_{ij} \in [-d, d]$. We also assume

$$(s_{11}, s_{12}) \notin \{(d,d), (-d,-d), (-d,d), (d,-d)\}, \tag{11}$$

which occurs with overwhelming probability. Let $\epsilon \in \{1, -1\}$ which will be determined later. We set $S' = (\mathbf{s}_1', \ldots, \mathbf{s}_k')$ as follows.

$$\begin{aligned} \mathbf{s}_1' &= (\epsilon c_2, 0, \ldots, 0)^t \\ \mathbf{s}_2' &= (-\epsilon c_1, 0, \ldots, 0)^t \\ \mathbf{s}_\ell' &= (0, \ldots, 0)^t \quad \text{for } \ell \ne 1, 2 \end{aligned} \tag{12}$$

Then, it satisfies that $S' \cdot \mathbf{c} \equiv \mathbf{s}_1' c_1 + \mathbf{s}_2' c_2 \equiv \mathbf{0} \bmod q$.

Let $S'' = S + S' \in [-d, d]^{m\times k}$. The only terms of S'' differing from S are $s_{11}'' = s_{11} + \epsilon c_2$ and $s_{12}'' = s_{12} - \epsilon c_1$. If $|s_{11}|, |s_{12}| < d$, then one can choose any $\epsilon \in \{-1, 1\}$. If $s_{11} = \pm d$ and $|s_{12}| < d$, then set ϵ so that $\epsilon c_2 = \mp 1$. If $s_{12} = \pm d$ and $|s_{11}| < d$, then set ϵ so that $\epsilon c_1 = \pm 1$.

(2) Set $T' \equiv (T + A \cdot S') \bmod q$.
(3) Output $\mathsf{pk}' = T'$ and sig_μ as a signature on μ under the public key pk'.

Note that $\mathsf{sk}' = S + S'$ is a valid private key corresponding to $\mathsf{pk}' = T'$ since $T' \equiv (T + A \cdot S') \equiv A \cdot (S + S') \bmod q$ and $S + S' \in [-d, d]^{m\times k}$. Therefore, the attacker, who knows $\mathsf{sk} = S$ such that $T \equiv AS \bmod q$ also knows the private key $\mathsf{sk}' = S + S'$ of pk'.

The validity of $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^k$ as a signature on the message μ under the new public key pk' follows from the facts below:

(i) $\|\mathbf{z}\| \le \eta\sigma\sqrt{m}$ since $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ is a valid signature.
(ii) $H(A\mathbf{z} - T'\mathbf{c} \bmod q, \mu) = \mathbf{c}$ since we have

$$\begin{aligned} A\mathbf{z} - T'\mathbf{c} &\equiv A\mathbf{z} - \left(T + A \cdot S'\right)\mathbf{c} \equiv A\mathbf{z} - T\mathbf{c} \mod q, \\ \mathbf{c} &= H\left(A\mathbf{z} - T\mathbf{c} \bmod q, \mu\right). \end{aligned} \tag{13}$$

Therefore, the attacker, who was the original signer, has succeeded in a weak key substitution attack on Lyubashevsky's signature scheme.

3.3. Attacks on BLISS Signature Scheme. BLISS [9] is possibly one of the most efficient lattice-based signature schemes. It has been implemented in both software and hardware and boasts implementation efficiency comparable to classical factoring and discrete-logarithm-based schemes. BLISS can be seen as a ring-based optimization of the earlier lattice-based scheme of Lyubashevsky, sharing the same "Fiat-Shamir with aborts" structure.

The security of the BLISS signature scheme is based on the hardness of the $\mathcal{R}$-$\mathbf{SIS}_{q,n,m,\beta}$ problem which is the ring variant of the SIS problem. We first describe the matrix version of BLISS signature scheme and then explain its ring version. For more detailed descriptions and definition of the $\mathcal{R}$-$\mathbf{SIS}_{q,n,m,\beta}$ problem, we refer to [9]. The scheme construction and proof work for matrix version are equally well for ring version, when instantiated with polynomials.

In this subsection, we will assume that q is a prime such that $q \equiv 1 \pmod{2n}$ and n is a power of 2. For any integer q, we define the quotient ring $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$ and $\mathcal{R}_{2q} = \mathbb{Z}_{2q}[x]/(x^n + 1)$.

Let $\mathbb{B} = \{0, 1\}$ and $\mathbb{T} = \{-1, 0, 1\}$ be the set of binary and ternary integers, respectively. We define $\mathbb{B}^n_\omega$ (resp., $\mathbb{T}^n_\omega$), the set of binary vectors (resp., ternary vectors) of length n and Hamming weight ω (i.e., vectors with exactly ω out of n nonzero entries). Depending on the context, we consider $\mathbb{B}^n_\omega$ and $\mathbb{T}^n_\omega$ as a subset of $\mathbb{Z}^n_{2q}$ or $\mathcal{R}_{2q}$ and regard bold lower case letters as vectors or polynomials. For every integer x in the range $[-q, q)$ and any positive integer d, x can be uniquely written $x = \lfloor x \rceil_d \cdot 2^d + [x \bmod 2^d]$, where $[x \bmod 2^d] \in [-2^{d-1}, 2^{d-1})$. For every integer vector $\mathbf{x} = (x_i)_{1 \le i \le n}$, $\lfloor \mathbf{x} \rceil_d$ denotes $(\lfloor x_i \rceil_d)_{1 \le i \le n}$. Let $\mathbf{v}_1 \mid \mathbf{v}_2$ denote the concatenation of two vectors $\mathbf{v}_1$ and $\mathbf{v}_2$.

3.3.1. Matrix Version of BLISS

Description of the Matrix Version of BLISS. We describe the key generation algorithm KeyGen.mBLISS, signature generation algorithm Sign.mBLISS, and verification algorithm Verify.mBLISS of the matrix version of the BLISS signature scheme.

KeyGen.mBLISS(1^κ): On the given input 1^κ, the algorithm outputs the key pair $(\mathsf{pk} = A, \mathsf{sk} = S)$ such that $S \in \mathbb{Z}^{m \times n}_{2q}$ has a small norm, $A \in \mathbb{Z}^{n \times m}_{2q}$, and $AS \equiv qI_n \bmod 2q$. The algorithm set $\eta \in \mathbb{R}$ so that $\Pr_{\mathbf{z} \leftarrow D^m_\sigma}[\|\mathbf{z}\| \le \eta\sqrt{m}\sigma] \le 1 - 2^\kappa$. Let H denote a hash function $H : \{0, 1\}^* \longrightarrow \mathbb{B}^n_\omega$. The algorithm also outputs public parameter $\mathsf{pp} = (H, \sigma, B_2 := \eta\sqrt{m}\sigma)$.

Sign.mBLISS($\mathsf{pp}, \mathsf{sk}, \mathsf{pk}, \mu \in \{0, 1\}^*$): On the given inputs pp, sk, pk, and a message μ, the algorithm computes a signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ of the message μ as follows:

(1) $\mathbf{y} \longleftarrow D^m_\sigma$.
(2) $\mathbf{c} \longleftarrow H(A\mathbf{y} \bmod 2q, \mu)$.
(3) Choose a random bit $b \in \{0, 1\}$.
(4) $\mathbf{z} \longleftarrow \mathbf{y} + (-1)^b S\mathbf{c}$.
(5) Output $(\mathbf{z}, \mathbf{c})$ with probability $1/(M \exp(-\|S\mathbf{c}\|^2/2\sigma^2)\cosh(\langle \mathbf{z}, S\mathbf{c}\rangle/\sigma^2))$; otherwise **restart**.

Verify.mBLISS($\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig}_\mu$): On the given inputs pp, pk, μ, and a signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$, the algorithm accepts or rejects the signature according to the following steps:

(1) If $\|\mathbf{z}\| > B_2$, then output 0.
(2) If $\|\mathbf{z}\|_\infty \ge q/4$, then output 0.
(3) Output 1 if and only if $\mathbf{c} = H(A\mathbf{z}+q\mathbf{c} \bmod 2q, \mu)$.

Note that the signer outputs the signature $(\mathbf{z}, \mathbf{c})$ where $\mathbf{z}$ is distributed according to D^m_σ. It can be seen from Lemma 7 by taking $g_v = (1/2)D^m_{\mathbf{Sc},\sigma} + (1/2)D^m_{-\mathbf{Sc},\sigma}$ and $f = D^m_\sigma$ where $v = \mathbf{Sc}$.

Strong Key Substitution Attack. We present a strong key substitution attack on the matrix version of BLISS signature scheme.

Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c}) \in \mathbb{Z}^m_{2q} \times \mathbb{Z}^m_{2q}$ on a message $\mu \in \{0, 1\}^*$ under the public key $\mathsf{pk} = A \in \mathbb{Z}^{n \times m}_{2q}$ is given. One proceeds as follows to obtain a new public key pk' such that the signature $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ is a valid signature on the message μ under the new public key pk'.

To succeed in strong key substitution attack, it is enough to find a new matrix $A' \in \mathbb{Z}^{n \times m}_{2q}$ such that $\mathbf{c} = H(A'\mathbf{z}+q\mathbf{c} \bmod 2q, \mu)$, which holds when $A'\mathbf{z} \equiv A\mathbf{z} \bmod 2q$. In the following we show how to find such a matrix A'.

(1) We may assume that there exists $j \in \{1, \ldots, m\}$ such that z_j is invertible modulo $2q$.

(2) Let $\mathbf{t} = (t_1, \ldots, t_n)^T = A\mathbf{z} \bmod 2q$ and $\mathbf{z} = (z_1, \ldots, z_m)^T$. For each $i \in \{1, \ldots, n\}$, choose $a'_{i,1}, \ldots, a'_{i,j-1}, a'_{i,j+1}, \ldots, a'_{i,m}$ uniformly at random from $\mathbb{Z}_{2q}$, and then compute $a'_{i,j} \equiv z_j^{-1}(t_i - \sum_{1 \le k \ne j \le m} a'_{i,k} z_k) \bmod 2q$.

(3) Defining a matrix $A' = (a'_{i,j}) \in \mathbb{Z}^{n \times m}_{2q}$, we have $A'\mathbf{z} \equiv \mathbf{t} \bmod 2q$ because of step (2).

(4) Output $\mathsf{pk}' = A'$ and $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ as a signature on the message μ under the public key pk'.

We note that the validity of $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ as a signature on the message μ under $\mathsf{pk}' = A'$ can be checked as follows:

(i) $\|\mathbf{z}\|_2 \le B_2$ and $\|\mathbf{z}\|_\infty < q/4$ since sig_μ is a valid signature.

(ii) The equation $A'\mathbf{z} + q\mathbf{c} \equiv A\mathbf{z} + q\mathbf{c} \bmod 2q$ implies that $\mathbf{c} = H(A\mathbf{z} + q\mathbf{c} \bmod 2q, \mu) = H(A'\mathbf{z} + q\mathbf{c} \bmod 2q, \mu)$.

The described attack succeeds unless there is no $j \in \{1, \ldots, m\}$ such that z_j is invertible in $\mathbb{Z}_{2q}$. Note that the signer outputs the signature $(\mathbf{z}, \mathbf{c})$ where $\mathbf{z}$ is distributed according to D^m_σ by Lemma 7. Therefore it is enough to estimate the success probability of our attack for $\mathbf{z} \longleftarrow D^m_\sigma$. Let $f(x) = e^{-x^2/(2\sigma^2)}$ and a be a positive real number. Since f is a nonincreasing function in $[0, \infty)$, $\sum_{x=0}^\infty f(x) \ge \int_0^\infty f(x)dx$ and $\sum_{x=1}^\infty f(ax) \le (1/a)\int_0^\infty f(x)dx$. We thus have $f(\mathbb{Z}) = \sum_{x \in \mathbb{Z}} f(x) \ge \int_{-\infty}^\infty f(x)dx - f(0) = \sqrt{2\pi}\sigma - 1$ and $f(a\mathbb{Z}) = \sum_{x \in \mathbb{Z}} f(ax) \le 1 + (1/a)\int_{-\infty}^\infty f(x)dx = 1 + \sqrt{2\pi}\sigma/a$. We also

note that $\Pr_{\mathbf{z}\longleftarrow D_\sigma^m}[\mathbf{z}=\mathbf{a}] = \prod_{1\le i\le m}\Pr_{z_i\longleftarrow D_\sigma^m}[z_i = a_i]$ for any $\mathbf{a}\in\mathbb{Z}^m$. Then

$$\begin{aligned}
&\Pr_{\mathbf{z}\longleftarrow D_\sigma^m}\left[z_j \text{ is non-invertible modulo } 2q\right]\\
&= \Pr_{z_j\longleftarrow D_\sigma}\left[z_j \text{ is non-invertible modulo } 2q\right]\\
&\le \frac{\left\{\sum_{z_j\equiv 0 \bmod 2}\rho_\sigma\left(z_j\right)+\sum_{z_j\equiv 0 \bmod q}\rho_\sigma\left(z_j\right)\right\}}{\sum_{z_j\in\mathbb{Z}}\rho_\sigma\left(z_j\right)} \qquad (14)\\
&= \frac{\rho_\sigma(2\mathbb{Z})+\rho_\sigma(q\mathbb{Z})}{\rho_\sigma(\mathbb{Z})} \le \frac{1}{2}+\frac{1}{q}+\epsilon,
\end{aligned}$$

where $\epsilon = (5q+2)/2q(\sqrt{2\pi}\sigma-1) < 0.013$ for parameters proposed in BLISS ($\sigma\ge 100$). This implies that the probability that all of $z_1,\ldots,z_m$ are noninvertible modulo $2q$ is at most $(1/2+1/q+\epsilon)^m$. Thus, the success probability of our attack is at least $1-(1/2+1/q+\epsilon)^m$ which is very high.

Weak Key Substitution Attack. We now present a weak key substitution attack on the matrix version of BLISS signature scheme.

Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z},\mathbf{c}) \in \mathbb{Z}_{2q}^m \times \mathbb{Z}_{2q}^m$ on a message $\mu\in\{0,1\}^*$ under the public key $\mathsf{pk} = A \in \mathbb{Z}_{2q}^{n\times m}$ is given. The signer, who owns $\mathsf{pk} = A$ and $\mathsf{sk} = S$ such that $AS \equiv qI_n \bmod 2q$, proceeds as follows to obtain a new public key $\mathsf{pk}' = A'$ and the corresponding private key $\mathsf{sk}' = S'$ such that the signature $\mathsf{sig}_\mu = (\mathbf{z},\mathbf{c})$ is a valid signature on the message μ under the new public key pk'. To succeed in weak key substitution attack, it is sufficient to find matrices A' and S' such that $A'\mathbf{z}\equiv A\mathbf{z} \bmod 2q$ and $A'S'\equiv qI_n \bmod 2q$. In the following we show how to find such matrices A' and S'.

(1) Compute a matrix $M\in\mathbb{Z}_{2q}^{n\times n}$ such that $M\equiv I_n \bmod 2$ and $MA\mathbf{z}\equiv A\mathbf{z} \bmod q$, which imply that $MA\mathbf{z}\equiv A\mathbf{z} \bmod 2q$.

(a) Computing such a matrix, M is easy if $A\mathbf{z}\not\equiv 0 \bmod q$. We first compute a matrix $Y\in\mathbb{Z}_q^{n\times n}$ such that $Y\cdot A\mathbf{z}\equiv 0 \bmod q$. We then set $M = 2Y + I_n \bmod 2q$. It is clear to see that $M\equiv I_n \bmod 2$ and $MA\mathbf{z}\equiv A\mathbf{z} \bmod q$.

(2) We set $\mathsf{pk}' = A' = MA \bmod 2q$.

Since $\mathsf{pk} = A$ and $\mathsf{sk} = S$ satisfy $AS\equiv qI_n \bmod 2q$, we have $AS\equiv 0 \bmod q$ and $AS\equiv I_n \bmod 2$. From the construction of M, we also have $MAS\equiv 0 \bmod q$ and $MAS\equiv I_n \bmod 2$, which imply $A'S\equiv qI_n \bmod 2q$. Thus, the signer obtains a valid key pair $\mathsf{pk}' = A'$ and $\mathsf{sk}' = S$.

The validity of $\mathsf{sig}_\mu = (\mathbf{z},\mathbf{c})$ as a signature on the message μ under the public key $\mathsf{pk}' = A'$ can be checked as follows:

(i) $\|\mathbf{z}\|_2 \le B_2$ and $\|\mathbf{z}\|_\infty \le q/4$ since sig_μ is a valid signature.

(ii) $\mathbf{c} = H(A'\mathbf{z} + q\mathbf{c} \bmod 2q, \mu)$ from the following equations:

$$\begin{aligned}
&\mathbf{c} = H\left(A\mathbf{z} + q\mathbf{c} \bmod 2q, \mu\right) \text{ and}\\
&A\mathbf{z}\equiv MA\mathbf{z}\equiv A'\mathbf{z} \bmod 2q.
\end{aligned} \qquad (15)$$

Therefore, the signer of the signature $\mathsf{sig}_\mu = (\mathbf{z},\mathbf{c})$ succeeds in a weak key substitution attack on the matrix version of BLISS signature scheme.

3.3.2. Ring Version of BLISS

Description of the Ring Version of BLISS. We describe the key generation algorithm KeyGen.BLISS, signature generation algorithm Sign.BLISS, and verification algorithm Verify.BLISS of the ring version of the BLISS signature scheme. Let us define $p = \lfloor 2q/2^d\rfloor$ where d is the number of dropped bits, and ζ such that $\zeta\cdot(q-2)\equiv 1 \bmod 2q$.

The notation $f(x)\longleftarrow D_\sigma^n$ means that $f(x) = \sum_{0\le i<n} f_i x^i$ and $(f_0,\ldots,f_{n-1})$ are sampled from the distribution D_σ^n.

For $S = (\mathbf{s}_1,\mathbf{s}_2)^T \in \mathscr{R}_{2q}$ and an integer $\tau\le n$, define

$$N_\tau(S) = \max_{\substack{I\subset\{1,\ldots,n\}\\ \#I=\tau}}\sum_{i\in I}\left(\max_{\substack{J\subset\{1,\ldots,n\}\\ \#J=\tau}}\sum_{j\in J}T_{i,j}\right), \qquad (16)$$

where $T = (T_{i,j}) = \widehat{S}^T\widehat{S}\in\mathbb{R}^{n\times n}$ and $\widehat{S} = (\widehat{S}_1,\widehat{S}_2)^T$ is a matrix in $\mathbb{R}^{2n\times n}$ such that j-th column of $\widehat{S}_i\in\mathbb{R}^{n\times n}$ is the coefficient vector of polynomial $\mathbf{s}_i x^{j-1} \bmod x^n+1$ for $i=1,2$ and $j=1,\ldots,n$.

KeyGen.BLISS(1^κ): On the given input 1^κ, the algorithm outputs the key pair ($\mathsf{pk} = A, \mathsf{sk} = S$) generated as follows. We note that a key pair (A,S) satisfies $AS\equiv q \bmod 2q$. The algorithm sets $\eta\in\mathbb{R}$ so that $\Pr_{\mathbf{z}\longleftarrow D_\sigma^{2n}}[\|\mathbf{z}\|\le\eta\sqrt{2n}\sigma]\le 1-2^{-\kappa}$. The algorithm also sets a positive integer $\tau\le n$ and a constant C so that 25% of the keys are accepted. Let H denote a hash function $H:\{0,1\}^*\longrightarrow\mathbb{B}_\omega^n$. The algorithm also outputs public parameter $\mathsf{pp} = (H,\sigma,B_2 := \eta\sqrt{n}\sigma, B_\infty)$ where $2B_\infty + (2^d+1) < q/2$.

(1) Choose $\mathbf{f},\mathbf{g}$ as uniform polynomials of degree less than n with exactly $d_1 = \lceil\delta_1 n\rceil$ entries in $\{\pm 1\}$, $d_2 = \lceil\delta_2 n\rceil$ entries in $\{\pm 2\}$, and other entries in $\{0\}$ where $0\le\delta_1<1$ and $0\le\delta_2<1$ are given densities.

(2) $S = (\mathbf{s}_1,\mathbf{s}_2)^T \longleftarrow (\mathbf{f}, 2\mathbf{g}+1)^T$.

(3) If $N_\tau(S)\ge C^2\cdot 5\cdot(\lceil\delta_1 n\rceil + 4\lceil\delta_2 n\rceil)\cdot\tau$, then **restart**.

(4) $\mathbf{a}_q \longleftarrow (2\mathbf{g}+1)/\mathbf{f} \bmod q$ (**restart** if $\mathbf{f}$ is not invertible).

(5) $A = (\mathbf{a}_1, q-2)\longleftarrow(2\mathbf{a}_q, q-2) \bmod 2q$.

Sign.BLISS($\mathsf{pp},\mathsf{sk},\mathsf{pk},\mu\in\{0,1\}^*$): On the given inputs pp, sk, pk, and a message μ, the algorithm computes a signature $\mathsf{sig}_\mu = (\mathbf{z}_1,\mathbf{z}_2^\dagger,\mathbf{c})$ of the message μ as follows:

(1) $\mathbf{y}_1, \mathbf{y}_2 \longleftarrow D_\sigma^n$.
(2) $\mathbf{u} \longleftarrow \zeta \cdot \mathbf{a}_1 \cdot \mathbf{y}_1 + \mathbf{y}_2 \bmod 2q$.
(3) $\mathbf{c} \longleftarrow H(\lfloor \mathbf{u} \rceil_d \bmod p, \mu)$.
(4) Choose a random bit b.
(5) $\mathbf{z}_1 \longleftarrow \mathbf{y}_1 + (-1)^b \mathbf{s}_1 \mathbf{c}$.
(6) $\mathbf{z}_2 \longleftarrow \mathbf{y}_2 + (-1)^b \mathbf{s}_2 \mathbf{c}$.
(7) **Continue** with probability $1/(M \exp(-\|S\mathbf{c}\|^2/2\sigma^2) \cosh(\langle \mathbf{z}, S\mathbf{c} \rangle / \sigma^2))$; otherwise **restart**.
(8) $\mathbf{z}_2^\dagger \longleftarrow (\lfloor \mathbf{u} \rceil_d - \lfloor \mathbf{u} - \mathbf{z}_2 \rceil_d) \bmod p$.
(9) **Output** $(\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$.

Verify.BLISS$(\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig}_\mu)$: On the given inputs $\mathsf{pp}, \mathsf{pk}, \mu, \mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$, the algorithm accepts or rejects the signature according to the following steps:

(1) $\mathbf{z} \longleftarrow \mathbf{z}_1 \mid (2^d \cdot \mathbf{z}_2^\dagger)$.
(2) If $\|\mathbf{z}\|_2 > B_2$, then output 0.
(3) If $\|\mathbf{z}\|_\infty > B_\infty$, then output 0.
(4) Output 1 if and only if $\mathbf{c} = H(\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu)$.

As in the matrix version of BLISS, the signer outputs the signature $(\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ where $\mathbf{z}_1$ is sampled from D_σ^n by Lemma 7.

Strong Key Substitution Attack. Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c}) \in \mathcal{R}_{2q} \times \mathcal{R}_{2q} \times \mathcal{R}_{2q}$ on a message $\mu \in \{0,1\}^*$ under the public key $A = (\mathbf{a}_1, q-2) \in \mathcal{R}_{2q} \times \mathcal{R}_{2q}$ is given. One proceeds as follows to obtain a new public key pk' where the signature sig_μ is a valid signature on the message μ under the new public key pk'.

Since we want to find $A' = (\mathbf{a}_1', q-2)$ satisfying the equation

$$H\left(\lfloor \zeta \cdot \mathbf{a}_1' \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu\right) = H\left(\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu\right), \tag{17}$$

where $\zeta(q-2) \equiv 1 \bmod 2q$, it suffices to find $\mathbf{a}_1' \in \mathcal{R}_{2q}$ such that $\mathbf{a}_1'\mathbf{z}_1 \equiv \mathbf{a}_1\mathbf{z}_1 \bmod 2q$. To find such a polynomial $\mathbf{a}_1'$, we consider the greatest common divisor of two polynomials $\mathbf{z}_1$ and $x^n + 1$. Let $\mathbf{g}_q(x)$ be the gcd of $\mathbf{z}_1$ and $x^n + 1$ modulo q, and let $\mathbf{g}_2(x)$ be the gcd of $\mathbf{z}_1$ and $x^n + 1$ modulo 2. Since $q \equiv 1 \bmod 2n$, the polynomial $x^n + 1$ is completely factorized as a product of distinct linear polynomials modulo q; that is, $x^n + 1 \equiv \prod_{i=1}^n (x - \alpha_i) \bmod q, \alpha_i \in \mathbb{Z}_q$. Since n is a power of two, we also have $x^n + 1 \equiv (x+1)^n \bmod 2$.

Case 1. If $\mathbf{g}_q(x) \neq 1$, there exists $i \in \{1, \ldots, n\}$ such that $\mathbf{z}_1 \equiv (x - \alpha_i)\check{\mathbf{z}}_1 \bmod q$ for some $\check{\mathbf{z}}_1 \in \mathcal{R}_q$. We set $\mathbf{h}(x) \equiv (x^n + 1)/(x - \alpha_i) \bmod q$ and define $\mathbf{a}_1' \equiv \mathbf{a}_1 + 2\mathbf{h} \bmod (2q, x^n + 1)$. In this case, we output $A' = (\mathbf{a}_1', q-2)$ as a new public key pk' and $\mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ as a signature on the message μ under the public key pk'.

Case 2. If $\mathbf{g}_2(x) \neq 1$, we set $\mathbf{h}(x) \equiv (x^n + 1)/(x + 1) \equiv (x + 1)^{n-1} \bmod 2$ and define $\mathbf{a}_1' \equiv \mathbf{a}_1 + q\mathbf{h} \bmod (2q, x^n + 1)$. In this case, we output $A' = (\mathbf{a}_1', q-2)$ as a new public key pk' and $\mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ as a signature on the message μ under the public key pk'.

In both cases, the validity of $\mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ as a signature on the message μ under the public key pk' can be checked as follows:

(i) $\|\mathbf{z}_1 \mid (2^d \cdot \mathbf{z}_2^\dagger)\| \leq B_2$ and $\|\mathbf{z}_1 \mid (2^d \cdot \mathbf{z}_2^\dagger)\|_\infty \leq B_\infty$ since sig_μ is a valid signature.

(ii) In both cases $\mathbf{g}_q \neq 1$ and $\mathbf{g}_2 \neq 1$, we have $\mathbf{a}_1\mathbf{z}_1 \equiv \mathbf{a}_1'\mathbf{z}_1 \bmod (2q, x^n + 1)$, which implies

$$\left\lfloor \zeta \cdot \mathbf{a}_1' \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \right\rceil_d + \mathbf{z}_2^\dagger \bmod p = \left\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \right\rceil_d + \mathbf{z}_2^\dagger \bmod p. \tag{18}$$

Thus, we have $\mathbf{c} = H(\lfloor \zeta \cdot \mathbf{a}_1' \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu)$.

As described, our attack succeeds when $\mathbf{z}_1$ is noninvertible in $\mathcal{R}_2$ or $\mathbf{z}_1$ is noninvertible in $\mathcal{R}_q$. Note that the signer outputs the signature $(\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ where $\mathbf{z}_1$ is distributed according to D_σ^n by Lemma 7. Therefore it is enough to estimate the success probability of our attack for $\mathbf{z}_1 \longleftarrow D_\sigma^n$. To compute success probability of our attack, we first consider the case that $\mathbf{z}_1$ is noninvertible in $\mathcal{R}_2$. Recall that, by Lemma 2, if $\sigma \geq \eta_\epsilon(2\mathbb{Z}^n)$, the distribution of $(D_\sigma^n \bmod 2\mathbb{Z}^n)$ is within statistical distance at most 2ϵ of uniform over $(\mathbb{Z}^n \bmod 2\mathbb{Z}^n)$. Noting that $(2\mathbb{Z}^n)^* = (1/2)\mathbb{Z}^n$ and $\lambda_1^\infty((2\mathbb{Z}^n)^*) = 1/2$, by Lemma 3, we have

$$\eta_\epsilon(2\mathbb{Z}^n) \leq \frac{1}{\lambda_1^\infty((2\mathbb{Z}^n)^*)} \sqrt{\frac{\ln(2n/(1+1/\epsilon))}{\pi}} = 2\sqrt{\frac{\ln(2n/(1+1/\epsilon))}{\pi}}. \tag{19}$$

Therefore, if $\sigma \geq 2\sqrt{\ln(2n/(1+1/\epsilon))/\pi}$, then the distribution of $(D_\sigma^n \bmod 2\mathbb{Z}^n)$ is uniform over $\mathbb{Z}^n/2\mathbb{Z}^n \cong \mathbb{Z}_2^n$ within statistical distance at most 2ϵ. Hence, for $\mathbf{z}_1(x) \longleftarrow D_\sigma^n$, the probability that $\mathbf{z}_1(x)$ is not invertible in $\mathcal{R}_2$ is greater than or equal to $1/2 - 2\epsilon$. This is summarized in the following theorem.

Theorem 14. *If* $\sigma \geq 2\sqrt{\ln(2n/(1+1/\epsilon))/\pi}$,

$$\Pr_{f(x) \longleftarrow D_\sigma^n}\left[f(x) \text{ is non-invertible in } \mathcal{R}_2\right] \geq \frac{1}{2} - 2\epsilon. \tag{20}$$

Taking $\epsilon = 2^{-n}$, we have $\eta_\epsilon(2\mathbb{Z}^n) < 2\sqrt{\ln(n)}$. For the proposed parameter sets for BLISS, we have $\sigma \geq 100$ and $n \geq 256$, which imply $\sigma \geq 2\sqrt{\ln(n)} \geq \eta_\epsilon(2\mathbb{Z}^n)$. Thus, the probability that $\mathbf{z}_1(x)$ is noninvertible in $\mathcal{R}_2$ is greater than or equal to $1/2 - 2^{-n+1}$.

We now consider the case that $\mathbf{z}_1(x)$ is noninvertible in $\mathcal{R}_q$. Before continuing we first show that the following theorem holds. Note that this is essentially from [13, Lemma 11].

Theorem 15. *Let $n \geq 8$ be a power of 2 such that $\Phi(x) = x^n + 1$ splits into n linear factors modulo prime $q \geq 5$ as $\Phi(x) \equiv \prod_{i=1}^{n}(x - \alpha_i) \bmod q, \alpha_i \in \mathbb{Z}_q$. Let $\epsilon \in (0, 1/2)$ be an arbitrary real number. For $i \neq j \in \{1, \ldots, n\}$, we have the following.*

(i) *If $\sigma \geq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{1/n}$,*

$$\Pr_{f(x) \longleftarrow D_\sigma^n}\left[f(\alpha_i) \equiv 0 \bmod q\right] \geq \frac{1}{q} - 2\epsilon. \tag{21}$$

(ii) *If $\sigma \geq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{2/n}$,*

$$\Pr_{f(x) \longleftarrow D_\sigma^n}\left[f(\alpha_i) \equiv 0 \bmod q \wedge f(\alpha_j) \equiv 0 \bmod q\right] \leq \frac{1}{q^2} + 2\epsilon. \tag{22}$$

Proof. Let $I = \langle q, x - \alpha_i \rangle$ be an ideal of $\mathcal{R} = \mathbb{Z}[x]/\Phi(x)$. From $\mathcal{R}/I \equiv \mathbb{Z}_q[x]/(x - \alpha_i) \equiv \mathbb{Z}_q$, we have $\mathcal{N}(I) = q$ and so $\lambda_1(I) \leq \sqrt{n} q^{1/n}$ by Minkowski's theorem. Since I is an ideal of $\mathcal{R}$, we have $\lambda_n(I) = \lambda_1(I)$, and Lemma 4 gives $\eta_\epsilon(I) \leq \sqrt{\ln(2n(1 + 1/\epsilon))/\pi} \cdot \lambda_n(I) \leq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{1/n}$. Thus, if $\sigma \geq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{1/n}$, by Lemma 2, $(f \bmod I)$ is within statistical distance $\leq 2\epsilon$ to the uniform distribution on $\mathcal{R}/I$. As a result, we have $\Pr_{f(x) \longleftarrow D_\sigma^n}[f(x) \equiv 0 \bmod I] = \Pr_{f(x) \longleftarrow D_\sigma^n}[f(\alpha_i) \equiv 0 \bmod q] \geq 1/q - 2\epsilon$.

Let $J = \langle q, (x - \alpha_i)(x - \alpha_j) \rangle$ be an ideal of $\mathcal{R}$. We then have $\mathcal{N}(J) = q^2$ and $\lambda_1(J) \leq \sqrt{n} q^{2/n}$, because $\mathcal{R}/J \cong \mathbb{Z}_q[x]/(x - \alpha_i)(x - \alpha_j)$. Lemmas 4 and 2 then show that $(f \bmod J)$ is within statistical distance $\leq 2\epsilon$ to the uniform distribution on $\mathcal{R}/J$ when $\sigma \geq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{2/n}$. On the other hand, since $f(x) \equiv Ax + B \bmod J$ for $A = (\alpha_i - \alpha_j)^{-1}(f(\alpha_i) - f(\alpha_j)) \bmod q$, $B = f(\alpha_i) - A\alpha_i \bmod q$, $f(x) \equiv 0 \bmod J$ is equivalent to $f(\alpha_i) \equiv 0 \bmod q$ and $f(\alpha_j) \equiv 0 \bmod q$. Thus, by combining these results, we have $\Pr_{f(x) \longleftarrow D_\sigma^n}[f(x) \equiv 0 \bmod J] = \Pr_{f(x) \longleftarrow D_\sigma^n}[f(\alpha_i) \equiv 0 \bmod q \wedge f(\alpha_j) \equiv 0 \bmod q] \leq 1/q^2 + 2\epsilon$. □

If $\sigma \geq \sqrt{n \ln(2n(1 + 1/\epsilon))/\pi} \cdot q^{2/n}$, we have

$$\begin{aligned}
&\Pr_{\mathbf{z}_1(x) \longleftarrow D_\sigma^n}\left[\mathbf{z}_1 \text{ is non-invertible in } \mathcal{R}_q\right] \\
&= \Pr_{\mathbf{z}_1(x) \longleftarrow D_\sigma^n}\left[\bigvee_{1 \leq i \leq n} \mathbf{z}_1(\alpha_i) \equiv 0 \bmod q\right] \\
&\geq \sum_{1 \leq i \leq n} \Pr_{\mathbf{z}_1(x) \longleftarrow D_\sigma^n}\left[\mathbf{z}_1(\alpha_i) \equiv 0 \bmod q\right] \\
&\quad - \sum_{1 \leq i \neq j \leq n} \Pr_{\mathbf{z}_1(x) \longleftarrow D_\sigma^n}\left[\mathbf{z}_1(\alpha_i) \equiv 0 \bmod q \wedge \mathbf{z}_1(\alpha_j)\right. \\
&\quad \left.\equiv 0 \bmod q\right] \geq n\left(\frac{1}{q} - 2\epsilon\right) - \binom{n}{2}\left(\frac{1}{q^2} + 2\epsilon\right) = \frac{n}{q} \\
&\quad - \frac{n(n-1)}{2q^2} - n(n+1)\epsilon.
\end{aligned} \tag{23}$$

Taking $\epsilon = q^{-3}$, if $\sigma \geq \sqrt{n \ln(2n(1 + q^3))/\pi} \cdot q^{2/n}$, the probability that $\mathbf{z}_1 \longleftarrow D_{\mathbb{Z}^n,\sigma}$ is noninvertible in $\mathcal{R}_q$ is at least $n/q - n(n-1)/2q^2 - n(n+1)/q^3$, which is nonnegligible in n since in general q is polynomial in n. For the proposed parameter sets of BLISS having at least 128-bit security, we have $n = 512$ and $q = 12289$ and $\sigma > 100$ always satisfies $\sigma \geq \sqrt{n \ln(2n(1 + q^3))/\pi} \cdot q^{2/n}$; thus the success probability is at least 0.04.

Weak Key Substitution Attack. We present a weak key substitution attack on the ring version of the BLISS signature scheme. In this case, our attack is successful only in a very limited case.

Suppose that a valid signature $\mathsf{sig}_\mu = (\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$ on a message $\mu \in \{0,1\}^*$ under the public key $\mathsf{pk} = (\mathbf{a}_1, q - 2)$ is given. In weak key substitution attacks the signer who owns the key pair $\mathsf{pk} = (\mathbf{a}_1, q-2), \mathsf{sk} = (\mathbf{f}, 2\mathbf{g}+1)^T$ wants to obtain a new public key $\mathsf{pk}' = (\mathbf{a}_1', q-2)$ and the corresponding private key $\mathsf{sk}' = (\mathbf{s}_1', \mathbf{s}_2')^T$ so that the signature sig_μ is a valid signature on the message μ under the new public key pk'.

Similar to the strong key substitution attack on BLISS, it suffices to find $\mathbf{a}_1' \in \mathcal{R}_{2q}$ and $(\mathbf{f}', 2\mathbf{g}' + 1)$ such that $\mathbf{a}_1'\mathbf{z}_1 \equiv \mathbf{a}_1\mathbf{z}_1 \bmod 2q$ and $\mathbf{a}_1' \equiv (2\mathbf{g}' + 1)/\mathbf{f}' \bmod q$. In the following we show how to find such polynomials.

(1) Compute a polynomial $\mathbf{b} \in \mathcal{R}_{2q}$ such that $\mathbf{b}\mathbf{z}_1 = \mathbf{0}$ in $\mathcal{R}_{2q}$ by using a similar method in the strong key substitution attack. This implies that $(2\mathbf{b}/\mathbf{f})\mathbf{z}_1 = \mathbf{0}$ in $\mathcal{R}_{2q}$.

(2) We set $\mathbf{a}_q' = \mathbf{a}_q + (2\mathbf{b})/\mathbf{f}$ in $\mathcal{R}_{2q}$.

Since $\mathbf{a}_q \equiv (2\mathbf{g}+1)/\mathbf{f} \bmod q$, we have $\mathbf{a}_q' \equiv (2(\mathbf{g}+\mathbf{b})+1)/\mathbf{f} \bmod q$. However, we cannot guarantee that $\mathbf{g}' = (\mathbf{g} + \mathbf{b})$ is small enough. Therefore, the signer obtains a valid key pair $\mathsf{pk}' = (\mathbf{a}_1', q-2) = (2\mathbf{a}_q', q-2)$ and $\mathsf{sk}' = (\mathbf{f}', 2\mathbf{g}' + 1)$ only if one can make $\mathbf{g}'$ small. One way to get a smaller $\mathbf{g}'$ is to apply a lattice reduction algorithm on the ideal lattice generated by $\mathbf{b}$ mod q. However, it does not guarantee that $\mathbf{g}'$ is small enough to be a valid private key.

The validity of $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ as a signature on the message μ under $\mathsf{pk}' = A'$ can be checked as follows:

(i) $\|\mathbf{z}\|_2 \leq B_2$ and $\|\mathbf{z}\|_\infty \leq B_\infty$ since sig_μ is a valid signature.

(ii) $\mathbf{c} = H(\lfloor \zeta \cdot \mathbf{a}_1' \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu)$ from the following equalities: $\mathbf{c} = H(\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu)$ and $\mathbf{a}_1 \cdot \mathbf{z}_1 \equiv \mathbf{a}_1' \cdot \mathbf{z}_1 \bmod 2q$.

Therefore, the signer of $\mathsf{sig}_\mu = (\mathbf{z}, \mathbf{c})$ succeeds in a weak key substitution attack on BLISS of ring version as long as $\mathbf{g}'$ is small enough for a valid private key.

4. Attack Possibility and Its Defense

4.1. Possibility of Key Substitution Attacks. In general, there are two ways for the certificate authority to register a new user as the owner of a public key. One is that the certificate authority (CA) requires users to prove possession of user's private key before issuing certificates using zero-knowledge proof. The other is that CA only checks whether the public key is different from any previously issued one.

Clearly, if CA only checks freshness of public keys to issue certificates, by our strong key substitution attacks, GPV signature scheme, Lyubashevsky's signature scheme, and BLISS do not provide the nonrepudiation property.

Thus, a simple and natural way to prevent strong key substitution attack is to require that CA issues certificate only after checking the possession of private key using zero-knowledge proofs. The problem with this solution is that all known approaches for lattice-based zero-knowledge proofs are not practical. The first zero-knowledge proofs in the lattice setting were introduced by Kawachi et al. and Ling et al. [17, 18]. If one would like to have 128 bits of quantum security, one of the most basic application[19] requires 400KB of total proof size and more complicated applications need more megabytes. Baum and Lyubashevsky [20] give a new approach for constructing amortized zero-knowledge proofs of knowledge of short solutions over polynomial rings. When the number of relations is as small as the security parameter, their proof is practical. However, as the number of samples increases, the protocol has the same efficiency as the previous works. Still, it seems that more researches on the lattice-based zero-knowledge proofs need to be done to design efficient lattice-based authentication systems.

Even if CA issues certificates using zero-knowledge proof, in order to provide the nonrepudiation property, it requires that the underlying signature scheme be secure under the weak key substitution attack since any malicious signer can be a successful weak key substitution attacker and repudiates his/her valid signature in the system. Our weak key substitution attacks on GPV signature scheme, Lyubashevsky's signature scheme, and BLISS show that these schemes cannot provide nonrepudiation of the signatures.

4.2. How to Prevent Key Substitution Attacks. Another way to prevent key substitution attack is to modify signature schemes to resist this attack. Menezes and Smart [5] took such an approach and suggested a method, we call it MS conversion, that converts a signature scheme Σ into a new signature scheme MS-Σ by prepend the signer's public key to the message in some unambiguous way prior to signing (for example, a field of fixed length may be reserved for the public key). By using formatted messages specific to each public key, the goal of the key substitution attack against Σ is converted to compute $(\mathsf{pk}', \mathsf{pk}' \parallel \mu, \mathsf{sig})$ from a valid triple $(\mathsf{pk}, \mathsf{pk} \parallel \mu, \mathsf{sig})$, which was regarded as meaningless by Menezes and Smart [5] since it belongs to message key substitution (MKS) attacks against MS-Σ.

However, we note that MS conversion is not enough to guarantee the original meaning of KS security without considering MKS security. The specific MKS attack of computing $(\mathsf{pk}', \mathsf{pk}' \parallel \mu, \mathsf{sig})$ indicates that anyone can use it to claim that the signature sig on the message μ is signed by the user with the public key pk', which is exactly the goal of key substitution attack. Therefore, it is important to check the infeasibility of computing $(\mathsf{pk}', \mathsf{pk}' \parallel \mu, \mathsf{sig})$ from a valid triple $(\mathsf{pk}, \mathsf{pk} \parallel \mu, \mathsf{sig})$ in the MS conversions to guarantee the security against key substitution attacks. Form our analysis, it is straightforward to prove that MS-Lyubashevsky's signature scheme and MS-BLISS signature scheme are secure against key substitution attacks if the hash function H is collision resistant.

Unlike these Fiat-Shamir type signature schemes as Lyubashevsky's signature scheme and BLISS, we see that the collision resistance of the hash function H is not enough for the MKS security of MS-GPV signature scheme. The MKS security of MS-GPV scheme introduces the following new problem: given a $(A, \mathsf{sig}_\mu, \mu)$ such that $A \cdot \mathsf{sig}_\mu \equiv H(A \parallel \mu) \bmod q$, compute a new A' satisfying $A' \cdot \mathsf{sig}_\mu \equiv H(A' \parallel \mu) \bmod q$. One can solve this new problem as follows: for a given $(A, \mathsf{sig}_\mu, \mu)$,

Step 1. Compute $\mathcal{Y} = \{Y \in \mathbb{Z}_q^{n\times m} \mid Y\mathsf{sig}_\mu = \mathbf{0} \bmod q\}$.

Step 2. Compute $X_Y \in \mathbb{Z}_q^{n\times n}$ and $Y \in \mathcal{Y}$ such that

$$H\left(\left(X_Y \cdot Y \bmod q\right) \parallel \mu\right) = \mathbf{0}. \tag{24}$$

Step 3. Output $A' = X_Y \cdot Y \bmod q$.

It is clear to see that $A' \cdot \mathsf{sig}_\mu \equiv H(A' \parallel \mu) \bmod q$. The hardness of this new problem has not been studied for the parameters of the GPV signature. It seems somewhat heuristic, but it needs more research to assess the hardness of the problem and we expect that it is easier than the classical computational problems such as the collision resistance of a hash function or SIS problem.

Table 1 summarizes the results of our key substitution attacks on three signature schemes and MS conversion.

5. Conclusion

In this paper, we present strong/weak key substitution attacks on GPV signature scheme, Lyubashevsky's signature scheme, and BLISS. These attacks draw concerns in practice since they make the digital signature scheme to disable the functionalities of nonrepudiation and authentication. And we suggest using the MS conversion [5] which binds the signer's public key and the message being signed on Lyubashevsky's signature scheme and BLISS. Also, we point out that it is necessary to prove the security against *message and key substitution* (MKS) attacks for the MS conversion of digital signature in order to guarantee the security against key substitution attacks.

Table 1: Key substitution attacks (KSA) on signature schemes based on SIS problem.

Scheme	Target equation for KSA	Result
GPV [7]	$A \cdot \mathsf{sig}_\mu \equiv H(\mu) \bmod q$	insecure
Lyubashevsky [8]	$\mathbf{c} = H(A\mathbf{z} - T\mathbf{c} \bmod q, \mu)$	insecure
matrix-BLISS [9]	$\mathbf{c} = H(A\mathbf{z} + q\mathbf{c} \bmod 2q, \mu)$	insecure
ring-BLISS [9]	$\mathbf{c} = H(\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{z}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, \mu)$	insecure‡
MS-GPV	$A \cdot \mathsf{sig}_\mu \equiv H(A \parallel \mu) \bmod q$	unknown
MS-Lyubashevsky	$\mathbf{c} = (A\mathbf{z} - T\mathbf{c} \bmod q, T \parallel \mu)$	secure
MS-matrix-BLISS	$\mathbf{c} = H(A\mathbf{z} + q\mathbf{c} \bmod 2q, A \parallel \mu)$	secure
MS-ring-BLISS	$\mathbf{c} = (\lfloor \zeta \cdot \mathbf{a}_1 \cdot \mathbf{c}_1 + \zeta \cdot q \cdot \mathbf{c} \rceil_d + \mathbf{z}_2^\dagger \bmod p, (\mathbf{a}_1, q-2) \parallel \mu)$	secure

‡Insecure under some conditions.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research was supported by Priority Research Centers Program of the Ministry of Education (Grant Number 2009-0093827). Seongan Lim was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT, and Future Planning (no: 2016R1D1A1B01008562).

References

[1] "NIST scoring package certification procedures in conjunction with NIST special databases 2 and 6," National Institute of Standards and Technology NIST IR 5173, 1993.

[2] European Telecommunications Standards Institute, "Quantum-Safe Cryptography," http://www.etsi.org/technologies-clusters/technologies/, quantum-safe-cryptography.

[3] S. Goldwasser, S. Micali, and R. L. Rivest, "'Paradoxical' Solution to The Signature Problem," in *Proceedings of the 25th Annual IEEE Symposium on the Foundations of Computer Science*, pp. 441–448, 1984.

[4] N. Koblitz and A. Menezes, "Another look at security definitions," *Advances in Mathematics of Communications*, vol. 7, no. 1, pp. 1–38, 2013.

[5] A. Menezes and N. Smart, "Security of signature schemes in a multi-user setting," *Designs, Codes and Cryptography. An International Journal*, vol. 33, no. 3, pp. 261–274, 2004.

[6] National Institute of Standards and Technology, *Digital Signature Standard*, vol. 186, FIPS Publication, 1994.

[7] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC '08)*, pp. 197–206, Victoria, Canada, May 2008.

[8] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Advances in Cryptology—EUROCRYPT 2012. EUROCRYPT 2012*, vol. 7237 of *Lecture Notes in Computer Science*, pp. 738–755, Springer, 2012.

[9] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Advances in cryptology—CRYPTO 2013. Part I*, vol. 8042 of *Lecture Notes in Comput. Sci.*, pp. 40–56, Springer, Heidelberg, 2013.

[10] C.-H. Tan, "Key substitution attacks on provably secure short signature schemes," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E88-A, no. 2, pp. 611-612, 2005.

[11] J.-M. Bohli, S. Röhrich, and R. Steinwandt, "Key substitution attacks revisited: Taking into account malicious signers," *International Journal of Information Security*, vol. 5, no. 1, pp. 30–36, 2006.

[12] S. Blake-Wilson and A. Menezes, "Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol," in *Public Key Cryptography*, vol. 1560 of *Lecture Notes in Computer Science*, pp. 154–170, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999.

[13] D. Stehlé and R. Steinfeld, "Making NTRU as secure as worst-case problems over ideal lattices," in *Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 6632 of *Advances in Cryptology - EUROCRYPT 2011*, pp. 27–47, Tallinn, Estonia, 2011.

[14] 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.

[15] C. Peikert, "Limits on the hardness of lattice problems in l_p norms," in *Proceedings of the IEEE Conference on Computational Complexity*, vol. 17, pp. 300–351, 2007.

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

[17] A. Kawachi, K. Tanaka, and K. Xagawa, "Concurrently secure identification schemes based on the worst-case hardness of lattice problems," in *Advances in cryptology—ASIACRYPT 2008*, vol. 5350 of *Lecture Notes in Comput. Sci.*, pp. 372–389, Springer, Berlin, 2008.

[18] S. Ling, K. Nguyen, D. Stehle, and H. Wang, "Improved zero-knowledge proofs of knowledge for the ISIS problem, and Applications," in *Public-key cryptography—PKC 2013*, vol. 7778 of *Lecture Notes in Comput. Sci.*, pp. 107–124, Springer, Heidelberg, 2013.

[19] V. Lyubashevsky, D. Micciancio, C. Peikert, and A. Rosen, "SWIFFT: A modest proposal for FFT hashing," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Preface*, vol. 5086, pp. 54–72, 2008.

[20] C. Baum and V. Lyubashevsky, "Simple amortized proofs of shortness for linear relations over polynomial rings," *Cryptology ePrint Archive, Report 2017*, p. 759, 2017.