Wuhan University
Journal of Natural Sciences

2022, Vol.27 No.1, 017-025

Article ID 1007-1202(2022)01-0017-09
DOI https://doi.org/10.1051/wujns/2022271017

An Algorithm Substitution Attack on Fiat-Shamir Signatures Based on Lattice

□ LIU Jinhui[1,2], YU Yong[3†], WU Fusheng[4], CHENG Yuehua[5], ZHANG Huanguo[5]

1. School of Cyber Security, Northwestern Polytechnical University, Xi'an 710072, Shaanxi, China;
2. Research & Development Institute of Northwestern Polytechnical University, Shenzhen 518057, Guangdong, China;
3. School of Cyber Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, Shaanxi, China;
4. School of Computer Science, Guizhou University of Finance and Economics, Guiyang 550025, Guizhou, China;
5. School of Computer Science, Wuhan University, Wuhan 430072, Hubei, China

Abstract: Many evidences have showed that some intelligence agencies (often called big brother) attempt to monitor citizens' communication by providing coerced citizens a lot of subverted cryptographic algorithms and coercing them to adopt these algorithms. Since legalized services on large number of various applications and system architectures depend on digital signature techniques, in the context some coerced users who use double authentication preventing signatures to design some novel digital signature techniques, have some convincing dissertations to defuse requests from authorities and big brothers creating some corresponding subverted signatures. As rapid progress in quantum computers, National Security Agency advisory memorandum and announcement of National Institute of Standards and Technology procedures from standardization focus on some cryptographic algorithms which are post quantum secure. Motivated by these issues, we design an algorithm substitution attack against Fiat-Shamir family based on lattices (e.g., BLISS, BG, Ring-TESLA, PASSSign and GLP) that are proven post-quantum computational secure. We also show an efficient deterable way to eliminate big brother's threat by leaking signing keys from signatures on two messages to be public. Security proof shows that our schemes satisfy key extraction, undetectability and deterability. Through parameters analysis and performance evaluation, we demonstrate that our deterring subverted Fiat-Shamir signature is practical, which means that it can be applied to privacy and protection in some system architectures.

Key words: algorithm substitution attack; double authentication preventing signatures; lattice; ring-SIS (small integer solution) problem
CLC number: TP 391

Received date: 2021-09-15
Foundation item: Supported by the National Natural Science Foundation of China (61802239, 61872229, 62062019, 62074131), Key Research and Development Program of Shaanxi Province (2020ZDLGY09-06, 2021ZDLGY06-04, 2021ZDLGY05-01), Natural Science Basic Research Plan in Shaanxi Province (2019JQ-667, 2020JQ-422), and Shenzhen Fundamental Research Program (20210317191843003)

Biography: LIU Jinhui, female, Ph.D., research direction: information security and cryptography. E-mail: jh.liu6666@ nwpu.edu.cn
† To whom correspondence should be addressed. E-mail: yuyongxy@163.com

0 Introduction

Since the first computer was intruded, hackers have been developing the technology of "backdoor" which allows them to enter the system again. The main functions of the backdoor is that it has no ability to prevent the system manager from entering this system again and discover these hackers. Many techniques have been used in this "backdoor", such as intercepting postal shipping to steal and substitute networking hardware, sabotaging Internet routers, injecting malware, installing backdoors, wire-tapping undersea cables and so on [1 -3].

In 2013, Edward Snowden brought shocking news that many ongoing surveillance programs with an underlying "backdoor" target at citizens conducting by National Security Agency (NSA) and partners from all over the world [4]. A typical example is a pseudorandom generator (PRG) named Dual_EC_ DRBG backdoored by NSA, from NIST (National Institute of Standards and Technology). After choosing a few concrete parameters employed in the PRG, an attacker or any adversary is not able to differentiate exports on PRG from any random number but can forecast following exports[5]. In this circumstances, post-Snowden cryptography attracts much of attentions in recent years.

As one of the research topics in post-Snowden cryptography, the notion of algorithm substitution attack (ASA) was formalized by Bellare *et al* [6] in some semantics from algorithms named symmetric encryption algorithms. The ASA method is capable of any attacker or old big brother to substitute a few of pieces of randomized encryption algorithms or signature algorithms with a modified one such that it can leak secret keys subliminally and undetectably to the adversary. Ateniese *et al* [7] first proposed a model of ASA on signature schemes, however, the subverted signature is generic and inefficient. Then Liu *et al* [8] introduced a much high efficient ASA method about one affirmatory crowd in some signature schemes. Recently, Beak *et al*[9] presented a much more efficient and undetectable method ASA from a classical DSA (digital signature algorithm) digital signature. At present most proposed subverted signatures only consider how to subvert signature schemes, there still needs some countermeasures to address big brother's threat, while a new proposed signatures named double authentication preventing signatures can be used to deter this kind of big brother's action.

The double authentication preventing signatures (DAPS) are a class of extraordinary digital signatures with double signatures extractability which means deterable when there exist two different signatures from messages (m_0, p_1) and (m_0, p_2), where $p_1 \neq p_2$. When a signature is subverted and satisfies double signature extractability, the subverted signature can be deterable by revealing real signature's signing secret keys to anyone. Unlike these two ring signatures with linkability and traceability[10-13], our DAPRS (double authentication preventing ring signatures) has stronger accountability which leads any two pairs of signatures produced by same member in a ring set to reveal his (or her) secret signing keys. As for linkable ring signatures, it allows anyone to efficiently decide whether any two pairs of signatures are produced by the same member without revealing his (or her) identity. As for traceable ring signatures, it can reveal his (or her) identity if any two signatures are produced by the same member. On the basis of the digital signatures in Refs. [14-16], most designed DAPS based on discrete logarithm problems and large integer factorization problems face new challenges because there exist polynomial computational complexity quantum algorithms to solve the two problems, such as Shor algorithm[17,18]. Hence, it is necessary to study some post quantum secure DAPS.

Lattice-based signature is a cutting-edge cryptographic "technology". It has several interesting properties, such as high computational efficiency, novel and powerful cryptographic functionalities/applications, strong provable security guarantees, believed "post-quantum" security and so on. Therefore, it is vital for us to study some lattice-based algorithm substitution attacks. While most efficient lattice-based signatures which are a promising post-quantum cryptography belong to Fiat-Shamir signature paradigms (e.g., BLISS[19,20], GLP[21], PASS-Sign[22], Ring-TESLA[23]) and Hash-and-sign paradigms (e.g., GGH[24], NTRUSign[25], GPV[25]) at the NIST workshop on post-quantum cryptography. Lattice-based Hash-and-sign paradigm follows that a trapdoor function can be provided by a short lattice basis. Most of them are heuristic security (no actual security proofs) and are relatively inefficient than lattice-based Fiat-Shamir (FS) signature paradigms[26]. Furthermore most lattice-based Hash-and-sign paradigms have unique signatures which are against subversion attacks[7]. Hence we aim at algorithm substitution attacks on FS lattice signature paradigms (FS-LBS). In this paper, we present ASA against those schemes that any three consecutive subverted signatures can extract signing keys. At the same time, we provide some countermeasures against ASA by using DAPS to deter the big brother's threaten. And we show that our scheme can be applied to some practical architectures based on some concrete experiment analysis.

The remainder of this paper is organized in the following sequence. Section 1 shows some preliminaries and cryptographic knowledge. Section 2 provides some notions about deterable subverted signatures and some design requirements. Section 3 presents our concrete deterable subverted FS-LBS scheme and gives proof of key extraction, undetectability and deterability. In Section 4, we make some parameter analysis and performance evaluation. Finally, we give our conclusions.

1 Preliminaries

1.1 Notations

Some basic notations have been shown in Table 1.

Symbols	Description
$\mathbf{Z}$	an integer ring
p	a large prime
q	a large prime power
$\mathbf{Z}_q$	a residual class ring
$\boldsymbol{Z}_q^{m\times m}$	an $m\times m$ matrix over $\mathbf{Z}_q$
$q-1$	a big number satisfying q=1 mod 2n
$\mathfrak{R}$ =Z [x]/(x^n+1)	a polynomial ring that is isomorphic to the integer lattice $\mathbf{Z}^n$
$\mathfrak{R}_q$	a set of polynomials, where their degree is $n-1$ and coefficients are from $[-\frac{p-1}{2},\frac{p-1}{2}]$
$\mathfrak{R}_1$	a set of polynomials, where their degree is $n-1$ and coefficients are from [−1, 1].
$\Vert \boldsymbol{a} \Vert_1$	$\sum_{i=0}^{n-1}\lvert\boldsymbol{a}_i\rvert$
$\Vert \boldsymbol{a} \Vert$	$\sqrt{\sum_{i=0}^{n-1}\lvert\boldsymbol{a}_i\rvert^2}$
$\Vert \boldsymbol{a} \Vert_\infty$	$\max_i \lvert\boldsymbol{a}_i\rvert$
Λ	a full rank integer lattice
$\boldsymbol{D}_{\Lambda,c,\sigma}$	a discrete distribution over subset of $\mathbf{Z}_q^m$

1.2 Cryptographic Problems on Lattices

Definition 1 (Ring-SIS$_{q,m,\beta}$[27,28]) Given m uniformly elements $R_i \in \mathfrak{R}_q$ at random and let $\boldsymbol{a} = (\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m)$, search a vector $z \in \mathfrak{R}^m$ but not zero vector with the relation $\|z\| \leqslant \boldsymbol{\beta}$ satisfying

$$\boldsymbol{a} \cdot \boldsymbol{z} = 0 \in \mathfrak{R}_q$$

Note that in ring-SIS, each $\boldsymbol{a}_i \in \mathfrak{R}_q$ corresponds to n related vectors $\boldsymbol{a}_i \in \mathbf{Z}_q^n$ in SIS, where n is the degree of $\mathfrak{R}$. Each $z_i \in \mathfrak{R}$ of a ring-SIS solution corresponds to a block of n integers, that means $\boldsymbol{a}_i \in \mathbf{Z}_q^{m \times m}$ and $z \in \mathbf{Z}^{m \times m}$.

Definition 2 (Ring-LWE$_{n,q,D_{R,\sigma}}$ [27,28]) Given m uniformly elements $\boldsymbol{a}_i, \boldsymbol{b}_i \in \mathfrak{R}_q$ at random and let $\boldsymbol{a} = (\boldsymbol{a}_1, \cdots, \boldsymbol{a}_m) \in \mathfrak{R}_q, \boldsymbol{b} = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_m) \in \mathfrak{R}_q$, this algorithm is to search a vector $\boldsymbol{s} \in \mathfrak{R}^m$ satisfying $\boldsymbol{b} = \boldsymbol{as} + \boldsymbol{e}$, here $\boldsymbol{e} \leftarrow \boldsymbol{D}_{\mathfrak{R}^m, \sigma}$.

Definition 3 (Rejection sampling lemma [29-33])

Suppose that $\boldsymbol{V} \subseteq \mathbf{Z}^m$. Let $\boldsymbol{h}: \boldsymbol{V} \to \mathbf{R}$ be a random distribution from a Hash value, and $\sigma = \omega(\sqrt{\log m})$. If a constant M exists, the following distribution

1) $\boldsymbol{v} \leftarrow \boldsymbol{h}$

2) $\boldsymbol{z} \leftarrow \boldsymbol{D}_\sigma^m$

3) Output $(\boldsymbol{z}, \boldsymbol{v})$ with probability of $\dfrac{1}{m}$ and the below distribution

1) $\boldsymbol{v} \leftarrow \boldsymbol{h}$

2) $\boldsymbol{z} \leftarrow \boldsymbol{D}_{\boldsymbol{v},\sigma}^m$

3) Output $(\boldsymbol{z}, \boldsymbol{v})$ with probability of $\min(\dfrac{\boldsymbol{D}_\sigma^m(\boldsymbol{z})}{M\boldsymbol{D}_{\boldsymbol{v},\sigma}^m(\boldsymbol{z})}, 1)$ is statistically indistinguishable within distance of $\dfrac{2^{-\omega(\log m)}}{M}$. In the following, we use the RejectionSample to represent the algorithm.

1.3 Description of Lattice Based Fiat-Shamir Type Signature Schemes

The Fiat-Shamir type signatures based on lattice consist of algorithms in the following:

Key Generation:

1) Pick $\boldsymbol{a} \leftarrow \mathfrak{R}$ at random.

2) Choose uniformly random $\boldsymbol{s}_1 \leftarrow \mathfrak{R}_1, \boldsymbol{s}_2 \leftarrow \mathfrak{R}_1$

3) Compute $\boldsymbol{t} = \boldsymbol{as}_1 + \boldsymbol{s}_2$

4) Output a pair of public key and secret key: $(\boldsymbol{a}, \boldsymbol{t}); (\boldsymbol{s}_1, \boldsymbol{s}_2)$

Sign $(\boldsymbol{\mu}, \boldsymbol{a}, \boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{t})$:

1) Select two random numbers $\boldsymbol{y}_1 \leftarrow \mathfrak{R}_1, \boldsymbol{y}_2 \leftarrow \mathfrak{R}_1$

2) Calculate $\boldsymbol{w} = \boldsymbol{ay}_1 + \boldsymbol{y}_2$

3) Compute a value $c = H(\boldsymbol{a}, \boldsymbol{t}, \boldsymbol{w}, \boldsymbol{\mu})$

4) Obtain $z_1 = \boldsymbol{y}_1 + c\boldsymbol{s}_1, z_2 = \boldsymbol{y}_2 + c\boldsymbol{s}_2$

5) Run the RejectionSample $(z_1, z_2, c\boldsymbol{s}_1, c\boldsymbol{s}_2)$ and go to 1) if it rejects.

6) Output a pair of signature (c, z_1, z_2)

Verify $(\boldsymbol{\mu}, \boldsymbol{a}, z_1, z_2, \boldsymbol{t})$:

1) Check $\boldsymbol{w} = \boldsymbol{a}z_1 + z_2 - c\boldsymbol{t}$ mod q whether holds or not.

2) Accept if and only if the equation $c = H(\boldsymbol{a}, \boldsymbol{t}, \boldsymbol{w}, \boldsymbol{\mu})$ and a small norm $\|(z_1, z_2)\|$ holds.

Here $\mathfrak{R}_1$ with tiny modulus is the subset of $\mathfrak{R}$. Cryptographic Hash function H outputs a low norm subset of $\mathfrak{R}$.

1.4 Double Authentication Preventing Signatures

A DAPS includes four probability polynomial time (PPT) algorithms (KGen, Sign,Ver, Extract) as follows:

1) Given a security parameter λ, the algorithm KGen(1^λ) outputs public keys pk and private keys sk.

2) The algorithm Sign(sk, a, p) outputs a signature π on a pair of public/private key (pk, sk) and a subject/message pair (a, p).

3) The algorithm Ver(pk, a, p, π) outputs either 0 for rejection or 1 for acceptance on pk, (a, p) and π.

4) The algorithm Extract outputs the private key sk on input pk, $(a_1, p_1), (a_2, p_2)$ and σ_1, σ_2, where $a_1 = a_2, p_1 \neq p_2$.

A DAPS satisfies two properties of existential unforgeability under chosen message attack (EUF-CMA) and double signature deterability (DSE)[13].

2 Our Deterable Subverted Signatures

We first provide the threat model in this section. Then we give formal definitions for the syntax of deterable subverted signatures. Compared with regular deterable digital signatures, these schemes need a "extraction key" for their manipulates if there exists a subversion attack. Finally we provide some security and functionality features of a deterable subverted signatures on the basis Refs. [7-9].

2.1 Threat Model

Since authentication services of various system models and applications depend upon digital signatures, in the context coerced users who use a DAPS to design some court convincing signatures to refuse big brothers' (or attackers') requirements, we construct a subverted signature with a deterable function by using an algorithm substitution attack on double authentication preventing signatures.

2.2 Notions of Deterable Subverted Signatures

Definition 4 A deterable subverted signature $\overline{\text{SIG}}$ for nonsubverted signature SIG includes four PPT algorithms as follows:

1) On inputting a security parameter ℓ, this algorithm $\overline{\text{Gen}}$ outputs a subversion key subk.

2) On inputting a subversion key subk, a state *l*, a private key sk, and a message μ, the algorithm $\overline{\text{SIG}}$ outputs a subverted signature σ by an updated status *l*.

3) On inputting a message μ, a public key pk and a subverted signature σ, this algorithm Ver outputs 1 which means accept and outputs 0 which means reject.

4) On inputting a pair of colliding messages (μ_1,μ_2), a public key pk, and its corresponding non-subverted signatures σ_1,σ_2, this algorithm Deter outputs the private key sk.

2.3 Security and Functionality Features

The key extraction algorithm means that anyone including big brothers and attackers can compute the signature private key from known information if he or she makes a signature on a pair of colliding messages.

Definition 5 Assume that SIG=(Gen, Sign, Ver) is generic signature scheme and $\overline{\text{SIG}}$=($\overline{\text{Gen}}$, $\overline{\text{SIG}}$, Ver, Deter) is a deterable subverted signatures for SIG. Consider a key extraction game $\text{Keyextraction}_{\beta,\text{SIG},\overline{\text{SIG}}(\ell)}$ as follows:

1) Using $\text{Gen}(1^{\ell})$, it can generate a pair of (pk, sk).

2) By the algorithm $\overline{\text{Gen}}(1^{\ell})$, it can generate a subversion key subk.

3) For $i=1,2,\cdots,Q_S$,

Compute $(\overline{\sigma}_i,l_i)\leftarrow\overline{\text{SIG}}(\text{subk},\text{sk},\mu_i,l_{i-1})$

if an adversary $\mathcal{B}$ queries every message μ_i

Return $(\overline{\sigma}_i,l_i)$ to $\mathcal{B}$.

4) $\mathcal{B}$ outputs sk' by $(\text{pk},\text{subk},\{\sigma_1,\cdots,\sigma_\ell\})$

5) Check the equation $\text{sk}'=\text{sk}$ whether holds or not. If it holds, return 1. Otherwise, it returns 0.

Define an advantage

$\text{Adv}^{\text{keyextract}}_{\mathcal{B},\text{SIG},\overline{\text{SIG}}}(\ell)=\Pr[\text{Keyextraction}_{\text{B},\text{SIG},\overline{\text{SIG}}}(\ell)=1]$.

Given the private key sk and its corresponding public key pair pk, the functionality undetectability means that any users can not find the detecting subversion.

Definition 6 Assume that a general signature SIG=(Gen, Sign, Ver) and a deterable signature

$\overline{\text{SIG}}$=($\overline{\text{Gen}}$, $\overline{\text{SIG}}$, Ver, Deter)

for SIG. Consider an undetectability game

$\text{Detect}_{\mathcal{A},\text{SIG},\overline{\text{SIG}}}(\ell)$ as follows:

1) Generate a pair of public/private key (pk,sk) by the algorithm $\text{Gen}(1^{\ell})$.

2) By the algorithm $\text{Gen}(1^{\ell})$, it can generate a subversion key subk.

3) Choose $b\in\{0,1\}$ randomly, the game $\mathcal{A}^{\text{Sign}O_b(\bullet),\text{Reset}(\bullet)}(\text{sk, pk})$ outputs its guess b'.

4) If $b'\neq b$, it returns 0, otherwise it returns 1.

$\text{Sign}O_b(\mu_i)$ is given as follows:

5) If b = 0, compute $\sigma_i'\leftarrow\text{Sign}(\text{sk},\mu_i)$

6) If b = 1, compute

$$(\sigma_i',l_i)\leftarrow\overline{\text{Sign}}(\text{subk},\text{sk},\mu_i,l_{i-1})$$

7) Return σ_i'

Reset(·) is given as follows: Reset(rt*ᵢ*) || rt*ᵢ* is a reset query.

Define advantage

$$\text{Adv}^{\text{detect}}_{\mathcal{A},\text{SIG},\overline{\text{SIG}}}(\ell)=|\Pr[\text{Detect}_{\mathcal{A},\text{SIG},\overline{\text{SIG}}}(\ell)=1]-\frac{1}{2}|$$

For any PPT adversary $\mathcal{A}$, if there exists a negligible function $\varepsilon(\ell)$ satisfying

$$\text{Adv}^{\text{detect}}_{\mathcal{A},\text{SIG},\overline{\text{SIG}}}(\ell)=|\Pr[\text{Detect}_{\mathcal{A},\text{SIG},\overline{\text{SIG}}}(\ell)=1]-\frac{1}{2}|\leqslant\varepsilon(\ell)$$

the deterable subverted signature is undetectable. It means that the Ver algorithm can output some same results when it is a subverted signature or a normal signature on some same messages.

Deterability means that it can be deterred if there exists algorithm substitution attack on signature scheme.

Definition 7 Given a general signature SIG=(Gen,Sign,Ver) and a deterrable signature

$\overline{\text{SIG}}$=($\overline{\text{Gen}}$, $\overline{\text{SIG}}$, Ver, Deter) for SIG, the deterability game $\text{Deter}_{\mathcal{C},\text{SIG},\overline{\text{SIG}}}(\ell)$ is given as follows:

1) According to the algorithm $\text{Gen}(1^{\ell})$, it generates a pair of public/private (pk, sk).

2) Run $\mathcal{C}$ (pk, sk), then generate $(\mu_1,\mu_2,\sigma_1,\sigma_2)$.

3) Return 0 if μ_1 and μ_2 are not colliding.

4) $v_i\leftarrow\text{Ver}(\text{pk},\mu_i,\sigma_i)$ for *i* = 1, 2.

5) Return 0 if $v_1=0$ or $v_2=0$.

6) Run $\text{Deter}(\text{pk},\mu_1,\mu_2,\sigma_1,\sigma_2)$, then generate sk'.

7) Return 0 if $\text{sk}'\neq\text{sk}$. Else return 1.

We define the advantage

$$\mathrm{Adv}^{\mathrm{Deter}}_{\mathcal{C},\mathrm{SIG},\overline{\mathrm{SIG}}}(\ell)=\Pr[\mathrm{Deter}_{\mathcal{C},\mathrm{SIG},\overline{\mathrm{SIG}}}(\ell)=1]$$

The advantage means that for any PPT adversary $\mathcal{C}$, if there exists a negligible function $\varepsilon(\cdot)$ satisfying

$$\Pr[\mathrm{Deter}_{\mathcal{C},\mathrm{SIG},\overline{\mathrm{SIG}}}(\ell)=1]\leqslant\frac{1}{2}$$

the deterable subverted signature is deterable. It means that our scheme can deter some signatures embedding backdoors.

3 Our Deterable Subverted Lattice Based Fiat-Shamir Type Signatures

This section introduces a self-enhancement or subverted attack on Fiat-Shamir type lattice signatures.

Our subverted Fiat-Shamir type lattice-based signatures (FS-LBS) are described as follows:

- Subverted key generation $\overline{\mathrm{SIG}}_{\text{FS-LBS}}$: On inputting a security parameter ℓ, a pseudo random Hash function $F:\{0,1\}^{\ell}\times\mathfrak{R}\to\mathfrak{R}_1$ and a random number $\kappa_1,\kappa_2\in\{0,1\}^{\ell}$, the algorithm $\overline{\mathrm{Gen}}_{\text{FS-LBS}}$ outputs κ_1,κ_2 and F which can be described as subk = (desc$F$, κ_1,κ_2).
- Subverted sign $\overline{\mathrm{Sign}}_{\text{FS-LBS}}$: On inputting public keys $(\boldsymbol{a},\boldsymbol{t})$ of FS-LBS, message μ, private keys $(\boldsymbol{s}_1,\boldsymbol{s}_2)$, subversion key subk and a state $l=(j,\tau)$, the algorithm outputs $(\overline{\sigma},l)$ as follows.

```
        $j\leftarrow 0,\ \tau\leftarrow 0$
      If $j=0$ mod 2,
    1) Select two random numbers
            $\boldsymbol{y}_1\leftarrow\mathfrak{R}_1,\boldsymbol{y}_2\leftarrow\mathfrak{R}_1$
    2) Calculate $\boldsymbol{w}=\boldsymbol{a}\boldsymbol{y}_1+\boldsymbol{y}_2$
    3) Compute a value $c=H(\boldsymbol{A},\boldsymbol{t},\boldsymbol{w},\mu)$
    4) Obtain $z_1=\boldsymbol{y}_1+c\boldsymbol{s}_1, z_2=\boldsymbol{y}_2+c\boldsymbol{s}_2$
    5) Run the RejectionSample$(z_1,z_2,c\boldsymbol{s}_1,c\boldsymbol{s}_2)$ and go to 1) if it rejects.
    6) Let $\tau=c$ and $\overline{\sigma}=(c,z_1,z_2)$
        Else
    7) Calculate $\boldsymbol{w}=\boldsymbol{a}\boldsymbol{y}'_1+\boldsymbol{y}'_2$
    8) Compute a value $c'=H(\boldsymbol{A},\boldsymbol{t},\boldsymbol{w}',\mu)$
    9) Obtain $z'_1=\boldsymbol{y}'_1+c'\boldsymbol{s}_1, z'_2=\boldsymbol{y}'_2+c'\boldsymbol{s}_2$
    10) Run RejectionSample $(z'_1,z'_2,c'\boldsymbol{s}_1,c'\boldsymbol{s}_2)$ and go to 1) if it rejects.
    11) Set $\tau=c'$ and $\overline{\sigma}=(c',z'_1,z'_2)$
        $j=j+1$
        Let $l=(j,\tau)$
        Return $((\overline{\sigma},l)$
    Verify $(\mu,\overline{\sigma},\boldsymbol{a},\boldsymbol{t})$:
    1) Check $\boldsymbol{w}'=\boldsymbol{a}z'_1+z'_2-c'\boldsymbol{t}$ mod $q$ whether holds or not.
    2) Accept if and only if the equation $c'=H(\boldsymbol{a},\boldsymbol{t},\boldsymbol{w}',\mu)$ and a small norm $\|(z'_1,z'_2)\|$ hold.
```

If a FS-LBS scheme is subverted, the action of the signer can be found by revealing real signer's signing secret keys to anyone. When the signing keys is vital for him, in some cases the signer will be punished or the signer will result in great economic losses, or there exist some court convincing reasons to deny big-brother or authority agency demands. Aiming at the subverted lattice-based Fiat-Shamir type signatures, we add a Deter algorithm. Our Deter algorithm makes sure that the lattice-based Fiat-Shamir type signature is against algorithm substitution attack.

- Deter

By the principle of DAPS, if there exists two FS-LBS signatures

$$\sigma_1=(c_1,z_{11},z_{12}),\sigma_2=(c_2,z_{21},z_{22})$$

On colliding messages μ_1 and μ_2, respectively, anyone can obtain the signing secret key $\boldsymbol{s}_1=\dfrac{z_{11}-z_{21}}{c_1-c_2}$ and $\boldsymbol{s}_2=\dfrac{z_{12}-z_{22}}{c_1-c_2}$ by solving a linear equation respectively.

Then we present our scheme satisfying Key extraction, Undetectability and Deterability.

Key extraction. From the subverted FS-LBS $\overline{\text{FS-LBS}}$, we show that the signing private keys of the FS-LBS can be extracted from the $\overline{\text{FS-LBS}}$. That is to say, any consecutive $\overline{\text{FS-LBS}}$ starting with odd or even index is able to release the signing private keys. Below we give the formal proof.

Theorem 1 Given subverted FS-LBS scheme $\overline{\text{FS-LBS}}$ which outputs any three consecutive signatures, the signing private keys of FS-LBS can be revealed with probability 1.

Proof Given three messages m,m',m'', an adversary $\mathcal{B}$ obtains three consecutive subverted FS-LBS $\overline{\sigma}_j=(c,z_1,z_2)$, $\overline{\sigma}_{j+1}=(c',z'_1,z'_2)$ and $\overline{\sigma}_{j+2}=$ (c'',z''_1,z''_2), respectively.

If $j=0$ mod 2, by using $\mathcal{B}$'s subversion keys subk (κ_1,κ_2,F), compute signing keys as follows:

$\boldsymbol{y}'_1=F(\kappa_1,c),\boldsymbol{y}'_2=F(\kappa_2,c)$,

Calculate $\boldsymbol{w}'=\boldsymbol{a}\boldsymbol{y}'_1+\boldsymbol{y}'_2$

Compute a value $c'=H(\boldsymbol{A},\boldsymbol{t},\boldsymbol{w}',\mu)$

$\boldsymbol{s}_1=c'^{-1}(z'_1-\boldsymbol{y}'_1)$ and $\boldsymbol{s}_2=c'^{-1}(z'_2-\boldsymbol{y}'_2)$

Return $\boldsymbol{s}_1,\boldsymbol{s}_2$.

If j = 1 mod 2, j + 1 = 0 mod 2. $\mathcal{B}$ chooses

$\overline{\sigma}_{j+1}=(c',z_1',z_2')$ and $\overline{\sigma}_{j+2}=(c'',z_1'',z_2'')$ to compute the signing keys $\boldsymbol{s}_1,\boldsymbol{s}_2$ by using the same method as above, so $\mathcal{B}$ can compute the signing keys by the subverted signature algorithm $\overline{\text{Sign}}_{\text{FS-LBS}}$. Hence,

$$\text{Adv}_{\mathcal{B},\overline{\text{FS-LBS}}}^{\text{extract}}(\lambda)=1.$$

Undetectability. We show that our constructed subverted FS-LBS scheme $\overline{\text{FS-LBS}}$ is undetectable by Theorem 2.

Theorem 2 Given subverted FS-LBS scheme $\overline{\text{FS-LBS}}$, the detection advantage is negligible under the assumption of pseudo-random function (PRF) *F*.

Proof By a sequence of games, we prove the theorem. We define the events $S_i(i=1,2,\cdots)$ of games G_i that is $b=b'$.

Game 0. The original undetectability game Detect

$$\text{Detect}_{\mathcal{A},\text{FS-LBS},\overline{\text{FS-LBS}}}(\lambda).$$

Game 1 As before, but we modify Game 0 to use $b=0$ for answering $\mathcal{A}$'s queries as Game 0 and to use a uniform random string for substituting $b=1$ ($j=1$ mod 2) and noncomputed $\boldsymbol{y}_1',\boldsymbol{y}_2'$ by PRF. A detailed description is given as follows.

$T\leftarrow\varnothing$.

If b=0, this game responds to a valid FS-LBS scheme and j = 0, $\tau=\varnothing$ to $\mathcal{A}$ after receiving every signing query on m and a reset query rt , respectively.

If b = 1, this game carries on as follows:

```
When $\mathcal{A}$ does some signing queries on $m$,
$j$ ←0, $\tau$←0
If $j$ = 0 mod 2
1) Pick $\boldsymbol{y}_1\leftarrow\mathfrak{R}_1,\boldsymbol{y}_2\leftarrow\mathfrak{R}_1$
2) Compute $\boldsymbol{w}=\boldsymbol{a}\boldsymbol{y}_1+\boldsymbol{y}_2$ and
3) Compute $c=H(\boldsymbol{A},\boldsymbol{t},\boldsymbol{w},\mu)$ and
4) Calculate $\boldsymbol{z}_1=\boldsymbol{y}_1+c\boldsymbol{s}_1,\boldsymbol{z}_2=\boldsymbol{y}_2+c\boldsymbol{s}_2$ and
5) Run the RejectionSample$(\boldsymbol{z}_1,\boldsymbol{z}_2,c\boldsymbol{s}_1,c\boldsymbol{s}_2)$, and return 0 if it accepts.
6) Set $\tau=c$ and $\overline{\sigma}=(c,\boldsymbol{z}_1,\boldsymbol{z}_2)$.
Else
1) If $(\tau,\boldsymbol{t}_1,\boldsymbol{t}_2)\notin T$, pick randomly $\boldsymbol{t}_1,\boldsymbol{t}_2\in\mathfrak{R}_1$ uniformly. Else extract $(\tau,\boldsymbol{t}_1,\boldsymbol{t}_2)\in T$ and compute
2) $\boldsymbol{y}_1'=t_1,\boldsymbol{y}_2'=t_2$,
3) $\boldsymbol{w}'=\boldsymbol{a}\boldsymbol{y}_1'+\boldsymbol{y}_2'$
4) $c'=H(\boldsymbol{A},\boldsymbol{t},\boldsymbol{w}',\mu)$
5) $\boldsymbol{z}_1'=\boldsymbol{y}_1'+c'\boldsymbol{s}_1,\boldsymbol{z}_2'=\boldsymbol{y}_2'+c'\boldsymbol{s}_2$
6) Run the RejectionSample$(\boldsymbol{z}_1',\boldsymbol{z}_2',c'\boldsymbol{s}_1,c'\boldsymbol{s}_2)$ and go to 1) if it rejects.
7) Set $T=T\cup\{\tau,\boldsymbol{t}_1,\boldsymbol{t}_2\}$, $\overline{\sigma}=(c',z_1',z_2')$
$j=j+1$
Return $\overline{\sigma}$
```

When $\mathcal{A}$ makes some reset queries rt, set j = 0, $\tau=\varnothing$.

First, Game 0 and Game 1 are indistinguishable by the distinguishing between PRF and some random functions, i.e.,

$$|\Pr[S_1]-\Pr[S_0]|=\text{Adv}_{\mathcal{A},F}^{\text{PRF}}(\lambda).$$

Aiming at Game 2, we modify this game as Game 1 in the following:

If j = 1 mod 2, whether $(\tau,\boldsymbol{t}_1,\boldsymbol{t}_2)$ in T or not. If is not checked, $(\boldsymbol{t}_1,\boldsymbol{t}_2)\in\mathfrak{R}_1$ is chosen randomly and $\boldsymbol{y}_1'=\boldsymbol{t}_1,\boldsymbol{y}_2'=\boldsymbol{t}_2$.

Secondly, we denote Col be the event that $\tau_j=\tau_l$ for some $l\leqslant Q_S$. Game 1 and Game 2 are both proceeding identically if the algorithm Col can not happen, i.e., $|\Pr[S_2]-\Pr[S_1]|\leqslant\Pr[\text{Col}]\leqslant\frac{{Q_S}^2}{|q|}$.

Due to Game 3, we modify this game as Game 2 in the following:

While $\mathcal{A}$ makes some reset queries rt, Game 3 is not able to reset j and τ but it answers the adversary $\mathcal{A}$'s other queries by some same ways similar to Game 2.

Finally, the distribution of subverted FS-LBS scheme $\overline{\text{FS-LBS}}$ is identical to the distribution of real FS-LBS scheme except of j=0 mod 2 and j=1 mod 2, because $(\boldsymbol{t}_1,\boldsymbol{t}_2)\in\mathfrak{R}_1$ is chosen randomly and $\boldsymbol{y}_1'=\boldsymbol{t}_1,\boldsymbol{y}_2'=\boldsymbol{t}_2$ depends on τ. That is to say, though this game can not be able to do anything on receiving these reset queries, this distribution between Game 2 and Game 3 is the same. That also means that $\mathcal{A}$ cannot be able to obtain any advantages in surmising b from inquiring about some signing oracles, i.e., $\Pr[S_2]=\Pr[S_3]=\frac{1}{2}$.

Taking all together, we have

$$\text{Adv}_{\mathcal{A},\text{FS-LBS},\overline{\text{FS-LBS}}}^{\text{detect}}(\lambda)\leqslant\text{Adv}_{\mathcal{A},F}^{\text{prf}}(\lambda)+\frac{Q_S^2}{|q|}.$$

Theorem 3 (Deterability). Given FS-LBS scheme, the $\overline{\text{FS-LBS}}$ can be deterable under solving a linear equation with probability 1.

Proof When FS-LBS scheme is not subverted, assume that an adversary $\mathcal{B}$ gets two FS-LBS signatures $\sigma_1=(c_1,z_{11},z_{12}),\sigma_2=(c_2,z_{21},z_{22})$ on colliding messages $\mu_1=(a,p_1),\mu_2=(a,p_2)$. By the signature algorithm of FS-LBS, $\mathcal{B}$ has the following relations:

$$\begin{cases} z_{11} = \boldsymbol{y}_1 + c_1 \boldsymbol{s}_1 \\ z_{12} = \boldsymbol{y}_2 + c_1 \boldsymbol{s}_2 \\ z_{21} = \boldsymbol{y}_1 + c_2 \boldsymbol{s}_1 \\ z_{22} = \boldsymbol{y}_2 + c_2 \boldsymbol{s}_2 \end{cases}$$

There are four linear equations with four unknown information $\boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{s}_1, \boldsymbol{s}_2$ on $\mathfrak{R}$. So these unknown information can be solved, i.e.,

$$\boldsymbol{s}_1 = \frac{z_{11} - z_{21}}{c_1 - c_2}, \boldsymbol{s}_2 = \frac{z_{12} - z_{22}}{c_1 - c_2}$$

If FS-LBS scheme is subverted, the subverted signature can be found. Due to the solved secret keys, a signature can be verified whether the signature is an original FS-LBS signature or a subverted signature $\overline{\text{FS-LBS}}$. Hence, the $\overline{\text{FS-LBS}}$ can be deterable by solving a linear equation with probability 1.

4 Parameter Analysis

4.1 Numerical Analysis

This part first numerically makes some efficiency of our deterable subverted FS-LBS scheme in terms of storage overhead and computational overhead which are listed in Table 2 and Table 3.

As for the storage overhead, it consists of size of pair of public/secret keys and size of signature which is listed in Table 2. The communication cost is determined by the number of *j*. As for the computational overhead, compared with the Hash functions, the most resource-consuming operation is the multiplication over ring $\mathfrak{R}$. In the signing process, Ver process and Deter process, the computational overhead is listed in Table 2, where the number of multiplications over ring $\mathfrak{R}$ is linear to the number of *j*. For simplicity, we denote that PM represents the polynomial point multiplications, PA represents the polynomial additions, PS represents the polynomial subtraction, RS represents polynomial Gauss sampling and *H* and *F* represent the Hash functions.

By implementation analysis in Ref. [9], we can see that there needs at most three consecutive signatures in the subverted FS-LBS which does not affect practicality of the subverted FS-LBS. So in our constructed scheme, we do not consider signature loss. Here we only analyze the security level, size of secret keys (sk), size of public keys (pk) and size of signature for some deterable subverted FS-LBS in Refs. [20, 21, 29-32]. From Tables 2-3, we can see that our deterable subverted signatures have reasonable efficiency in terms of communication cost, computational overhead and storage overhead.

Table 2 Storage and communication overhead of deterable subverted FS-LBS scheme

Items	Storage overhead
Public key	$O(m^2\log(q))$
Secret key	$O(m^2\log(2d+1))$
Signature	$O(m\log(12\sigma))$

Table 3 Computational overhead of deterable subverted FS-LBS scheme

Items	Computational overhead
$\overline{\text{Sign}}$	$O((\text{RS} + 2\text{PM} + 3\text{PA} + H)l$ $+(\text{ RS} + \text{PM} + 3\text{ PA}+ 2F\text{ })(j - l)),\ 1 \le l \le j$
Ver	$O(H + \text{RS} + \text{PM} + 3\text{PA} + 2F\text{ })$
Deter	$O(2\text{PS})$

4.2 Implementation

The implementation is conducted with NFLlib, which is a NTT-based fast lattice cryptography library, on Intel i7-7700 CPU @ 3.60GHz and Ubuntu linux operation system. By statistics, these important algorithm operations mainly consist one polynomial addition, one polynomial multiplication and one polynomial Gaussian. Since the implementation of any Hash function is not included in NFLlib, we test the running time of three hash functions by a HMAC based on SM3 algorithm. The execution time of each cryptographic operation in different parameters is shown in Table 4. Here the execution time of these Hash functions we consider is the same.

Experimental results for proposed deterable subverted FS-LBS of each algorithm are depicted in Fig. 1. We increase the number of *j* from 2 to 10 for each test to see the time cost of $\overline{\text{Sign}}$, Ver and Deter algorithm. Here procedure of subversion key generation can be considered as a random number, so we can omit its time consumption.

On one hand, for different parameters in Table 4, the time consuming of subverted sign $\overline{\text{Sign}}$ algorithm is about 0.1278×*l*+0.2294×(*j*−*l*) ms, 0.1275×*l*+0.2351 ×(*j*−*l*) ms, 0.1895×*l*+0.3623×(*j*−*l*) ms, 0.2084×*l*+ 0.3789 ×(*j*−*l*) ms, 0.4141×*l*+0.674 4×(*j*−*l*) ms for the number of *j*, *l*. The time efficiency of Ver algorithm is about 0.3344 ms, 0.3451 ms, 0.5373 ms, 0.5559 ms, 0.9614 ms. The time efficiency of Deter algorithm is about 0.0050 ms, 0.0046 ms, 0.0074 ms, 0.0095 ms, 0.0240 ms. On the other hand, suppose that *j* =10 and *l* = 1, 2, 3, 4, 5, according to Fig. 1, we can see that time cost of the total algorithm justifies the feasibility.

Table 4 The cryptographic operation time in the scheme

ms

n	q / bit	m	PA	PS	PM	RS	Hash function
8	60	16	0.004 56	0.002 50	0.003 33	0.002 43	0.105
128	14	216	0.003 35	0.002 30	0.002 43	0.002 62	0.110
1 024	60	2 048	0.002 48	0.003 69	0.002 27	0.002 56	0.175
8 192	124	16 384	0.004 54	0.004 75	0.006 52	0.004 74	0.177
32 768	124	65 536	0.012 00	0.012 00	0.026 78	0.037 50	0.287

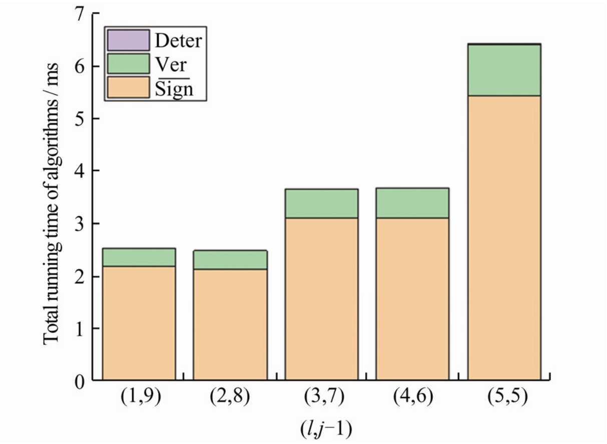

Fig. 1 Simulation results of our construction for different *j*, *l*

5 Conclusion

This paper first explores a novel algorithm substitution method on lattice-based Fiat-Shamir type signature schemes. Based on this, then we provide countermeasures to deterable signature subversion. Security proof shows that our construction satisfies three different security and privacy requirements. Parameter analysis demonstrates that our construction is feasible. In future, we will study our algorithm by widening range of possible schemes that is vulnerable to algorithm substitution attack or by other much more valuable methods and countermeasures on these post quantum secure signatures. In addition, some other possible work will focus on some algorithm substitution attacks on other cryptographic primitives.

References

[1] Easttom W. Cryptographic backdoors [C]//*Modern Cryptography*. Berlin: Springer-Verlag, 2021: 373-383.

[2] Peyrin T, Wang H. The Malicious framework: Embedding backdoors into tweakable block ciphers[C]// *Proc Annual International Cryptology Conference*. Berlin: Springer-Verlag, 2020: 249-278.

[3] Dauterman E, Corrigan-Gibbs H, Mazi`eres D, *et al*. True2F:Backdoor-resistant authentication tokens [C]// 2019 *IEEE Symposium on Security and Privacy* (SP). Washington D C: IEEE, 2019: 398-416.

[4] Ball J, Borger J, Greenwald G. Revealed: How US and UK spy agencies defeat internet privacy and security[J]. *The Guardian*, 2013, **ED-6**: 2-8.

[5] Bernstein D J, Lange T, Niederhagen R. Dual EC: A standardized back door[J]. *The New Codebreakers-Volume* 9100, 2015: 256-281. DOI: https://doi.org/10.1007/978-3-662-49301-4_17.

[6] Bellare M, Paterson K G, Rogaway P. Security of symmetric encryption against mass surveillance [C] // *Advances in Cryptology*, *CRYPTO* 2014. Berlin:Springer-Verlag, 2014: 1-19.

[7] Ateniese G, Magri B, Venturi D. Subversion-resilient signature schemes [C]// *Proceedings of the* 22*nd ACM SIGSAC Conference on Computer and Communications Security*, New York: ACM, 2015: 364-375.

[8] Liu C, Chen R, Wang Y, *et al*. Asymmetric subversion attacks on signature schemes [C]// *Australasian Conference on Information Security and Privacy*. Berlin: Springer-Verlag, 2018: 376-395.

[9] Baek J, Susilo W, Kim J, *et al*. Subversion in practice: How to efficiently undermine signatures [C]// *IEEE Access*, 2019: 376-395.

[10] Catalano D, Fuchsbauer G, Soleimanian A. Double-authentication-preventing signatures in the standard model [C]// *International Conference on Security and Cryptography for Networks*. Berlin: Springer-Verlag, 2020: 338-358.

[11] Poettering B, Stebila D. Double-authentication-preventing signatures [C]// *ESORICS*. Berlin: Springer-Verlag, 2014: 1-22.

[12] Boneh D, Kim S, Nikolaenko V. Lattice-based DAPS and

generalizations: Self-enforcement in signature schemes [C]// *International Conference on Applied Cryptography and Network Security*. Berlin: Springer-Verlag, 2017: 457-477.

[13] Poettering B, Stebila D. Short double- and *n*-times-authenticationpreventing signatures from ECDSA and more [C]// 2018 *IEEE European Symposium on Security and Privacy* (EuroS&P). Washington D C: IEEE Press, 2018: 273-287.

[14] Poettering B. Shorter double-authentication preventing signatures for small address spaces [C]//*International Conference on Cryptology in Africa*, *AFRICACRYPT* 2018. *Lecture Notes in Computer Science*. Berlin: Springer-Verlag, 2018: 344-361.

[15] Derler D, Ramacher S, Slamanig D. Generic double-authentication preventing signatures and a post-quantum instantiation [C]// *International Conference on Cryptology in Africa*. Berlin:Springer-Verlag, 2018: 258-276.

[16] Liu J H, Yu Y, Jia J, *et al*. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks [J]. *Tsinghua Science and Technology*, 2019, **24**(5): 575-584.

[17] Lyubashevsky V. Lattice signatures without trapdoors [C]// *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Berlin: Springer-Verlag, 2012: 738-755.

[18] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer [J]. *SIAM Review*, 1999, **41**(2): 303-332.

[19] Ajtai M. Generating hard instances of lattice problems [C]// *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. New York: ACM, 1996: 99-108.

[20] Ducas L, Durmus A, Lepoint T, *et al*. Lattice signatures and bimodal Gaussians [C]// *Annual Cryptology Conference*. Berlin: Springer-Verlag, 2013: 40-56.

[21] Güneysu T, Lyubashevsky V, Pöppelmann T, *et al*. Practical latticebased cryptography: A signature scheme for embedded systems [C]// *International Workshop on Cryptographic Hardware and Embedded Systems*, *ACM Transactions on Embedded Computter Systems*. New York: ACM, 2012: 530-547.

[22] Hoffstein J, Pipher J, Schanck J M, *et al*. Practical signatures from the partial Fourier recovery problem [C]//*International Conference on Applied Cryptography and Network Security*. Berlin: Springer-Verlag, 2014: 476-493.

[23] Akleylek S, Bindel N, Buchmann J, *et al*. An efficient lattice based signature scheme with provably secure instantiation [C]// *International Conference on Cryptology in Africa*. Berlin: Springer-Verlag, 2016: 44-60.

[24] Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems [C]//*Annual International Cryptology Conference*. Berlin: Springer-Verlag, 1997: 112-131.

[25] Hoffstein J, Howgrave-Graham N, Pipher J, *et al*. Digital signatures using the NTRU lattice [C]//*Cryptographers Track RSA Conference*. Berlin: Springer-Verlag, 2003: 122-140.

[26] Espitau T, Fouque P A, Gerard B, *et al*. Loop-abort faults on lattice based signature schemes and key exchange protocols [J]. *IEEE Transactions on Computers*, 2018, **67**(11): 1535-1549.

[27] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings [J] . *Journal of the ACM*, 2013, **60** (6): 1-34.

[28] Bert P, Fouque P A, Roux-Langlois A, *et al*. Practical implementation of ring-SIS/LWE based signature and IBE [C]//*International Conference on Post-Quantum Cryptography*. Berlin: Springer-Verlag, 2018: 271-291.

[29] Bai S, Galbraith S D. An improved compression technique for signatures based on learning with errors [C]// *Cryptographers' Track at the RSA Conference*. Berlin: Springer-Verlag, 2014: 28-47.

[30] Ducas L, Kiltz E, Lepoint T, *et al*. Crystals-dilithium: A lattice-based digital signature scheme [C]//*IACR Transactions on Cryptographic Hardware and Embedded Systems*, *A Lattice-Based Digital Signature Scheme*. New York: IACR, 2018: 238-268.

[31] Chopra A. GLYPH: A new insantiation of the GLP digital signature scheme [C]// *IACR Cryptology ePrint Archive*. New York: IACR, 2017: 1-14.

[32] Ducas L. Accelerating Bliss: The geometry of ternary polynomials[C]// *IACR Cryptology ePrint Archive*. New York: IACR, 2014: 1-12.

[33] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions [C]// *Proceedings of the* 40*th Annual ACM Symposium on Theory of Computing*. New York: ACM Press, 2008: 17-20.

□