On Multi-user Security of Lattice-based Signature under Adaptive Corruptions and Key Leakages

Masayuki Fukumitsu[1][0000−0001−7471−4477] and Shingo Hasegawa[2][0000−0001−9715−5495]

[1] University of Nagasaki, Nagayo, 851-2195 Japan
fukumitsu@sun.ac.jp
[2] Fukushima University, Fukushima, 960-1296 Japan
hasegawa@sss.fukushima-u.ac.jp

Abstract. We consider the multi-user security under the adaptive corruptions and key leakages ($\mathrm{MU}^{\mathrm{c\&l}}$ security) for lattice-based signatures. Although there exists an $\mathrm{MU}^{\mathrm{c\&l}}$ secure signature based on a number-theoretic assumption, or a leakage-resilient lattice-based signature in the single-user setting, $\mathrm{MU}^{\mathrm{c\&l}}$ secure lattice-based signature is not known.
We examine the existing lattice-based signature schemes from the viewpoint of $\mathrm{MU}^{\mathrm{c\&l}}$ security, and find that the security of the Lyubashevsky's signature, which is proven to have the ordinary single-user security only, can be extended to the multi-user security even if we take the adaptive corruptions and the key leakages into account.
Our security proof in the multi-user setting makes use of the feature of the SIS problem so that a SIS instance is set to the public parameter and a reduction algorithm can set a public key with a secret key in order to answer a corruption query. We also show that the entropy of the secret key is kept under the bounded leakage with a high probability and then the leakage resilience of signature holds.

Keywords: Lattice signature · Multi-user setting · Adaptive corruptions · Leakage resilience

1 Introduction

The signature scheme is a fundamental cryptographic primitive that enables a signer to prove the authenticity of a message. The security of the signature is widely studied. The most basic notion is the existential unforgeability against the chosen message attack (EUF-CMA)[11] in which an adversary cannot generate a forgery even if it can obtain polynomially many pairs of a message and a signature. The original definition of EUF-CMA [11] considers the *single-user setting*, the adversary is required to attack the signature with respect to a given challenge public key. However, the adversary can see many public keys in the real world, and it is sufficient that the adversary produces a forgery with respect to one of the public keys the adversary obtains. This situation is captured as the security in the *multi-user setting*.

The formal security of signatures in the multi-user setting is also studied. [9] showed a generic reduction from EUF-CMA, the security in the single-user setting, to the multi-user existential unforgeability against the chosen message attack (MU-EUF-CMA). However, the reduction is *loose* because it suffers the security loss depending on the number of users. Kiltz, Masny and Pan [17] clarified the relationship among security notions of the signature with respect to both the single-user setting and the multi-user setting. They showed the *tight* security reduction from EUF-CMA to MU-EUF-CMA in the random oracle model (ROM) [5], namely the security loss is independent of the number of users. Their reduction employs the random-self-reducibility (RSR).

When we consider the security in the multi-user setting, we should take into account the *corruption* of users unlike the single-user setting. Namely the adversary can obtain secret keys of users that the adversary designates adaptively, and can use them on generating a forgery with respect to a public key of an uncorrupted user. Such an attack and security is captured as the multi-user security under *the adaptive corruptions*. For signature schemes, this security notion is defined as the MU-EUF-CMA security under the adaptive corruptions (MU^{c}-EUF-CMA). The signature schemes having MU^{c}-EUF-CMA security are studied in the literature [2,10,7,12,21,13,14].

The multi-user security under the adaptive corruptions divides users into two types: corrupted users whose secret is fully revealed to the adversary and uncorrupted users whose secret is completely hidden. As the *intermediate* users, we can consider users whose secret information is *partially leaked*. This situation is captured by the multi-user security under the adaptive corruptions and *key leakages*.

Table 1. Comparison of properties among the known MU^{c}-EUF-CMA secure signature schemes

	Security	Model	Tightness	Instantiations
[2]	MU^{c}-EUF-CMA	Standard	✓	Matrix DDH
[10]	MU^{c}-EUF-CMA	ROM	✓	DDH
[7]	strong MU^{c}-EUF-CMA	ROM	✓	DDH, ϕ-Hiding
[12]	MU^{c}-EUF-CMA	Standard		Matrix DDH
[21]	MU^{c}-EUF-CMA	ROM	✓	DDH, ϕ-Hiding, dCSIDH, Multi-Secret-LWE, LWE
[14]	strong MU^{c}-EUF-CMA	Standard	almost	Multi-Secret-LWE+SIS
[13]	strong MU$^{c\&l}$-EUF-CMA	Standard	almost	Matrix DDH
[ours]	MU$^{c\&l}$-EUF-CMA	ROM		ℓ_2-SIS

Recently MU-EUF-CMA security under the adaptive corruptions and key leakages (MU$^{c\&l}$-EUF-CMA) is introduced with a concrete instantiation [13]. In [13], an almost tightly MU$^{c\&l}$-EUF-CMA secure signature scheme is proposed. The scheme is constructed based on the MDDH assumption [8] and its MU$^{c\&l}$-EUF-CMA security is proven in the standard model. On the other hand, there are signature schemes [7,21,14] based on cryptographic assumptions other than the MDDH assumption if we consider the MU^{c}-EUF-CMA security (namely without key leakage) only. Especially, the post-quantum constructions [21,14] exist based on lattice assumptions. However, only the signature scheme in [13] is the example of MU$^{c\&l}$-EUF-CMA secure signature and a post-quantum construction is not known. We summarize the explanation of the known MU^{c}-EUF-CMA secure signature schemes in Tab. 1.

1.1 Our Contribution

In this paper, we aim to construct a lattice-based MU$^{c\&l}$-EUF-CMA secure signature, which remains open as described above. The MU$^{c\&l}$-EUF-CMA secure signature of [13] is based on the publicly-verifiable quasi-adaptive hash proof system (PV-QA-HPS), which is a new primitive introduced in [13], and the quasi-adaptive non-interactive zero-knowledge proof (QA-NIZK) [15]. It is natural to consider a lattice-based PV-QA-HPS and then to apply the framework of [13] to it. However, it seems difficult to construct a PV-QA-HPS from a lattice assumption because a lattice-based construction does not satisfy the exact correctness [14] due to the noise arising in a lattice problem. One solution to address the problem is relaxing the requirement concerning the exact correctness. In fact, the probabilistic QA-HPS is proposed in [14] which is a variant of QA-HPS relaxing the correctness, and a lattice-based MU^{c}-EUF-CMA secure signature is constructed based on a probabilistic QA-HPS. The signature scheme satisfies the almost tight security in the standard model, however, it does not have the leakage resilience. Thus we take another approach to construct a lattice-based MU$^{c\&l}$-EUF-CMA secure signature. We directly consider whether or not the existing lattice-based signature schemes have the multi-user security under the adaptive corruptions and key leakages. Fortunately, we find that the security of the signature scheme by [20], denoted as Lyu, can be extended to the multi-user security even if we take the adaptive corruptions and the key leakages into account. We briefly describe the reason why our security proof works.

In [20], the ordinary EUF-CMA security (in the single-user setting) is proven in the ROM under the short integer solution (SIS) assumption. On a given SIS instance matrix $\boldsymbol{A} \in \mathbb{Z}_p^{n \times m}$ of row size n and column size m, the security reduction $\mathcal{R}$ constructed in [20] samples a secret key $\boldsymbol{S} \in \mathbb{Z}_p^{m \times \tilde{m}}$ of Lyu with small norm, and generates the corresponding public key $\boldsymbol{T} \leftarrow \boldsymbol{AS}$. Then, $\mathcal{R}$ invokes an adversary $\mathcal{A}$ against the EUF-CMA of Lyu twice to obtain pairs (μ, σ) and (μ', σ') of a message and a signature. By utilizing these pairs and the forking lemma [4], $\mathcal{R}$ finds a non-zero short vector $\boldsymbol{v}$ such that $\boldsymbol{Av} = \boldsymbol{0}$. The proof that $\boldsymbol{v}$ is non-zero proceeds by two facts (i) and (ii). The fact (i) states that there exist at least two secret keys $\boldsymbol{S}, \tilde{\boldsymbol{S}}$ of the challenge public key $\boldsymbol{T} = \boldsymbol{AS} = \boldsymbol{A}\tilde{\boldsymbol{S}}$ with overwhelming probability. This fact is used to guarantee that for the valid signatures σ and σ' under the public key $\boldsymbol{T}$, at least one of $\boldsymbol{S}$ and $\tilde{\boldsymbol{S}}$ induces that $\boldsymbol{v}$ is a non-zero vector. The fact (ii) states the upper bound for $\mathcal{A}$'s advantage to recognize which of $\boldsymbol{S}$ and $\boldsymbol{S}'$ is selected only from the challenge public key $\boldsymbol{T}$ during the EUF-CMA game. Namely, $\mathcal{A}$ can determine which of $\boldsymbol{S}$ and $\boldsymbol{S}'$ is used with at most $1/2 + \mathsf{negl}$. In particular, the latter result is proven by simulating the singing oracle without the secret key $\boldsymbol{S}$ and utilizing the honest-verifier zero-knowledge property and the random oracle.

On extending the security reduction $\mathcal{R}$ to the MU$^{c\&l}$-EUF-CMA case, the key observation is that $\mathcal{R}$ can select the challenge secret and public key pair by itself. Since a given SIS instance $\boldsymbol{A}$ is set to the

public parameter, not the public key, $\mathcal{R}$ can generate secret keys of all users with corresponding public keys including the challenge secret and public key during the game, and $\mathcal{R}$ can naturally respond to any corrupting oracle query and any leakage oracle query by $\mathcal{A}$. Moreover, this feature helps us to prove the fact (ii) above under our situation where the corrupting oracle and the leakage oracle are provided to $\mathcal{A}$. In the security proof, $\mathcal{R}$ samples secret keys $\{\boldsymbol{S}_k\}_k$ for all K users independently and uniformly at random. The independent sampling implies that the information about secret keys of the other users is useless even when $\mathcal{A}$ can obtain these other secret keys from the corrupting oracle. In other words, we do not need to consider the impact of the corruption of other users. Then we can proceed to the proof in the same way as the single-user security and it means that the security loss can be independent of the number K of users. We eventually show the fact (ii) under the condition that some bits of the secret key $\boldsymbol{S}_{k^*}$ are given to $\mathcal{A}$, where k^* indicates the target user. We evaluate the probability that the entropy of the challenge secret key $\boldsymbol{S}_{k^*}$ becomes 0 due to the leakage information. We can show that such a probability can be negligible by selecting parameters appropriately. Concretely, the probability that the conditional entropy is to be 0 can be $2^{-\rho}$ by setting ρ so that $\frac{\rho+n\bar{m}\log_2 p}{2L} = o(1)$ for the length L of the secret key. This implies that Lyu is MU$^{\text{c\&l}}$-EUF-CMA secure under the leakage of $(1/2 - o(1))L$ bits of $\boldsymbol{S}_{k^*}$. Note that [18] discussed the (single-user) EUF-CMA of Lyu with key leakage, however they did not give the details of parameter constraints.

We finally note the signing oracle simulation in the security proof. Concerning the simulation of the signing oracle, [3,6] pointed out the incompleteness of the security proofs for most of the lattice-based Fiat-Shamir signatures, including [20]. More precisely, such security proofs did not consider simulating the singing oracle when it fails to respond to a query. To fix the incompleteness, they proposed a method to simulate this failure case by employing the leftover hash lemma. We also evaluate the parameters that make their method applicable to our case. Overall, the parameter settings are given in Tab. 2.

1.2 Related Works and Open Problems

There exist leakage resilient lattice-based signatures in the single-user setting [18]. [18] showed EUF-CMA security under the key leakage for two lattice-based signature schemes which are based on the SIS assumption and the LWE assumption, respectively. The SIS-based scheme is essentially the same as the scheme of [20] and has a non-tight reduction in the ROM as well as ours. Since we show the MU$^{\text{c\&l}}$-EUF-CMA security for the signature scheme, our result is just an extension of the SIS-based scheme of [18] with the evaluation of the parameters.

In [18], the LWE-based scheme is also considered. They claimed the tight EUF-CMA security under the key leakage for the scheme based on the leakage resilient lossy (LRlossy) ID scheme which is defined as a variant of the lossy ID scheme [1]. Although their LWE-based scheme achieves the tight security, it seems difficult to prove the multi-user security immediately. In the key generation of their scheme, an LWE instance $(\boldsymbol{A}, \boldsymbol{T})$ is set as the public key, whereas a SIS instance $\boldsymbol{A}$ is merely set as the public parameter in Lyu. This suggests that our key observation explained above cannot be directly applied to their LWE scheme. Thus an LWE-based MU$^{\text{c\&l}}$-EUF-CMA signature remains open.

In [14], an LWE-based signature scheme, which is almost tightly MU$^{\text{c}}$-EUF-CMA secure, is proposed. Their signature scheme does not have the leakage resilience since the building block probabilistic QA-HPS does not have the exact correctness and then the framework of [13] cannot be applied to it. A new variant of QA-HPS with the exact correctness which can be instantiated from the LWE assumption in order to achieve a leakage-resilient signature from the LWE assumption is also an interesting open problem.

2 Preliminaries

$\mathbb{N}$, $\mathbb{P}$, $\mathbb{Z}$ and $\mathbb{R}$ denote the sets of the natural numbers, the primes, the integers and the reals, respectively. For any integers $a \leq b$, we denote by $[a, b] \subseteq \mathbb{Z}$ the subset of integers x such that $a \leq x \leq b$. In particular, $[1, b]$ is simply represented by $[b]$. We set $\mathbb{Z}_{|d|} = [-d, d]$ for $d \in \mathbb{N}$.

For any probability distribution D over a set X, $x \leftarrow\!\$\, D$ means that $x \in X$ is chosen according to D. When D is the uniform distribution over a finite set X, $x \leftarrow\!\$\, D$ is simply represented by $x \leftarrow\!\$\, X$. $|a|$ stands for the absolute value of a real $a \in \mathbb{R}$, $|X|$ stands for the cardinality of a set X, and $|s|$ stands for the length of a string $s \in \{0,1\}^*$. We say that a function ϵ on $\lambda \in \mathbb{N}$ is negligible if for any polynomial ν, there exists a natural number $\lambda_0 \in \mathbb{N}$ such that for any $\lambda \geq \lambda_0$, it holds that $\epsilon(\lambda) \leq 1/\nu(\lambda)$. The notation **w/ prob.** is abbreviated from "with probability". PPT is abbreviated from probabilistic polynomial-time.

2.1 Lattices

For any $p \in \mathbb{P}$, let $\mathbb{Z}_p$ be the residue ring modulo p. We represent all the elements in $\mathbb{Z}_p$ by using $\mathbb{Z}_{|(p-1)/2|}$. For any $\boldsymbol{x} = \begin{bmatrix} x_1 & \cdots & x_n \end{bmatrix}^T \in \mathbb{Z}_p^n$, the ℓ_1-norm $\|\boldsymbol{x}\|_1$ and the ℓ_2-norm $\|\boldsymbol{x}\|$ are expressed as $\|\boldsymbol{x}\|_1 = \sum_{i=1}^n |x_i|$ and $\|\boldsymbol{x}\| = \sqrt{\sum_{i=1}^n |x_i|^2}$.

Discrete Gaussian distribution The Gaussian distribution centered by $\boldsymbol{v} \in \mathbb{R}^m$ with the standard deviation s is defined by $\mathfrak{N}_{\boldsymbol{v},s}^m(\boldsymbol{x}) = (\frac{1}{\sqrt{2\pi s^2}})^m e^{-\frac{\|\boldsymbol{x}-\boldsymbol{v}\|^2}{2s^2}}$ for any $\boldsymbol{x} \in \mathbb{R}^m$. In particular, when $\boldsymbol{v} = \boldsymbol{0}$, $\mathfrak{N}_{\boldsymbol{v},s}^m$ is denoted by $\mathfrak{N}_s^m$. The discrete Gaussian distribution centered by $\boldsymbol{v} \in \mathbb{Z}^m$ with the standard deviation s is given by $\mathfrak{D}_{\boldsymbol{v},s}^m(\boldsymbol{x}) = \mathfrak{N}_{\boldsymbol{v},s}^m(\boldsymbol{x})/\mathfrak{N}_s^m(\mathbb{Z}^m)$ for any $\boldsymbol{x} \in \mathbb{Z}^m$, where $\mathfrak{N}_s^m(\mathbb{Z}^m) = \sum_{\boldsymbol{x}\in\mathbb{Z}^m} \mathfrak{N}_s^m(\boldsymbol{x})$. For the discrete Gaussian distribution, the following lemma holds.

Lemma 1 ([19, Lemma 4.4 (2)]). *For any vector $\boldsymbol{z} \in \mathbb{Z}^m$ and any real number $s \geq 3/\sqrt{2\pi}$, it holds that $\mathfrak{D}_s^m(\boldsymbol{z}) \leq 2^{-m}$.*

Rejection sampling We recap the rejection sampling [19]. For our purpose, we give a generalized variant. More specifically, the error probability considered in [19] was set concretely as 2^{-100}, whereas we treat this probability generally by involving new parameters. Therefore, we first prepare the following auxiliary lemmas.

Lemma 2 ([19, Lemma 4.3]). *For any $\boldsymbol{v} \in \mathbb{R}^m$, and any $s, r > 0$, we have*

$$\Pr_{\boldsymbol{z} \leftarrow\$ \mathfrak{D}_s^m}[|\langle \boldsymbol{z}, \boldsymbol{v}\rangle| > r] < 2e^{-\frac{r^2}{2\|\boldsymbol{v}\|^2 s^2}}.$$

Employing Lemma 2, we generalize [19, Lemma 4.5] in the following way.

Lemma 3. *For any $\boldsymbol{v} \in \mathbb{Z}^m$, for any positive α, α', if $s = \alpha\|\boldsymbol{v}\|$, then we have*

$$\Pr_{\boldsymbol{z} \leftarrow\$ \mathfrak{D}_s^m}\left[\frac{\mathfrak{D}_s^m(\boldsymbol{z})}{\mathfrak{D}_{\boldsymbol{v},s}^m(\boldsymbol{z})} \leq \exp\left(\frac{\sqrt{2\alpha'}}{\alpha} + \frac{1}{2\alpha^2}\right)\right] > 1 - 2e^{-\alpha'}.$$

Proof. We can obtain the following formula as in the proof of [19, Lemma 4.5].

$$\frac{\mathfrak{D}_s^m(\boldsymbol{z})}{\mathfrak{D}_{\boldsymbol{v},s}^m(\boldsymbol{z})} = \exp\left(\frac{-2\langle \boldsymbol{z}, \boldsymbol{v}\rangle + \|\boldsymbol{v}\|^2}{2s^2}\right).$$

Applying Lemma 2 to the case where $r = \sqrt{2\alpha'}\|\boldsymbol{v}\|s$, The probability that $|\langle \boldsymbol{z}, \boldsymbol{v}\rangle| \leq \sqrt{2\alpha'}\|\boldsymbol{v}\|s$ is at least $1 - 2e^{-\alpha'}$. Under the condition that $|\langle \boldsymbol{z}, \boldsymbol{v}\rangle| \leq \sqrt{2\alpha'}\|\boldsymbol{v}\|s$, it holds that

$$\begin{aligned}
\frac{\mathfrak{D}_s^m(\boldsymbol{z})}{\mathfrak{D}_{\boldsymbol{v},s}^m(\boldsymbol{z})} &= \exp\left(\frac{-2\langle \boldsymbol{z}, \boldsymbol{v}\rangle + \|\boldsymbol{v}\|^2}{2s^2}\right) \\
&\leq \exp\left(\frac{2\sqrt{2\alpha'}\|\boldsymbol{v}\|s + \|\boldsymbol{v}\|^2}{2s^2}\right) \\
&= \exp\left(\frac{2\sqrt{2\alpha'}\|\boldsymbol{v}\|s}{2s^2} + \frac{\|\boldsymbol{v}\|^2}{2s^2}\right) \\
&= \exp\left(\frac{\sqrt{2\alpha'}\|\boldsymbol{v}\|}{s} + \frac{\|\boldsymbol{v}\|^2}{2s^2}\right) \\
&= \exp\left(\frac{\sqrt{2\alpha'}\|\boldsymbol{v}\|}{\alpha\|\boldsymbol{v}\|} + \frac{\|\boldsymbol{v}\|^2}{2(\alpha\|\boldsymbol{v}\|)^2}\right) \\
&= \exp\left(\frac{\sqrt{2\alpha'}}{\alpha} + \frac{1}{2\alpha^2}\right).
\end{aligned}$$

□

Lemma 4 (Core of Rejection Sampling [19, Lemma 4.7]). *For any set V, let $h : V \to \mathbb{R}$ and $f : \mathbb{Z}^m \to \mathbb{R}$ be probability distributions. Let $\{g_v : \mathbb{Z}^m \to \mathbb{R} \mid v \in V\}$ be a family of probability distributions. Assume that there exist a non-negative function $\epsilon : \mathbb{N} \to \mathbb{R}$ and a constant $M \in \mathbb{R}$ such that for any $v \in V$,*

$$\Pr_{z \leftarrow\$ f}[M \cdot g_v(z) \geq f(z)] \geq 1 - \epsilon.$$

Then the followings hold for the following algorithms $\overline{\mathsf{Real}}$ and $\overline{\mathsf{Ideal}}$:

- *the statistical distance between the outputs of* Real *and* Ideal *is at most ϵ/M; and*
- *the probability that $\overline{\mathsf{Real}}$ outputs (z, v) is at least $(1 - \epsilon)/M$.*

$\overline{\mathsf{Real}}$	$\overline{\mathsf{Ideal}}$
$v \leftarrow\$ h$	$v \leftarrow\$ h$
$z \leftarrow\$ g_v$	$z \leftarrow\$ f$
w/prob. $\min\left\{\frac{f(z)}{Mg_v(z)}, 1\right\}$:	**w/prob.** $\frac{1}{M}$:
return (z, v)	**return** (z, v)

From Lemma 4, we generalize the rejection sampling of [20, Theorem 3.4] as follows.

Lemma 5 (Rejection Sampling). *Let $T, \alpha, \alpha' \in \mathbb{R}$, and let $s = \alpha T$. We denote by h a probability distribution over $\mathbb{Z}^m_{|T|}$. We introduce the two algorithms* Real *and* Ideal *in Fig. 1. For $M = \exp(\sqrt{2\alpha'}/\alpha + 1/(2\alpha^2))$, the followings hold:*

- *the statistical distance between the outputs of* Real *and* Ideal *is at most $2e^{-\alpha'}/M$; and*
- Real *successfully returns $(\boldsymbol{v}, \boldsymbol{z})$ with probability at least $1/M - 2e^{-\alpha'}/M$.*

Proof. We set $f = \mathfrak{D}^m_s$ and $g_v = \mathfrak{D}^m_{\boldsymbol{v},s}$. Lemma 3 implies that for any $\boldsymbol{z} \leftarrow\$ \mathfrak{D}^m_s$

$$\Pr_{\boldsymbol{z} \leftarrow\$ \mathfrak{D}^m_s}\left[\frac{f(\boldsymbol{z})}{g_v(\boldsymbol{z})} \leq \exp\left(\frac{\sqrt{2\alpha'}}{\alpha} + \frac{1}{2\alpha^2}\right)\right] > 1 - 2e^{-\alpha'}.$$

Applying Lemma 4 to $f = \mathfrak{D}^m_s$, $g_v = \mathfrak{D}^m_{\boldsymbol{v},s}$ $\epsilon = 2e^{-\alpha'}$ and $M = \exp(\sqrt{2\alpha'}/\alpha + 1/(2\alpha^2))$, we can obtain our lemma. □

ℓ_2-Short integer solution (ℓ_2-SIS) assumption [20] Let $p \in \mathbb{P}$, and let $n, m, \zeta \in \mathbb{N}$. ℓ_2-$\mathsf{SIS}_{p,n,m,\zeta}$ *problem* asks for finding a non-zero vector $\boldsymbol{v} \in \mathbb{Z}^m_p$ such that $\|\boldsymbol{v}\| \leq \zeta$ and $\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0}$ for a given random matrix $\boldsymbol{A} \leftarrow\$ \mathbb{Z}^{n \times m}_p$. $(T_{\mathsf{SIS}}, \epsilon_{\mathsf{SIS}})$-$\ell_2$-$\mathsf{SIS}_{p,n,m,\zeta}$ *assumption* states that for any probabilistic algorithm $\mathcal{A}$, which runs in time T_{SIS}, $\mathcal{A}$ solves the ℓ_2-$\mathsf{SIS}_{p,n,m,\zeta}$ problem with probability at most ϵ_{SIS}.

For solving the ℓ_2-$\mathsf{SIS}_{p,n,m,\zeta}$ problem, we assume as in [20] that $\boldsymbol{A}$ is represented as the Hermite Normal Form. Namely, $\boldsymbol{A}$ is of the form $\boldsymbol{A} = \left[\overline{\boldsymbol{A}}\ \boldsymbol{I}\right]$.

Real	Ideal
$\boldsymbol{v} \leftarrow\$ h$	$\boldsymbol{v} \leftarrow\$ h$
$\boldsymbol{z} \leftarrow\$ \mathfrak{D}^m_{\boldsymbol{v},s}$	$\boldsymbol{z} \leftarrow\$ \mathfrak{D}^m_s$
w/ prob. $\min\left\{\frac{\mathfrak{D}^m_s(\boldsymbol{z})}{M\mathfrak{D}^m_{\boldsymbol{v},s}(\boldsymbol{z})}, 1\right\}$:	**w/ prob.** $\frac{1}{M}$:
return $(\boldsymbol{v}, \boldsymbol{z})$	**return** $(\boldsymbol{v}, \boldsymbol{z})$

Fig. 1. Algorithms Real and Ideal for rejection sampling

2.2 Entropy

The min-entropy of a random variable X is defined by

$$H_\infty(X) = \min_{x \in \{0,1\}^n} \{-\log_2 \Pr[X = x]\}.$$

The min-entropy of X under a condition that an event E happens is given by

$$H_\infty(X \mid E) = \min_{x \in \{0,1\}^n} \{-\log_2 \Pr[X = x \mid E]\}.$$

We employ the following lemma.

Lemma 6 ([16, Lemma 1]). *Let X be a random variable of min-entropy H, and let $\Delta \in [0, H]$. Let $f : \{0,1\}^* \to \{0,1\}^\gamma$ be a function. We set that $Y = \{y \in \{0,1\}^\gamma \mid H_\infty(X \mid y = f(X)) \leq H - \Delta\}$. Then, it holds that*

$$\Pr[f(X) \in Y] \leq 2^{\gamma - \Delta}.$$

A family $\mathsf{F} = \{f : Y \to W\}$ of hash functions is said to be 2-*universal* if for any $y, y' \in Y$ satisfying that $y \neq y'$, we have

$$\Pr_{f \leftarrow\!\$ \mathsf{F}}[f(y) = f(y')] \leq \frac{1}{|W|}.$$

As in [6], we use the following 2-universal family.

Lemma 7 ([6]). *Let $p \in \mathbb{P}$ and let $n, m \in \mathbb{N}$. A family $\left\{f_{\boldsymbol{A}} : \mathbb{Z}_p^m \to \mathbb{Z}_p^n \mid f_{\boldsymbol{A}}(\boldsymbol{y}) = \boldsymbol{A}\boldsymbol{y}\right\}$ parameterized by $\boldsymbol{A} \in \mathbb{Z}_p^{n \times m}$ is 2-universal.*

Then, the leftover hash lemma is given as follows.

Lemma 8 (Leftover Hash Lemma [6]). *Let $\{f : Y \to W\}$ be a family of 2-universal hash functions, let Z be a random variable over the set Y, and let $\epsilon > 0$ be a real. If $H_\infty(Z) \geq |W| + 2\log\frac{1}{\epsilon}$, then the statistical distance between the following two distributions is at most ϵ.*

- *$(f, f(y))$: $f \leftarrow\!\$ \{f : Y \to W\}$, $y \leftarrow\!\$ D_Z$, where D_Z is the probability distribution of Z;*
- *(f, w): $f \leftarrow\!\$ \{f : Y \to W\}$, $w \leftarrow\!\$ W$.*

2.3 General Forking Lemma

We now recap the (general) forking lemma formalized in [4]. Let $Q \in \mathbb{N}$ and let C be a finite set whose size is at least 2. Consider a PPT instance generator IGen that returns a randomly chosen instance $x \in \{0,1\}^*$ on a given security parameter 1^λ, and a PPT algorithm $\mathcal{C}$ that returns a pair $(I, y) \in [0, Q] \times \{0,1\}^*$ of a number I and a string y on a given pair $(x, \{h_q\}_{q \in [Q]})$ of an instance x and values $h_1, h_2, \ldots, h_Q \in C$. We define the probability acc as follows:

$$\mathsf{acc} = \Pr\Big[I \geq 1 \mid x \leftarrow\!\$ \mathsf{IGen}(1^\lambda);\ h_1, \ldots, h_Q \leftarrow\!\$ C;\ (I, y) \leftarrow\!\$ \mathcal{C}(x, \{h_q\}_{q \in [Q]})\Big]. \tag{1}$$

$\mathcal{F}_{\mathcal{C}}(x)$

$\omega \leftarrow\!\$ \{0,1\}^\lambda$
$h_1, \ldots, h_Q \leftarrow\!\$ C$
$(I, y) \leftarrow\!\$ \mathcal{C}(x, \{h_q\}_{q \in [1,Q]}; \omega)$
return $(0, \epsilon, \epsilon)$ **if** $I = 0$
$h'_I, \ldots, h'_Q \leftarrow\!\$ C$
$(I', y') \leftarrow\!\$ \mathcal{C}(x, \{h_q\}_{q \in [1, I-1]} \cup \{h'_q\}_{q \in [I,Q]}; \omega)$
return $(0, \epsilon, \epsilon)$ **if** $I \neq I' \vee h_I = h'_I$
return $(1, y, y')$

Fig. 2. An algorithm $\mathcal{F}$ for forking lemma involving $\mathcal{C}$

$\mathsf{Game}^{\mathsf{MU}^{\mathsf{c\&l}}\text{-}\mathsf{EUF\text{-}CMA}}_{\mathcal{A},K,\iota}(1^\lambda)$

$\mathsf{pp} \leftarrow\!\!\$\ \mathsf{Pgen}(1^\lambda)$
$\mathfrak{L}_s \leftarrow \emptyset;\ \mathfrak{L}_c \leftarrow \emptyset;\ l \leftarrow 0$
for $k \in [K]$:
  $(\mathsf{sk}_k, \mathsf{pk}_k) \leftarrow\!\!\$\ \mathsf{KGen}(\mathsf{pp})$
$(k^*, \mu^*, \sigma^*) \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{O}_c, \mathsf{O}_l, \mathsf{O}_s}(\mathsf{pp}, \{\mathsf{pk}_k\}_{k\in[K]})$
return 0 **if** $\mathsf{pk}_{k^*} \in \mathfrak{L}_c \vee (k^*, \mu^*) \in \mathfrak{L}_s \vee \mathsf{Vf}(\mathsf{pp}, \mathsf{pk}_{k^*}, \mu^*, \sigma^*) = 0$
return 1

$\mathsf{O}_s(k, \mu)$
$\sigma \leftarrow\!\!\$\ \mathsf{Sign}(\mathsf{pp}, \mathsf{sk}_k, \mu)$
$\mathfrak{L}_s \leftarrow \mathfrak{L}_s \cup \{(k, \mu)\}$
return σ

$\mathsf{O}_c(k)$
$\mathfrak{L}_c \leftarrow \mathfrak{L}_c \cup \{k\}$
return sk_k

$\mathsf{O}_l(k, f)$
return $\perp$ **if** $l + |f(\mathsf{sk}_k)| > \iota$
$l \leftarrow l + |f(\mathsf{sk}_k)|$
return $f(\mathsf{sk}_k)$

Fig. 3. $\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA game

We also formalize a PPT algorithm $\mathcal{F}_\mathcal{C}$ given in Fig. 2, called the forking algorithm, and the related probability frk in the following way:

$$\mathsf{frk} = \Pr\big[b = 1 \mid x \leftarrow\!\!\$\ \mathsf{IGen}(1^\lambda);\ (b, y, y') \leftarrow\!\!\$\ \mathcal{F}_\mathcal{C}(x)\big].$$

Lemma 9 (General Foking Lemma [4, Lemma 1]). *For the relationship between the probabilities* acc *and* frk *formalized above, it holds that*

$$\mathsf{frk} \geq \mathsf{acc} \cdot \left(\frac{\mathsf{acc}}{Q} - \frac{1}{|C|}\right). \tag{2}$$

2.4 Digital Signature

Syntax A *digital signature* DS consists of the following four algorithms:

Pgen It takes a security parameter 1^λ as input, and returns a public parameter pp.
KGen It takes a public parameter pp as input, and returns a secret key and a public key $(\mathsf{sk}, \mathsf{pk})$.
Sig It takes a secret key sk and a message μ as input, and returns a signature σ.
Vf It takes a public key pk, a message μ and a signature σ as input, and returns 1 if σ is valid with respect to (pk, μ) or 0 otherwise.

Correctness The correctness of DS is defined as follows: for any security parameter λ and any message μ, when $\mathsf{pp} \leftarrow\!\!\$\ \mathsf{Pgen}(1^\lambda)$, $(\mathsf{sk}, \mathsf{pk}) \leftarrow\!\!\$\ \mathsf{KGen}(1^\lambda)$ and then $\sigma \leftarrow\!\!\$\ \mathsf{Sig}(\mathsf{sk}, \mu)$, $\mathsf{Vf}(\mathsf{pk}, \mu, \sigma)$ always returns 1 if $\sigma \neq \perp$.

Security The multi-user existential unforgeability against the chosen message attack under the adaptive corruptions and key leakages ($\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA) is defined by the related game formalized in Fig. 3. Then, a digital signature scheme is $(T_{\mathsf{c\&l}}, \epsilon_{\mathsf{c\&l}}, K, Q_s, Q_c, Q_l, \iota)$-$\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA if for any PPT adversary $\mathcal{A}$, which runs in time $T_{\mathsf{c\&l}}$ and can make Q_s queries to the signing oracle O_s, Q_c queries to the corrupting oracle O_c and Q_l queries to the leakage oracle O_l in order to obtain at most ι-bits information about secret keys $\{\mathsf{sk}_k\}_{k\in[K]}$, $\mathsf{Game}^{\mathsf{MU}^{\mathsf{c\&l}}\text{-}\mathsf{EUF\text{-}CMA}}_{\mathcal{A},K,\iota}(1^\lambda)$ returns 1 with probability at most $\epsilon_{\mathsf{c\&l}}$. When $\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA is considered in the random oracle model, $(T_{\mathsf{c\&l}}, \epsilon_{\mathsf{c\&l}}, K, Q_\mathsf{H}, Q_s, Q_c, Q_l, \iota)$-$\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA denotes $(T_{\mathsf{c\&l}}, \epsilon_{\mathsf{c\&l}}, K, Q_s, Q_c, Q_l, \iota)$-$\mathsf{MU}^{\mathsf{c\&l}}$-EUF-CMA with at most Q_H random oracle queries made by $\mathcal{A}$.

$\mathsf{Pgen}(1^\lambda)$	$\mathsf{KGen}(\mathsf{pp})$	$\mathsf{Sign}(\mathsf{pp},\mathsf{sk},\mathsf{pk},\mu)$	$\mathsf{Vf}(\mathsf{pp},\mathsf{pk},\mu,\sigma)$
$\boldsymbol{A} \leftarrow\!\!\$\ \mathbb{Z}_p^{n\times m}$	$\boldsymbol{S} \leftarrow\!\!\$\ \mathbb{Z}_{\lvert d\rvert}^{m\times\tilde{m}}$	$\boldsymbol{y} \leftarrow\!\!\$\ \mathfrak{D}_s^m$	$\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}\boldsymbol{c}$
return $\mathsf{pp} \leftarrow \boldsymbol{A}$	$\boldsymbol{T} \leftarrow \boldsymbol{A}\boldsymbol{S}$	$\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{y}$	**return** 1 **if** $\lVert\boldsymbol{z}\rVert \le \eta s\sqrt{m} \wedge \boldsymbol{c} = H(\mathsf{pk},\boldsymbol{w},\mu)$
	$(\mathsf{sk},\mathsf{pk}) \leftarrow (\boldsymbol{S},\boldsymbol{T})$	$\boldsymbol{c} \leftarrow H(\mathsf{pk},\boldsymbol{w},\mu)$	**return** 0
	return $(\mathsf{sk},\mathsf{pk})$	$\boldsymbol{z} \leftarrow \boldsymbol{y} + \boldsymbol{S}\boldsymbol{c}$	
		w/ prob. $p(\boldsymbol{S},(\boldsymbol{c},\boldsymbol{z}))$:	
		return $\sigma \leftarrow (\boldsymbol{c},\boldsymbol{z})$	
		else : **return** $\perp$	

Fig. 4. Plain Lyubashevesky Signature Scheme Lyu

Table 2. Parameters for Lyu

n	the row size of $\boldsymbol{A}$	a polynomial in λ
m	the column size of $\boldsymbol{A}$	$m \ge 2n$
p	modulo	prime and a polynomial in λ
ν	the expanding parameter for m	$m \approx \nu(n) + n\frac{\log_2 p}{\log_2(2d+1)}$ ($\nu = 64$ in [20])
$\tilde{m}$	the column size of $\boldsymbol{S}$	
d	the upper bound of absolute values of entries in $\boldsymbol{S}$	$d \ge 1$
κ	the ℓ_1-norm of $\boldsymbol{c} \in \mathcal{CH}$	$\binom{\tilde{m}}{\kappa} \ge 2^{\nu(n)}$
η	the parameter for $\boldsymbol{z}$	
α'	the parameter for $p(\boldsymbol{S},(\boldsymbol{c},\boldsymbol{z}))$ related to Rejection Sampling	$\frac{\mathfrak{D}_s^m(\boldsymbol{z})}{\mathfrak{D}_{\boldsymbol{S}\boldsymbol{c},s}^m(\boldsymbol{z})} \le \exp\left(\frac{d\kappa\sqrt{2\alpha' m}}{s} + (\frac{d\kappa\sqrt{m}}{2s})^2\right)$ w. prob. $1-2e^{-\alpha'}$ ($\alpha' = 72$ in [19, Lemma 4.5])
M	the constant in Rejection Sampling	$m \ge n\log_2 p + \log_2\left(1 - \frac{1-2e^{-\alpha'}}{M}\right) + 2\alpha'\log_2 e - 2$
s	the standard deviation for $\mathfrak{D}$	$M \approx \frac{\mathfrak{D}_s^m(\boldsymbol{z})}{\mathfrak{D}_{\boldsymbol{S}\boldsymbol{c},s}^m(\boldsymbol{z})} \wedge s \approx 12d\kappa\sqrt{m}$
L	the size of $\mathsf{sk} = \boldsymbol{S}$	$L = \lvert\mathsf{sk}\rvert = m\tilde{m}\log_2(2d+1)$
δ	the ratio of the leakage bit over L	$\iota = \delta L$
ρ	the adjusting parameter for δ	$\delta \le \frac{1}{2} - \frac{\rho(n)+n\tilde{m}\log_2 p}{2L} = \frac{1}{2} - o(1)$

3 MU$^{\mathsf{c\&l}}$-EUF-CMA Security of Lyubashevesky Signature

Let $p \in \mathbb{P}$, let $n, m, \tilde{m}, d \in \mathbb{N}$ and let $s \in \mathbb{R}$. We set $\mathcal{CH} = \left\{\boldsymbol{c} \in \mathbb{Z}_{|1|}^{\tilde{m}} \mid \lVert\boldsymbol{c}\rVert_1 \le \kappa\right\}$, and then $H : \{0,1\}^* \to \mathcal{CH}$. Then the Lyubashevesky signature scheme Lyu [20] is described in Fig. 4 and the parameters for Lyu are listed in Tab. 2. For any $\boldsymbol{S} \in \mathbb{Z}^{m\times\tilde{m}}$, any $\boldsymbol{c} \in \mathbb{Z}^{\tilde{m}}$ and any $\boldsymbol{z} \in \mathbb{Z}^m$, let $p(\boldsymbol{S},(\boldsymbol{c},\boldsymbol{z}))$ denote $\min\left\{\frac{\mathfrak{D}_s^m(\boldsymbol{z})}{MD_{\boldsymbol{S}\boldsymbol{c},s}^m(\boldsymbol{z})}, 1\right\}$.

Then, the MU$^{\mathsf{c\&l}}$-EUF-CMA of Lyu with $\iota = \left(\frac{1}{2} - o(1)\right)L$ bits leakages can be shown as follows.

Theorem 1. *let $n, m, p, \nu, \tilde{m}, d, \kappa, \eta, M, s, L, \delta, \rho$ be parameters set as in Tab. 2, and let $\zeta = 2(\eta s + d\kappa)\sqrt{m}$. Then,* Lyu *is $(T_{\mathsf{c\&l}}, \epsilon_{\mathsf{c\&l}}, K, Q_{\mathsf{H}}, Q_s, Q_c, Q_l, \iota)$-MU$^{\mathsf{c\&l}}$-EUF-CMA in the random oracle model under the $(T_{\mathsf{SIS}}, \epsilon_{\mathsf{SIS}})$-$\ell_2$-SIS$_{p,n,m,\zeta}$ assumption, where for $\tilde{Q} = Q_{\mathsf{H}} + Q_s + 1$ and a negligible function ϵ_{tw},*

$$T_{\mathsf{c\&l}} = 2T_{\mathsf{SIS}} - O(Km(n+\tilde{m}) + Q_{\mathsf{H}} + Q_s) \text{ and}$$
$$\epsilon_{\mathsf{c\&l}} \le \sqrt{2\tilde{Q}\epsilon_{\mathsf{SIS}} + \frac{\tilde{Q}}{|\mathcal{CH}|} + \frac{\tilde{Q}}{3^{\nu(n)}} + \frac{\tilde{Q}}{2^{\rho(n)}}} + \frac{Q_s(Q_s+Q_{\mathsf{H}})}{2^{n+1}} + Q_s\left(\frac{2(1+M)}{Me^{\alpha'}} + \epsilon_{\mathsf{tw}}\right).$$

Proof. We show this theorem by the hybrid argument. Let $\mathcal{A}$ be an adversary against MU$^{\mathsf{c\&l}}$-EUF-CMA of Lyu. Our sequential games Game$_1$, Game$_2$ and Game$_3$ are given in Fig. 5. We now explain the description of each game and evaluate the winning probability of each game.

Game$_1$ Game$_1$ is the original MU$^{\mathsf{c\&l}}$-EUF-CMA game of Lyu. Here, $\mathfrak{L}_{\mathsf{H}}$ is a key-value list such that a key consists of an input $(\mathsf{pk},\boldsymbol{w},\mu)$ to O_{H}, and the corresponding value consists of its hash value

$\underline{\mathsf{Game}_1,\ \mathsf{Game}_2,\ \mathsf{Game}_3}$

$\mathsf{pp} = \boldsymbol{A} \leftarrow\!\$\ \mathbb{Z}_p^{n\times m}$
$\mathfrak{L}_{\mathsf{H}} \leftarrow \emptyset;\ \mathfrak{L}_s \leftarrow \emptyset;\ \mathfrak{L}_c \leftarrow \emptyset;\ l \leftarrow 0;\ q \leftarrow 0$
for $k \in [K]$:
  $\boldsymbol{S}_k \leftarrow\!\$\ \mathbb{Z}_{|d|}^{m\times \tilde{m}}$
  $\boldsymbol{T}_k \leftarrow \boldsymbol{A}\boldsymbol{S}_k$
  $(\mathsf{sk}_k, \mathsf{pk}_k) \leftarrow (\boldsymbol{S}_k, \boldsymbol{T}_k)$
$(k^*, \mu^*, \sigma^*) \leftarrow\!\$\ \mathcal{A}^{\mathsf{O}_{\mathsf{H}},\mathsf{O}_c,\mathsf{O}_l,\mathsf{O}_s}(\mathsf{pp}, \{\mathsf{pk}_k\}_{k\in[K]})$
$(\boldsymbol{c}^*, \boldsymbol{z}^*) \leftarrow \sigma^*$
$\boldsymbol{w}^* \leftarrow \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}_{k^*}\boldsymbol{c}^*$
return 0 **if** $\mathsf{pk}_{k^*} \in \mathfrak{L}_c \vee (k^*, \mu^*) \in \mathfrak{L}_s \vee$
  $\|\boldsymbol{z}^*\| > \eta s\sqrt{m} \vee \boldsymbol{c}^* \neq \mathsf{O}_{\mathsf{H}}(\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*)$
return 1

$\underline{\mathsf{O}_c(k)}$

$\mathfrak{L}_c \leftarrow \mathfrak{L}_c \cup \{k\}$
return sk_k

$\underline{\mathsf{O}_l(k, f)}$

return $\perp$ **if** $l + |f(\mathsf{sk}_k)| > \iota$
$l \leftarrow l + |f(\mathsf{sk}_k)|$
return $f(\mathsf{sk}_k)$

$\underline{\mathsf{O}_{\mathsf{H}}(\mathsf{pk}, \boldsymbol{w}, \mu)}$

if $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu] \neq \perp$:
  $q \leftarrow q + 1$
  $\boldsymbol{c} \leftarrow\!\$\ \mathcal{CH}$
  $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu] \leftarrow (\boldsymbol{c}, q)$
return $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu]$

$\underline{\mathsf{O}_s(k, \mu) \quad /\!/\ \mathsf{Game}_1}$

$\boldsymbol{y} \leftarrow\!\$\ \mathfrak{D}_s^m$
$\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{y}$
$\boldsymbol{c} \leftarrow \mathsf{O}_{\mathsf{H}}(\mathsf{pk}_k, \boldsymbol{w}, \mu)$
$\boldsymbol{z} \leftarrow \boldsymbol{y} + \boldsymbol{S}_k\boldsymbol{c}$
w/ prob. $p(\boldsymbol{S}_k, (\boldsymbol{c}, \boldsymbol{z}))$:
  return $\sigma \leftarrow (\boldsymbol{c}, \boldsymbol{z})$
else : **return** $\perp$
$\mathfrak{L}_s \leftarrow \mathfrak{L}_s \cup \{(k, \mu)\}$

$\underline{\mathsf{O}_s(k, \mu) \quad /\!/\ \mathsf{Game}_2}$

$\boldsymbol{y} \leftarrow\!\$\ \mathfrak{D}_s^m$
$\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{y}$
$q \leftarrow q + 1$
$\boldsymbol{c} \leftarrow\!\$\ \mathcal{CH}$
$\boldsymbol{z} \leftarrow \boldsymbol{y} + \boldsymbol{S}_k\boldsymbol{c}$
abort if $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \neq \perp$
$\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \leftarrow (\boldsymbol{c}, q)$
w/ prob. $p(\boldsymbol{S}_k, (\boldsymbol{c}, \boldsymbol{z}))$:
  return $\sigma \leftarrow (\boldsymbol{c}, \boldsymbol{z})$
else : **return** $\perp$
$\mathfrak{L}_s \leftarrow \mathfrak{L}_s \cup \{(k, \mu)\}$

$\underline{\mathsf{O}_s(k, \mu) \quad /\!/\ \mathsf{Game}_3}$

$\boldsymbol{z} \leftarrow\!\$\ \mathfrak{D}_s^m$
$q \leftarrow q + 1$
$\boldsymbol{c} \leftarrow\!\$\ \mathcal{CH}$
w/ prob. $1/M$:
  $\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}_k\boldsymbol{c}$
  $\sigma \leftarrow (\boldsymbol{c}, \boldsymbol{z})$
else :
  $\boldsymbol{w} \leftarrow\!\$\ \mathbb{Z}_p^n$
  $\sigma \leftarrow \perp$
abort if $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \neq \perp$
$\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \leftarrow (\boldsymbol{c}, q)$
return σ
$\mathfrak{L}_s \leftarrow \mathfrak{L}_s \cup \{(k, \mu)\}$

Fig. 5. Sequential games for Theorem 1

$\boldsymbol{c} \in \mathcal{CH}$ and an index q to indicate when the hash value $\boldsymbol{c}$ of the tuple $(\mathsf{pk}, \boldsymbol{w}, \mu)$ is added to the list. Observe that the chance to add a new value to $\mathfrak{L}_{\mathsf{H}}$ is that $\mathcal{A}$ directly accesses a random oracle O_{H} and accesses O_{H} via the signing oracle O_s. Game_1 checks whether or not $\boldsymbol{c}^* = \mathsf{O}_{\mathsf{H}}(\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*)$ after $\mathcal{A}$ returns $(k^*, \mu^*, (\boldsymbol{c}^*, \boldsymbol{z}^*))$. This implies that the size of $\mathfrak{L}_{\mathsf{H}}$ at the time when Game_1 is finished is at most $Q_{\mathsf{H}} + Q_s + 1 = \tilde{Q}$. For the winning probability of Game_1 by $\mathcal{A}$, we have

$$\Pr[\mathsf{Game}_1 = 1] = \epsilon_{\mathrm{c\&l}}. \tag{3}$$

Game_2 Game_2 proceeds in the same way as in Game_1 except that O_s programs a hash value $\boldsymbol{c}$ which is uniformly chosen by itself. Since O_s sets a hash value in the same way as O_{H}, the procedures of Game_1 and Game_2 are identical unless O_s aborts. Therefore, we now evaluate such an abort probability.

The abort probability is evaluated by estimating the chance of meeting $\boldsymbol{w}$ that has already appeared in $\mathfrak{L}_{\mathsf{H}}$. As explained in Subsect. 2.1, we now assume that the public matrix $\boldsymbol{A}$ is expressed as Hermite Normal Form, namely $\boldsymbol{A} = \left[\overline{\boldsymbol{A}}\ \boldsymbol{I}\right]$ for some $\overline{\boldsymbol{A}} \in \mathbb{Z}_p^{n\times(m-n)}$. It follows from Lemma 1 that for any

vector $\tilde{\boldsymbol{w}} \in \mathbb{Z}_p^n$,

$$\begin{aligned}\Pr_{\boldsymbol{y} \leftarrow\!\$\, \mathfrak{D}_s^m}[\boldsymbol{A}\boldsymbol{y} = \tilde{\boldsymbol{w}}] &= \Pr_{\boldsymbol{y} = \begin{bmatrix}\boldsymbol{y}_1 \\ \boldsymbol{y}_2\end{bmatrix} \leftarrow\!\$\, \mathfrak{D}_s^m}\left[\begin{bmatrix}\overline{\boldsymbol{A}} & \boldsymbol{I}\end{bmatrix}\begin{bmatrix}\boldsymbol{y}_1 \\ \boldsymbol{y}_2\end{bmatrix} = \tilde{\boldsymbol{w}}\right] \\ &= \Pr_{\boldsymbol{y} = \begin{bmatrix}\boldsymbol{y}_1 \\ \boldsymbol{y}_2\end{bmatrix} \leftarrow\!\$\, \mathfrak{D}_s^m}\left[\overline{\boldsymbol{A}}\boldsymbol{y}_1 + \boldsymbol{y}_2 = \tilde{\boldsymbol{w}}\right] \\ &= \Pr_{\boldsymbol{y}_2 \leftarrow\!\$\, \mathfrak{D}_s^n}\left[\boldsymbol{y}_2 = \tilde{\boldsymbol{w}} - \overline{\boldsymbol{A}}\boldsymbol{y}_1\right] \\ &\le 2^{-n}.\end{aligned}$$

Since $\mathcal{A}$ makes at most q_{H} queries to O_{H}, $\mathfrak{L}_{\mathsf{H}}$ has at most $i - 1 + Q_{\mathsf{H}}$ entities just before making i-th query to O_s. Therefore, the abort probability can be evaluated by

$$\sum_{i=1}^{Q_s} \frac{i - 1 + Q_{\mathsf{H}}}{2^n} \le \frac{Q_s(Q_s + Q_{\mathsf{H}})}{2^{n+1}}.$$

Therefore, we have

$$\Pr[\mathsf{Game}_2 = 1] \ge \Pr[\mathsf{Game}_1 = 1] - \frac{Q_s(Q_s + Q_{\mathsf{H}})}{2^{n+1}}. \tag{4}$$

Game_3 Game_3 proceeds in the same way as Game_2 except that O_s is simluated without $\boldsymbol{S}_k$ as in Fig. 5. We evaluate the difference between the probabilities of Game_2 and Game_3.

By employing Lemma 5, we first evaluate the statistical distance between the distributions of the output $(\boldsymbol{c}, \boldsymbol{z})$ in both the games in the case where O_s does not return $\perp$. On O_s of Game_2, it follows from $\boldsymbol{y} \leftarrow\!\$\, \mathfrak{D}_s^m$ that the distribution of $\boldsymbol{z}$ is regarded as the distribution $D_{\boldsymbol{v},s}^m$ by letting $\boldsymbol{v} \leftarrow \boldsymbol{S}_k\boldsymbol{c}$. According to the parameters in [20], for any $\boldsymbol{v} \in \mathbb{Z}_p^m$, there exist two vectors $\boldsymbol{c} \in \mathcal{CH}$ such that $\boldsymbol{v} = \boldsymbol{S}_k\boldsymbol{c}$ with the negligible probability ϵ_{tw}. Thus, outputting $(\boldsymbol{c}, \boldsymbol{z})$ instead of $(\boldsymbol{v}, \boldsymbol{z})$ does not affect employing Lemma 5. Therefore, the distribution of the output by O_s can be regarded as that of Real. On the other hand, observe that $\boldsymbol{z} \leftarrow\!\$\, \mathfrak{D}_s^m$ by O_s in Game_3. By the same reason discussed in the distribution of $(\boldsymbol{c}, \boldsymbol{z})$ in Game_2, outputting $\boldsymbol{c}$ does not affect employing Lemma 5 and the distribution of the output $(\boldsymbol{c}, \boldsymbol{z})$ by O_s in Game_3 can be regarded as that of Ideal. Applying Lemma 5 to O_s of Game_2 and Game_3, we can see that the statistical distance of the distributions of $(\boldsymbol{c}, \boldsymbol{z})$ in both the games is at most $2e^{-\alpha'}/M$.

Since $\boldsymbol{c}$ is programmed as the hash value of $(\mathsf{pk}_k, \boldsymbol{w}, \mu)$ even when O_s returns $\perp$, we next evaluate the statistical distance of the distributions of $(\boldsymbol{w}, \boldsymbol{c})$ in the case where O_s returns $\perp$ as in [6]. Observe that $\boldsymbol{c}$ is chosen uniformly at random from $\mathcal{CH}$ in both games. Hence, we merely evaluate the statistical distance of the distributions of $\boldsymbol{w}$. In Game_2, O_s sets $\boldsymbol{w}$ as $\boldsymbol{A}\boldsymbol{y}$ for $\boldsymbol{A} \in \mathbb{Z}_p^{n \times m}$ and $\boldsymbol{y} \leftarrow\!\$\, \mathfrak{D}_s^m$, whereas it chooses $\boldsymbol{w}$ uniformly at random from $\mathbb{Z}_p^n$ in Game_3. We can estimate the probability that O_s returns $\perp$ in Game_2 is $1/M - 2e^{-\alpha'}/M$ by Lemma 5. Lemma 1 and Tab. 2 imply that

$$\begin{aligned}H_\infty(\boldsymbol{y}) &\ge m \\ &\ge n\log_2 p + \log_2\left(1 - \frac{1 - 2e^{-\alpha'}}{M}\right) + 2\alpha'\log_2 e - 2 \\ &= n\log_2 p + \log_2\left(1 - \left(\frac{1}{M} - \frac{2e^{-\alpha'}}{M}\right)\right) + 2\log_2\frac{1}{2e^{-\alpha'}}.\end{aligned}$$

Therefore, we have

$$\begin{aligned}&H_\infty(\boldsymbol{y} \mid \perp \leftarrow \mathsf{O}_s) \\ &\quad\ge H_\infty(\boldsymbol{y}) - \log_2 \Pr[\perp \leftarrow \mathsf{O}_s] \\ &\quad\ge m - \log_2\left(1 - \left(\frac{1}{M} - \frac{2e^{-\alpha'}}{M}\right)\right) \\ &\quad\ge \left(n\log_2 p + \log_2\left(1 - \left(\frac{1}{M} - \frac{2e^{-\alpha'}}{M}\right)\right) + 2\log_2\frac{1}{2e^{-\alpha'}}\right) - \log_2\left(1 - \left(\frac{1}{M} - \frac{2e^{-\alpha'}}{M}\right)\right) \\ &\quad\ge \left|\mathbb{Z}_p^n\right| + 2\log_2\frac{1}{2e^{-\alpha'}}.\end{aligned}$$

$\mathcal{R}(\boldsymbol{A})$

for $k \in [K]$:
  $\boldsymbol{S}_k \leftarrow\!\!\$\ \mathbb{Z}_{|d|}^{m \times \tilde{m}}$
  $\boldsymbol{T}_k \leftarrow \boldsymbol{A}\boldsymbol{S}_k$
$(b, y, y') \leftarrow\!\!\$\ \mathcal{F}_{\mathcal{C}}(\boldsymbol{A}, \{(\boldsymbol{S}_k, \boldsymbol{T}_k)\}_{k\in[K]})$
return $\perp$ **if** $b = 0$
$(k, \boldsymbol{w}, \boldsymbol{c}, \boldsymbol{z}) \leftarrow y;\ (k', \boldsymbol{w}', \boldsymbol{c}', \boldsymbol{z}') \leftarrow y'$
return $\perp$ **if** $(k, \boldsymbol{w}) \neq (k', \boldsymbol{w}')$
return $\boldsymbol{z} - \boldsymbol{z}' - \boldsymbol{S}_k(\boldsymbol{c} - \boldsymbol{c}')$

$\mathcal{C}(\boldsymbol{A}, \{(\boldsymbol{S}_k, \boldsymbol{T}_k)\}_{k\in[K]}, \{h_q\}_{q\in[\tilde{Q}]})$

$\mathsf{pp} \leftarrow \boldsymbol{A}$
$\mathfrak{L}_{\mathsf{H}} \leftarrow \emptyset;\ \mathfrak{L}_s \leftarrow \emptyset;\ \mathfrak{L}_c \leftarrow \emptyset;\ l \leftarrow 0;\ q \leftarrow 0$
for $k \in [K] : (\mathsf{sk}_k, \mathsf{pk}_k) \leftarrow (\boldsymbol{S}_k, \boldsymbol{T}_k)$
$(k^*, \mu^*, \sigma^*) \leftarrow\!\!\$\ \mathcal{A}^{\mathsf{O_H}, \mathsf{O}_c, \mathsf{O}_l, \mathsf{O}_s}(\mathsf{pp}, \{\mathsf{pk}_k\}_{k\in[K]})$
$(\boldsymbol{c}^*, \boldsymbol{z}^*) \leftarrow \sigma^*$
$\boldsymbol{w}^* \leftarrow \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}_{k^*}\boldsymbol{c}^*$
return $(0, \epsilon)$ **if** $\mathsf{pk}_{k^*} \in \mathfrak{L}_c \vee (k^*, \mu^*) \in \mathfrak{L}_s \vee$
  $\|\boldsymbol{z}^*\| > \eta s\sqrt{m} \vee \boldsymbol{c}^* \neq \mathsf{O_H}(\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*)$
$(\boldsymbol{c}^*, I) \leftarrow \mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*]$
return $(I, (k^*, \boldsymbol{w}^*, \boldsymbol{c}^*, \boldsymbol{z}^*))$

$\mathcal{F}_{\mathcal{C}}(\boldsymbol{A}, \{(\boldsymbol{S}_k, \boldsymbol{T}_k)\}_{k\in[K]})$

$\omega \leftarrow\!\!\$\ \{0,1\}^{\lambda}$
$h_1, \ldots, h_Q \leftarrow\!\!\$\ \mathcal{CH}$
$(I, (k, \boldsymbol{w}, \boldsymbol{c}, \boldsymbol{z})) \leftarrow\!\!\$\ \mathcal{C}(\boldsymbol{A}, \{(\boldsymbol{S}_k, \boldsymbol{T}_k)\}_{k\in[K]}, \{h_q\}_{q\in[1,Q]}; \omega)$
return $(0, \epsilon, \epsilon)$ **if** $I = 0$
$h'_I, \ldots, h'_Q \leftarrow\!\!\$\ \mathcal{CH}$
$(I', (k', \boldsymbol{w}', \boldsymbol{c}', \boldsymbol{z}')) \leftarrow\!\!\$\ \mathcal{C}(\boldsymbol{A}, \{(\boldsymbol{S}_k, \boldsymbol{T}_k)\}_{k\in[K]}, \{h_q\}_{q\in[1,I-1]} \cup \{h'_q\}_{q\in[I,Q]}; \omega)$
return $(0, \epsilon, \epsilon)$ **if** $I \neq I' \vee h_I = h'_I$
return $(1, (k, \boldsymbol{w}, \boldsymbol{c}, \boldsymbol{z})), (k', \boldsymbol{w}', \boldsymbol{c}', \boldsymbol{z}')))$

$\mathsf{O}_s(k, \mu)$

$\boldsymbol{z} \leftarrow\!\!\$\ \mathfrak{D}_s^m$
$q \leftarrow q + 1$
$\boldsymbol{c} \leftarrow\!\!\$\ \mathcal{CH}$
w/ prob. $1/M$:
  $\boldsymbol{w} \leftarrow \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}_k\boldsymbol{c}$
  $\sigma \leftarrow (\boldsymbol{c}, \boldsymbol{z})$
else :
  $\boldsymbol{w} \leftarrow\!\!\$\ \mathbb{Z}_p^n$
  $\sigma \leftarrow \perp$
abort if $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \neq \perp$
$\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}_k, \boldsymbol{w}, \mu] \leftarrow (\boldsymbol{c}, q)$
return σ
$\mathfrak{L}_s \leftarrow \mathfrak{L}_s \cup \{(k, \mu)\}$

$\mathsf{O}_c(k)$

$\mathfrak{L}_c \leftarrow \mathfrak{L}_c \cup \{k\}$
return sk_k

$\mathsf{O}_l(k, f)$

return $\perp$ **if** $l + |f(\mathsf{sk}_k)| > \iota$
$l \leftarrow l + |f(\mathsf{sk}_k)|$
return $f(\mathsf{sk}_k)$

$\mathsf{O_H}(\mathsf{pk}, \boldsymbol{w}, \mu)$

if $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu] \neq \perp$:
  $q \leftarrow q + 1$
  $\boldsymbol{c} \leftarrow h_q$
  $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu] \leftarrow (\boldsymbol{c}, q)$
return $\mathfrak{L}_{\mathsf{H}}[\mathsf{pk}, \boldsymbol{w}, \mu]$

Fig. 6. Reduction $\mathcal{R}$ and forked algorithm $\mathcal{C}$

As in Lemma 7, the function mapping $\boldsymbol{y} \in \mathbb{Z}_p^m$ to $\boldsymbol{A}\boldsymbol{y} \in \mathbb{Z}_p^n$ is known to be 2-universal. It follows from Lemma 8 that the statistical distance between the distributions of $\boldsymbol{w}$ set in O_s of Game_2 and Game_3 is at most $2e^{-\alpha'}$ in the case where O_s returns $\perp$.

Recall that $\mathcal{A}$ makes at most Q_s queries to $\mathsf{O_{Sig}}$. Lemma 5 implies that

$$|\Pr[\mathsf{Game}_3 = 1] - \Pr[\mathsf{Game}_2 = 1]| \leq Q_s \left(\frac{2(1+M)}{Me^{\alpha'}} + \epsilon_{\mathsf{tw}} \right). \tag{5}$$

Reduction of ℓ_2-SIS from Game_3 We aim to construct a reduction $\mathcal{R}$ that solves the ℓ_2-SIS problem by employing the forking lemma (Lemma 9) with the procedures of Game_3. For the forking lemma, we first construct the algorithm $\mathcal{C}$ as in Fig. 6 that is the target of the fork. $\mathcal{C}$ plays Game_3 with $\mathcal{A}$ and then returns the index I indicating when $(\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*)$ has been added to $\mathfrak{L}_{\mathsf{H}}$, the index $k^* \in [K]$ and the transcript $(\boldsymbol{w}^*, \boldsymbol{c}^*, \boldsymbol{z}^*)$ from the forgery $(k^*, \mu^*, (\boldsymbol{c}^*, \boldsymbol{z}^*))$ returned by $\mathcal{A}$ with $\boldsymbol{w}^* = \boldsymbol{A}\boldsymbol{z} - \boldsymbol{T}_{k^*}\boldsymbol{c}^*$. Since $\mathcal{C}$ surely makes a query $(\boldsymbol{w}^*, \boldsymbol{c}^*, \boldsymbol{z}^*)$ to $\mathsf{O_H}$, it is guaranteed that $I \geq 1$. In other words, $\mathcal{C}$ returns $(0, \epsilon)$

only when $\mathcal{A}$ loses Game_3. This implies that the probability acc defined in Eq. (1) can be expressed as

$$\mathsf{acc} = \Pr[\mathsf{Game}_3 = 1]. \tag{6}$$

Then, the algorithm $\mathcal{R}$ given as in Fig.6 runs the forking algorithm $\mathcal{F}_{\mathcal{C}}$ depicted in Fig. 6 with $\mathcal{C}$. Here, $\mathcal{F}_{\mathcal{C}}$ chooses h_q from the set $\mathcal{CH}$ for any $q \in [\tilde{Q}]$. Lemma 9 implies that $I = I'$ and $h_I \neq h'_I$ with probability frk that is evaluated as follows:

$$\mathsf{frk} \geq \mathsf{acc} \cdot \left(\frac{\mathsf{acc}}{\tilde{Q}} - \frac{1}{|\mathcal{CH}|} \right) \geq \frac{\mathsf{acc}^2}{\tilde{Q}} - \frac{1}{|\mathcal{CH}|}. \tag{7}$$

By the construction presented in Fig. 6, $\mathcal{C}$ sets the input value h_q as the hash value $\boldsymbol{c}_q$ of the q-th entry added into $\mathfrak{L}_{\mathsf{H}}$ for each $q \in [\tilde{Q}]$ during running O_{H} and O_s. Recall that I and I' set in $\mathcal{F}_{\mathcal{C}}$ are the indices when $\mathcal{C}$ adds $(\mathsf{pk}_{k^*}, \boldsymbol{w}^*, \mu^*)$ into $\mathfrak{L}_{\mathsf{H}}$ for the first execution of $\mathcal{A}$ and the second execution of $\mathcal{A}$, respectively. It follows again from the construction of $\mathcal{C}$ that $\boldsymbol{c} = h_I$ and $\boldsymbol{c}' = h_{I'}$ for the values $\boldsymbol{c}$ and $\boldsymbol{c}'$ appeared in $\mathcal{R}$. Namely, it holds that

$$\boldsymbol{c} = h_I \neq h'_I = \boldsymbol{c}'.$$

Since the same randomness ω is used in both the first execution and the second execution of $\mathcal{A}$ by $\mathcal{F}_{\mathcal{C}}$ and $I = I'$, we also have

$$k = k' = k^* \text{ and } \boldsymbol{w} = \boldsymbol{w}'.$$

It follows from $I = I' \geq 1$, namely $\mathcal{A}$ has win Game_3, that

$$\boldsymbol{w} = \boldsymbol{A}\boldsymbol{z} - \boldsymbol{A}\boldsymbol{S}_{k^*}\boldsymbol{c} \text{ and } \boldsymbol{w}' = \boldsymbol{A}\boldsymbol{z}' - \boldsymbol{A}\boldsymbol{S}_{k^*}\boldsymbol{c}'.$$

By letting $\boldsymbol{v} = \boldsymbol{z} - \boldsymbol{z}' - \boldsymbol{S}_{k^*}(\boldsymbol{c} - \boldsymbol{c}')$, it holds that $\boldsymbol{A}\boldsymbol{v} = \boldsymbol{0}$. On the other hand, the winning condition of Game_3 implies that $\|\boldsymbol{z}\|, \|\boldsymbol{z}'\| \leq \eta s\sqrt{m}$. It follows from $\boldsymbol{S}_{k^*} \in \mathbb{Z}_{|d|}^{m \times \tilde{m}}$ and $\boldsymbol{c}, \boldsymbol{c}' \in \mathcal{CH}$ that $\|\boldsymbol{S}_{k^*}\boldsymbol{c}\|, \|\boldsymbol{S}_{k^*}\boldsymbol{c}'\| \leq \kappa d\sqrt{m}$. These imply that

$$\|\boldsymbol{v}\| = \|\boldsymbol{z} - \boldsymbol{z}' - \boldsymbol{S}_{k^*}(\boldsymbol{c} - \boldsymbol{c}')\| \leq \|\boldsymbol{z}\| + \|\boldsymbol{z}'\| + \|\boldsymbol{S}_{k^*}\boldsymbol{c}\| + \|\boldsymbol{S}_{k^*}\boldsymbol{c}'\| \leq 2(\eta s + d\kappa)\sqrt{m} = \zeta.$$

Therefore, $\boldsymbol{v}$ can be a solution of the ℓ_2-SIS problem under the condition that $\boldsymbol{v} \neq \boldsymbol{0}$.

The rest of the proof is devoted to show that $\boldsymbol{v} = \boldsymbol{z} - \boldsymbol{z}' - \boldsymbol{S}_{k^*}(\boldsymbol{c} - \boldsymbol{c}') \neq \boldsymbol{0}$ with high probability. The following lemma guarantees that there exists at least two short vectors $\boldsymbol{S}_{k^*}, \tilde{\boldsymbol{S}}_{k^*}$ such that $\boldsymbol{A}\boldsymbol{S}_{k^*} = \boldsymbol{A}\tilde{\boldsymbol{S}}_{k^*}$. This lemma is given by generalizing [19, Lemma 5.2].

Lemma 10. *Let $p \in \mathbb{P}$, let $n \in \mathbb{N}$, let $d \geq 1$, and let $m > \nu(n) + n \cdot \log p / \log(2d+1)$. We set $\boldsymbol{A} \in \mathbb{Z}_p^{n \times m}$. For any random vector $\boldsymbol{s} \leftarrow\!\!\$\, \mathbb{Z}_{|d|}^n$, the probability that there exists another vector $\tilde{\boldsymbol{s}} \leftarrow\!\!\$\, \mathbb{Z}_{|d|}^n$ such that $\boldsymbol{A}\boldsymbol{s} = \boldsymbol{A}\tilde{\boldsymbol{s}}$ is at least $1 - 3^{-\nu(n)}$.*

Since $\boldsymbol{c} \neq \boldsymbol{c}'$, this lemma implies that even if $\boldsymbol{z} - \boldsymbol{z}' + \boldsymbol{S}_{k^*}(\boldsymbol{c}' - \boldsymbol{c}) = \boldsymbol{0}$, then it is guaranteed that $\boldsymbol{z} - \boldsymbol{z}' + \tilde{\boldsymbol{S}}_{k^*}(\boldsymbol{c}' - \boldsymbol{c}) \neq \boldsymbol{0}$ and $\boldsymbol{A}(\boldsymbol{z} - \boldsymbol{z}' + \tilde{\boldsymbol{S}}_{k^*}(\boldsymbol{c}' - \boldsymbol{c})) = \boldsymbol{0}$.

For the information about $\boldsymbol{S}_{k^*}$, $\mathcal{A}$ is given $\boldsymbol{T}_{k^*} = \boldsymbol{A}\boldsymbol{S}_{k^*}$, signatures from O_s and the ι bits from O_l. As in the procedure on Game_3, O_s no longer uses $\boldsymbol{S}_{k^*}$. The only chance to obtain such information is the use of the leakage oracle O_l. We can see that O_l does not affect to detect which of $\boldsymbol{S}_{k^*}$ or $\tilde{\boldsymbol{S}}_{k^*}$ is used. To show this fact, we now consider the queries made by $\mathcal{A}$ to O_l during the first execution and the second execution of $\mathcal{C}$. We suppose that $\mathcal{A}$ has made a function f_i to O_l at i-th query during the first execution of $\mathcal{C}$ for each $i \in [Q_l]$, whereas it also has made a function f'_i to O_l at i-th query during the second execution of $\mathcal{C}$ for each $i \in [Q_l]$. The most significant information about $\boldsymbol{S}_{k^*}$ from O_l can be obtained when $\mathcal{A}$ makes queries (k^*, f_i) and (k^*, f'_i) to O_l. The total bits of the obtained information in this case is 2ι bits, since $\mathcal{A}$ can obtain at most ι-bits information from O_l during each of the first execution and the second execution of $\mathcal{C}$. We set the function $f : \mathbb{Z}_{|d|}^{m \times \tilde{m}} \to \{0,1\}^{2\iota + n\tilde{m}\log_2 p}$ mapping a matrix $\boldsymbol{S} \in \mathbb{Z}_{|d|}^{m \times \tilde{m}}$ to the concatenated string $f_1(\boldsymbol{S}) | \cdots | f_Q(\boldsymbol{S}) | f'_1(\boldsymbol{S}) | \cdots | f'_Q(\boldsymbol{S}) | \boldsymbol{T}_{n^*} \in \{0,1\}^{2\iota} \times \mathbb{Z}_p^{n \times \tilde{m}}$. We note that $f(\boldsymbol{S}_{k^*})$ denotes all information on $\boldsymbol{S}_{k^*}$ that can be obtained by $\mathcal{A}$. Then, the entropy of $\boldsymbol{S}_{k^*}$ under the condition that $\mathcal{A}$ can obtain such leaked information about $\boldsymbol{S}_{k^*}$ is evaluated by the following lemma.

Lemma 11. *Let $(\boldsymbol{S}_{k^*}, \boldsymbol{T}_{k^*})$ be a key pair given as in Fig. 6. Then, for $L = |\boldsymbol{S}_{k^*}| = m\tilde{m}\log_2(2d+1)$ and $\iota = \delta L$ such that there exists a polynomial ρ on n such that $\delta \leq \frac{1}{2} - \frac{\rho(n)+n\tilde{m}\log_2 p}{2L} = \frac{1}{2} - o(1)$, it holds that $H_\infty(\boldsymbol{S}_{k^*} \mid f(\boldsymbol{S}_{k^*})) = 0$ with probability at most $2^{-\rho(n)}$.*

Proof. We show this lemma by employing Lemma 6. Since $\boldsymbol{S}_{k^*}$ is chosen uniformly at random from $\mathbb{Z}_{|d|}^{m\times\tilde{m}}$, $H = H_\infty(\boldsymbol{S}_{k^*})$ is L. The length $|f(\boldsymbol{S}_{k^*})|$ can be evaluated as $2\iota + n\tilde{m}\log_2 p$. It follows from Lemma 6 and $\Delta = H$ that $H_\infty(\boldsymbol{S}_{k^*} \mid f(\boldsymbol{S}_{k^*})) = 0$ with probability at most $2^{|f(\boldsymbol{S}_{k^*})|-H}$. By $\iota = \delta L$, we have

$$2^{|f(\boldsymbol{S}_{k^*})|-H} = 2^{2\delta L + n\tilde{m}\log_2 p - L} \leq 2^{2(\frac{1}{2} - \frac{\rho(n)+n\tilde{m}\log_2 p}{2L})L + n\tilde{m}\log_2 p - L} = 2^{-\rho(n)}.$$

The proof is complete. □

Under the conditions that there exists at least two secret keys $\boldsymbol{S}_{k^*}$ and $\tilde{\boldsymbol{S}}_{k^*}$ of $\boldsymbol{T}_{k^*}$ and $H_\infty(\boldsymbol{S}_{k^*} \mid f(\boldsymbol{S}_{k^*})) > 0$, $\mathcal{A}$ can distinguish which of $\boldsymbol{S}_{k^*}$ and $\tilde{\boldsymbol{S}}_{k^*}$ is used in Game_3 with probability only $1/2$. Lemmas 10 and 11 imply that the probability that $\mathcal{R}$ solves the ℓ_2-SIS problem on the given $\boldsymbol{A}$ can be evaluated as follows.

$$\begin{aligned}
\epsilon_{\mathsf{SIS}} &\geq \frac{1}{2}\left(1 - \frac{1}{3^{\nu(n)}}\right)\left(1 - \frac{1}{2^{\rho(n)}}\right) \cdot \mathsf{frk} \\
&\geq \frac{1}{2}\left(1 - \frac{1}{3^{\nu(n)}} - \frac{1}{2^{\rho(n)}}\right) \cdot \mathsf{frk} \\
&\geq \frac{1}{2}\mathsf{frk} - \frac{1}{2\cdot 3^{\nu(n)}} - \frac{1}{2\cdot 2^{\rho(n)}}.
\end{aligned} \tag{8}$$

Observe that the running time of $\mathcal{R}$ is evaluated as $2T_{\mathsf{c\&l}} + O(Km(n+\tilde{m}) + Q_{\mathsf{H}} + Q_s) = T_{\mathsf{SIS}}$. On the other hand, by combining Eqs. (3)–(8), the success probability of solving ℓ_2-SIS is evaluated as

$$\epsilon_{\mathsf{SIS}} \geq \frac{1}{2}\cdot\frac{1}{\tilde{Q}}\left(\epsilon_{\mathsf{c\&l}} - \frac{Q_s(Q_s+Q_{\mathsf{H}})}{2^{n+1}} - Q_s\left(\frac{2(1+M)}{Me^{\alpha'}} + \epsilon_{\mathsf{tw}}\right)\right)^2 - \frac{1}{2\cdot|\mathcal{CH}|} - \frac{1}{2\cdot 3^{\nu(n)}} - \frac{1}{2\cdot 2^{\rho(n)}}.$$

This implies that

$$\epsilon_{\mathsf{c\&l}} \leq \sqrt{2\tilde{Q}\epsilon_{\mathsf{SIS}} + \frac{\tilde{Q}}{|\mathcal{CH}|} + \frac{\tilde{Q}}{3^{\nu(n)}} + \frac{\tilde{Q}}{2^{\rho(n)}}} + \frac{Q_s(Q_s+Q_{\mathsf{H}})}{2^{n+1}} + Q_s\left(\frac{2(1+M)}{Me^{\alpha'}} + \epsilon_{\mathsf{tw}}\right).$$

□

Acknowledgments. We would like to thank anonymous reviewers of ProvSec 2024 for their valuable comments and suggestions. This work was supported by JSPS KAKENHI Grant Numbers JP22K12023 and JP23K11105.

References

1. Abdalla, M., Fouque, P.A., Lyubashevsky, V., Tibouchi, M.: Tightly secure signatures from lossy identification schemes. Journal of Cryptology **29**(3), 597–631 (2016). https://doi.org/10.1007/s00145-015-9203-7, https://doi.org/10.1007/s00145-015-9203-7
2. Bader, C., Hofheinz, D., Jager, T., Kiltz, E., Li, Y.: Tightly-secure authenticated key exchange. In: Dodis, Y., Nielsen, J.B. (eds.) Theory of Cryptography. pp. 629–658. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
3. Barbosa, M., Barthe, G., Doczkal, C., Don, J., Fehr, S., Grégoire, B., Huang, Y.H., Hülsing, A., Lee, Y., Wu, X.: Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 358–389. Springer Nature Switzerland, Cham (2023)
4. Bellare, M., Neven, G.: Multi-signatures in the plain public-key model and a general forking lemma. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. pp. 390–399. CCS '06, Association for Computing Machinery, New York, NY, USA (2006). https://doi.org/10.1145/1180405.1180453, https://doi.org/10.1145/1180405.1180453

5. Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security. p. 62–73. CCS '93, Association for Computing Machinery, New York, NY, USA (1993). https://doi.org/10.1145/168588.168596, https://doi.org/10.1145/168588.168596
6. Devevey, J., Fallahpour, P., Passelègue, A., Stehlé, D., Xagawa, K.: A detailed analysis of fiat-shamir with aborts. Cryptology ePrint Archive, Paper 2023/245 (2023), https://eprint.iacr.org/2023/245, https://eprint.iacr.org/2023/245
7. Diemert, D., Gellert, K., Jager, T., Lyu, L.: More efficient digital signatures with tight multi-user security. In: Garay, J.A. (ed.) Public-Key Cryptography – PKC 2021. pp. 1–31. Springer International Publishing, Cham (2021)
8. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for diffie-hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013. pp. 129–147. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
9. Galbraith, S., Malone-Lee, J., Smart, N.: Public key signatures in the multi-user setting. Information Processing Letters **83**(5), 263–266 (2002). https://doi.org/https://doi.org/10.1016/S0020-0190(01)00338-6, https://www.sciencedirect.com/science/article/pii/S0020019001003386
10. Gjøsteen, K., Jager, T.: Practical and tightly-secure digital signatures and authenticated key exchange. In: Shacham, H., Boldyreva, A. (eds.) Advances in Cryptology – CRYPTO 2018. pp. 95–125. Springer International Publishing, Cham (2018)
11. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing **17**(2), 281–308 (1988). https://doi.org/10.1137/0217017
12. Han, S., Jager, T., Kiltz, E., Liu, S., Pan, J., Riepel, D., Schäge, S.: Authenticated key exchange and signatures with tight security in the standard model. In: Malkin, T., Peikert, C. (eds.) Advances in Cryptology – CRYPTO 2021. pp. 670–700. Springer International Publishing, Cham (2021)
13. Han, S., Liu, S., Gu, D.: Almost tight multi-user security under adaptive corruptions & leakages in the standard model. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. pp. 132–162. Springer Nature Switzerland, Cham (2023)
14. Han, S., Liu, S., Wang, Z., Gu, D.: Almost tight multi-user security under adaptive corruptions from lwe in the standard model. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 682–715. Springer Nature Switzerland, Cham (2023)
15. Jutla, C.S., Roy, A.: Shorter quasi-adaptive nizk proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) Advances in Cryptology - ASIACRYPT 2013. pp. 1–20. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
16. Katz, J., Vaikuntanathan, V.: Signature schemes with bounded leakage resilience. In: Matsui, M. (ed.) Advances in Cryptology – ASIACRYPT 2009. pp. 703–720. Springer Berlin Heidelberg, Berlin, Heidelberg (2009)
17. Kiltz, E., Masny, D., Pan, J.: Optimal security proofs for signatures from identification schemes. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016. pp. 33–61. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
18. Liu, Y., Zhou, Y., Zhang, R., Tao, Y.: (full) leakage resilience of fiat-shamir signatures over lattices. Frontiers of Computer Science **16**(5), 165819 (2022). https://doi.org/10.1007/s11704-021-0586-3, https://doi.org/10.1007/s11704-021-0586-3
19. Lyubashevsky, V.: Lattice signatures without trapdoors. Cryptology ePrint Archive, Paper 2011/537 (2011), https://eprint.iacr.org/2011/537, https://eprint.iacr.org/2011/537
20. Lyubashevsky, V.: Lattice signatures without trapdoors. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. pp. 738–755. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)
21. Pan, J., Wagner, B.: Lattice-based signatures with tight adaptive corruptions and more. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) Public-Key Cryptography – PKC 2022. pp. 347–378. Springer International Publishing, Cham (2022)