Short Lattice Signature Scheme with Tighter Reduction under Ring-SIS Assumption

Kaisei Kajita[1], Go Ohtake[1], Kazuto Ogawa[1⋆], Koji Nuida[2], and Tsuyoshi Takagi[3]

[1] Japan Broadcasting Corporation, 1-10-11 Kinuta, Setagaya-ku, Tokyo, Japan
kajita.k-bu@nhk.or.jp
[2] Kyushu University, 744 Motooka, Nishi-ku Fukuoka, Japan
[3] The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo, Japan

Abstract. We propose a short signature scheme under the ring-SIS assumption in the standard model.[†] Specifically, by revisiting an existing construction [Ducas and Micciancio, CRYPTO 2014], we demonstrate lattice-based signatures with improved reduction loss. As far as we know, there are no ways to use multiple tags in the signature simulation of security proof in the lattice tag-based signatures. We address the tag-collision possibility in the lattice setting, which improves reduction loss. Our scheme generates tags from messages by constructing a scheme under a mild security condition that is existentially unforgeable against random message attack with auxiliary information. Thus our scheme can reduce the signature size since it does not need to send tags with the signatures. Our scheme has short signature sizes of $O(1)$ and achieves tighter reduction loss than that of Ducas et al.'s scheme. Our proposed scheme has two variants. Our scheme with one property has tighter reduction and the same verification key size of $O(\log n)$ as that of Ducas et al.'s scheme, where n is the security parameter. Our scheme with the other property achieves much tighter reduction loss of $O(Q/n)$ and verification key size of $O(n)$, where Q is the number of signing queries.

1 Introduction

1.1 Background

Digital signatures are one of the most fundamental cryptographic primitives that guarantee authenticity of electronic documents and are an indispensable component of our digital infrastructure. When using digital signatures, each signer has a pair of keys consisting of one secret (signing) and one public (verification) key. A signer signs a document with the secret key, and the document's authenticity is publicly verifiable with the public key.

The performance of cryptographic primitives, such as digital signatures, can be evaluated using *reduction loss* relative to a difficult problem. Reduction loss is the gap in difficulty between breaking the cryptographic primitive and solving the difficult problem.

⋆ Presently, the author is on loan to the National Institute of Information and Communications Technology.

† A preliminary version of this paper was presented in [28] at ProvSec 2020.

When there is approximately no reduction loss (i.e., when breaking the cryptographic primitive is at least as difficult as solving the difficult problem), the cryptographic primitive is called *tightly secure*. The reduction loss can have a dramatic impact on the scheme's parameters. Lowering the reduction loss of the cryptographic primitive is important because this enables security parameters to be made as small as possible without compromising security.

The model of signature schemes with a random oracle is called the *random oracle model*. It is an ideal framework for discussing the security of cryptosystems, replacing the execution of the hash function $H(\cdot)$ with a query to a random oracle, the output of which is uniformly random. In general, a signature scheme in the *standard model* (i.e., without a random oracle) is superior to that in the random oracle model under the same condition. We now discuss digital signature schemes in the standard model.

In 1994, Shor showed that quantum computers can efficiently solve the integer factorization problem and the discrete logarithm problem [39]. *Post-Quantum Cryptography (PQC)*, which is believed to be resistant to an attack from a quantum computer, is studied worldwide. Lattice-based cryptography has been increasing since the original work of Ajtai and Dwork [2, 3] and that is believed to be a promising candidate for the NIST's call for PQC standards [35]. In July 2020, the third-round finalists of the NIST PQC standardization are announced [36]. The finalists for digital signatures except Rainbow [16] are all lattice-based schemes [17, 19]. Many efficient signature schemes, such as NIST PQC finalists, are built in the random oracle model.

The assumptions used in the composition of the signature are also an important part of the evaluation. The construction of an efficient lattice-based scheme under *a standard assumption* (i.e., general assumption such as the one-wayness of trapdoor permutation or more specific assumption such as the short integer solution (SIS) assumption) with tight reduction loss in the standard model is desirable.

Table 1. Signature schemes under (ring) SIS assumption in standard model: n is security parameter; β is SIS parameter: Q is number of signing queries; and $\epsilon, \delta, \ell, \alpha$, and c are parameters for each scheme. Unit of size in SIS assumption is $\mathbb{Z}_q^n$ and that in ring-SIS assumption is $\mathcal{R}_q$.

Scheme	$\lvert vk\rvert$	$\lvert sk\rvert$	$\lvert sig\rvert$	Reduction loss	Assumption	β
CHKP10 [12]	$O(n)$	$O(n)$	$O(n)$	$O(nQ)$	SIS	$\Omega(n^2)$
Boyen10 [10]	$O(n)$	$O(1)$	$O(1)$	$O(nQ)$	SIS	$\Omega(n^{7/2})$
BHJKSS13 [9]	$O(1)$	$O(1)$	$O(\log n)$	$O(nQ)$	SIS	$\Omega(n^{5/2})$
BKKP15 [8]	$O(1)$	$O(1)$	$O(n)$	$O(1)$	SIS	$\Omega(n^{3/2})$
Alperin-Sheriff15 [4]	$O(1)$	$O(1)$	$O(1)$	$O(nQ)$	SIS	$\Omega(n^{11/2}\delta^{2\delta})$
BL16 [11]	$O(n)$	$O(1)$	$O(1)$	$O(n)$	SIS+PRF	$\Omega(n^{7/2}\ell^{4c})$
DM14 [18]	$O(\log n)$	$O(1)$	$O(1)$	$O\left(\left(\frac{Q^2}{\epsilon}\right)^c\right)$	ring-SIS	$\Omega(n^{7/2})$
Proposed scheme with $C_i = \lfloor \alpha c^i \rfloor$	$O(\log n)$	$O(1)$	$O(1)$	$O\left(\left(\frac{Q}{n}\right)^c\right)$	ring-SIS	$\Omega(n^{7/2})$
Proposed scheme with $C_i = i$	$O(n)$	$O(1)$	$O(1)$	$O\left(\frac{Q}{n}\right)$	ring-SIS	$\Omega(n^{7/2})$

1.2 Related Works

If a signature of lattice-based signature schemes consists of a single lattice vector, i.e., it increases at a rate of order $O(1)$, the size of the signature is called *short*. The direct constructions of short lattice-based signatures were presented by Lyubashevsky and Micciancio [31] and Gentry et al. [22]. Lyubashevsky and Micciancio proposed a provably secure one-time signature scheme in the standard model. Gentry et al. constructed a signature scheme in the random oracle model that uses a sampling algorithm from Gaussian distribution.

We give a comparison of post-quantum signature schemes in the standard model in Table 1. In 2010, Cash et al. [12] provided the first lattice-based signature scheme in the standard model by applying chameleon hash function with reduction loss of $O(nQ)$, where n is the security parameter and Q is the number of signing queries. However, the size of signatures and secret keys of Cash et al.'s scheme are not short. Boyen [10] proposed the *vanishing trapdoor* technique and constructed a short signature scheme in the standard model with reduction loss of $O(nQ)$. The signature and secret key size of Boyen's signature is $O(1)$. In 2013, Böhl et al. [9] formulated the *confined guessing* technique, which is an analyzing technique of security proof. Böhl et al. [9] explored tag-based signature schemes as a means to enable security reductions to standard computational assumptions, such as RSA, CDH, and SIS assumptions. In a tag-based signature scheme, each signature carries tag t that can be chosen freely. The benefit of this additional parameterization becomes apparent when one considers tags from a small domain: if there are only few, i.e., a polynomial number of tags, we could try to guess the tag used in the adversary's forgery in advance. In a signing simulation, a challenge instance is embedded in the signature along with the tag, so that the simulation succeeds when the guessed tag matches the tag used in the forgery. Their scheme has verification and signing keys of size $O(1)$ in the standard model with reduction loss of $O(nQ)$ but longer signatures, of size $O(\log n)$. In 2014, a new short-signature framework using the confined guessing and vanishing trapdoor techniques was proposed by Ducas and Micciancio [18]. We refer their scheme as DM14 hereafter. DM14 has relatively short verification keys of $O(\log n)$ with reduction loss of $O\left(\left(\frac{Q^2}{\epsilon}\right)^c\right)$ for an arbitrary constant $c > 1$ and adversarial advantage ϵ. DM14 focused on a certain tag set and adjusted the size of tag set so that the probability of at least one tag collision is negligible. A short-signature scheme with almost tight security in the standard model using pseudorandom functions was proposed by Boyen and Li. [11] in 2016. Their signature scheme eliminates the reduction loss's dependency on the number of adversary's queries, but their verification key is large and an additional assumption is needed because of using pseudorandom function. A tightly secure signature scheme with short keys in the standard model was proposed by Blazy et al. [8], but its signature size is large. A signature scheme that has short signatures and keys was proposed by Alperin-Sheriff [4], but its reduction loss is loose. Despite these outstanding studies, lattice-based signature schemes that have short signatures, keys, and tight reduction loss in the standard model remain unknown.

1.3 Contributions

We revisit DM14 [18] and apply two ideas to reduce reduction loss of DM14: considering multiple tag collisions and changing the construction of tag sets by applying Kajita et al.'s reduction technique [27]. Concerning tight security reductions, Kajita et al. [27] present a signature scheme with the tightest security reduction among known constant-size signature schemes secure under the computational Diffie-Hellman (CDH) assumption. They first construct a signature scheme, satisfying a security notion denoted as existentially unforgeable against extended random-message attacks (EUF-XRMA). They transform it to an EUF-CMA secure scheme without loosing the tightness by applying Abe et al.'s transformation technique [1].

In confined guessing, colliding with multiple tags is possible in non-lattice settings, such as Diffie-Hellman based and RSA-based, but has not been achieved in the lattice setting. The possibility of using multiple tags in the lattice setting has been an open problem since the confined guessing technique was proposed by Böhl et al. We first address this open problem of confined guessing in the lattice setting, where multiple tags cannot be used in a signature simulation. In order to let the tags collide, signatures must be aggregated and one signature must use multiple tags. However there are no ways to aggregate signatures at the signing simulation of confined guessing in the lattice setting, like Böhl et al.'s optimized CDH-based and RSA-based signature schemes [9]. On the other hand, many lattice-based aggregate signatures have been proposed so far [5, 40, 41, 26, 30]. There are two types of lattice-based aggregate signatures: sequential aggregate signatures (SAS) specifying the order of aggregation [5, 40] and unordered aggregate signatures (UAS) aggregating in random order [41, 30]. When we try to apply the existing aggregation technique to use multiple tags in a signature simulation, it does not work. First of all, the order of aggregation is fixed in SAS, which causes further problems and complications in signature simulation. Furthermore, because SAS uses hash chains [5], it is not suitable for configuration in the standard model. In UAS, signatures are aggregated using a lattice intersection method based on the Chinese Remainder Theorem. It is true that UAS does not specify the order of aggregation, but the use of Chinese Remainder Theorem makes the modulus q exponentially large, which is not a solution. Lattice signatures based on the SIS assumption using the confined guessing technique of Böhl et al. [9, 18] were very effective in achieving compact signatures and key lengths, but had the disadvantage of loose security reduction. We state and prove a new key lemma to indicate the possibility of tag collisions. This achieves a reduction loss of $O(Q)$ smaller than DM14 without any trade-off, where Q is the number of queries.

Next, to further reduce the reduction loss, we use the reduction technique of Kajita et al. [27]. In their technique, by reducing the domain of the tag, the reduction loss can be greatly reduced in exchange for the public key length. Here, we prepare two tag generation parameters with different domains, and consider each of them as a scheme with trade-off properties. This will be explained in detail later. Furthermore, we will use the properties of the security argument proposed by Kajita et al. in their reduction technique to improve the tag generation method. By constructing the tag from a random message, it is not necessary to send the tag with the signature, which leads to slightly smaller signatures.

We now explain the differences between these two ideas in detail, based on the tag generation parameter as mentioned above. Regarding a tag-generation parameter C_i increasing monotonically for an index i, each tag set is constructed as $\{0,1\}^{C_i}$ in DM14's method [18]. The number of elements in the tag sets directly leads to reduction loss in the security proof when using confined guessing because a challenger embeds a challenge problem into a certain target tag and hopes an adversary forges a signature associated with the target tag from the tag sets. We change the construction of tag sets from $C_i = \lfloor \alpha c^i \rfloor$ to $C_i = i$, where $c > 1$ and $\alpha \geq \frac{1}{c-1}$ to select a small tag set in the security proof by applying Kajita et al.'s reduction technique. We present two variants of our proposed signature scheme. The one is with $C_i = \lfloor \alpha c^i \rfloor$, which has a tighter reduction loss of $O\left(\left(\frac{Q}{n}\right)^c\right)$ than that of DM14 and the same verification key size of $O(\log n)$ as that of DM14. The other is with $C_i = i$, which achieves much tighter reduction loss of $O(\frac{Q}{n})$ at the cost of verification key size of $O(n)$. The variants of our signature scheme can be easily switched by changing the value of $C_i = \lfloor \alpha c^i \rfloor$ and $C_i = i$, respectively.

2 Preliminaries

Notation: If S is a set, $a \xleftarrow{\$} S$ denotes sampling a at uniformly random from S. We write $\mathsf{negl}(n)$ to denote an unspecified function $f(n)$ such that $f(n) = n^{-\omega(1)}$, meaning that such a function is negligible in n. For a probabilistic polynomial-time (PPT) algorithm $\mathcal{A}$, we write $y \leftarrow \mathcal{A}(x)$ to denote the experiment of running $\mathcal{A}$ for a given x, selecting an inner coin r uniformly from an appropriate domain, and assigning the results of this experiment to the variable y, i.e. $y = \mathcal{A}(x; r)$. Let $X = \{X_n\}_{n\in\mathbb{N}}$ and $Y = \{Y_n\}_{n\in\mathbb{N}}$ be probability ensembles such that each X_n and Y_n are random variables over $\{0,1\}^n$. The statistical distance between X_n and Y_n is $\mathsf{Dist}(X_n, Y_n) := \frac{1}{2}\sum_{s\in\{0,1\}^n} |\Pr[X_n = s] - \Pr[Y_n = s]|$. We write $X \equiv Y$ if $\mathsf{Dist}(X_n, Y_n) = 0$. We sometimes use a short notation $(\mathbf{A}, \mathbf{B})$ for the result of vertically stacking two matrices $\mathbf{A}$ and $\mathbf{B}$. We write # to denote the number of elements. Let g be a real valued function, we sometimes use a notation of $\tilde{O} = O(g(n)\log^k g(n))$ for some k. We denote $||\mathbf{x}|| = \sqrt{\sum_i x_i^2}$ as the Euclidean norm for $\mathbf{x} = \{x_i\}$.

2.1 Digital Signatures

A digital signature scheme is given by a triple, $\mathsf{SIG} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$, of PPT Turing machines, where for every sufficiently large $n \in \mathbb{N}$, the key-generation algorithm KGen takes as input security parameter 1^n and outputs a pair of verification and signing keys, (vk, sk). Let $\mathcal{M}_n$ be a message space. The signing algorithm Sign takes as input (vk, sk) and a message $m \in \mathcal{M}_n$ and produces a signature σ. The verification algorithm Vrfy takes as input vk, m, and σ, and outputs a verification result bit. For correctness, $\mathsf{Vrfy}(vk, m, \sigma) = 1$, where $\sigma = \mathsf{Sign}(sk, m)$, must hold for any (vk, sk) pair generated with $KGen(1^n)$ and for any $m \in \mathcal{M}_n$.

2.2 Security Classes

EUF-CMA: A digital signature scheme SIG is considered an EUF-CMA [20] if for any adversary $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(n) := \Pr[\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(n) = 1] = \mathsf{negl}(n)$, where $\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(n)$ is defined in Fig. 1. $\mathsf{Sign}_{sk}(\cdot)$ is a signing oracle with respect to sk that takes as input m, returns $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$, and records m to a message list Q_m, which is initially an empty list.

$\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(n)$:
$(vk, sk) \leftarrow \mathsf{KGen}(1^n)$;
$(m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}_{sk}(\cdot)}(vk)$
If $m^* \in Q_m$, then return 0
Return $\mathsf{Vrfy}(vk, m^*, \sigma^*)$.

Fig. 1. Experiment with EUF-CMA.

EUF-XRMA: A SIG is considered an EUF-XRMA [1] with respect to the message generator MsgGen, which is a PPT algorithm that takes as input a message-generation key gk and outputs m and ρ, if for any $\mathcal{A}$ and any positive integer Q, $\mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(n) := \Pr[\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(n) = 1] = \mathsf{negl}(n)$, where $\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(n)$ is defined in Fig. 2, and $Q_m = \{m_1, \ldots, m_Q\}$.

$\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(n)$:
$(vk, sk) \leftarrow \mathsf{KGen}(1^n)$;
$gk \leftarrow \mathsf{Setup}(1^n)$
For $\forall i \in [Q]$,
$(m_i, \rho_i) \leftarrow \mathsf{MsgGen}(gk)$;
$\sigma_i \leftarrow \mathsf{Sign}_{sk}(m_i)$
$(m^*, \sigma^*) \leftarrow \mathcal{A}(vk, \{m_i, \sigma_i, \rho_i\}_{i=1}^{Q})$
If $m^* \in Q_m$, then return 0
Return $\mathsf{Vrfy}(vk, m^*, \sigma^*)$.

Fig. 2. Experiment with EUF-XRMA. Setup algorithm is PPT algorithm that takes as input security parameter 1^n and outputs gk.

2.3 Lattice and Gaussian

A full-rank n-dimensional lattice is the set $\Lambda = \{\mathbf{Bz} : \mathbf{z} \in \mathbb{Z}^n\}$ of all integer combinations of n basis vectors $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}_q^{n \times n}$. For positive integers n and q, let $\mathbf{A} \in \mathbb{Z}_q^{n \times n}$

be arbitrary and define the following full-rank n-dimensional q-ary lattices:

$$\Lambda(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^n : \exists \mathbf{s} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{z} = \mathbf{A}^t\mathbf{s} \mod q\},$$
$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^n : \mathbf{A}\mathbf{z} = 0 \mod q\}.$$

For any $\mathbf{u} \in \mathbb{Z}_q^n$, define the coset (or shifted lattice) as $\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^n : \mathbf{A}\mathbf{z} = \mathbf{u} \mod q\}$.

We consider lattice problems restricted to ideal lattices [33]. We focus on rings of the form $\mathcal{R} = \mathbb{Z}[X]/\Phi_n(X)$ and $\mathcal{R}_q = (\mathcal{R}/q\mathcal{R})$, where n is a power of 2, q is an integer, and $\Phi_n(X) = X^n + 1$ is the cyclotomic polynomial of degree n [32]. For our construction, we require that $\Phi_n(X)$ does not split into low degree polynomials modulo the prime factors of q. More specifically, we choose $q = 3^k$. Note that the lattice dimensions and polynomial orders are the same for the sake of simplicity. The geometric quality of a matrix $\mathbf{A} \in \mathbb{R}^{m \times n}$ is measured by its spectral norm $s_1 = \sup_{\mathbf{x}} ||\mathbf{A}\mathbf{x}||/||\mathbf{x}||$ for every $\mathbf{x} \in \Lambda$.

The n-dimensional Gaussian function $\rho_s : \mathcal{R}^n \to (0, 1]$ is defined as $\rho_s(\mathbf{x}) = \exp(-\pi \cdot ||\mathbf{x}/s||^2)$ for a variance s. For any countable $X \subset \mathcal{R}^n$, let $\rho(X) = \sum_{\mathbf{x} \in X} \rho_s(\mathbf{x})$. The discrete Gaussian distribution $D_{\Lambda,s}$ over a lattice Λ is defined as $D_{\Lambda,s}(\mathbf{x}) = \rho_s(\mathbf{x})/\rho_s(\Lambda)$ for all $\mathbf{x} \in \Lambda$. The discrete Gaussian distribution over n-dimensional row vectors of ring $D_{\mathcal{R},s} := D_{\mathbb{Z},s}^n$ is defined by identifying the ring $\mathcal{R}$ with $\mathbb{Z}^n$ under the coefficient embedding. The discrete Gaussian distribution over the ring $\mathbf{x} \leftarrow D_{\mathcal{R},s}$ is a sub-Gaussian of parameter s. We then define the ring-SIS problem as follows.

Definition 1. *In the SIS over rings problem (*ring-SIS$_{w,q,\beta}$*), one is given a matrix $A \in \mathcal{R}^{1 \times w}$ and asked to find a non-zero vector $\mathbf{x} \in \Lambda_q^{\perp}(\mathbf{A})$ such that $||\mathbf{x}|| \leq \beta$.*

2.4 Lattice Trapdoor

We define lattice trapdoors as follows on the basis of DM14 [18]. For modulus $q = 3^k$ and $n \times n$ identity matrix $\mathbf{I}_n$, we define the gadget matrix $\mathbf{G} = [\mathbf{I}_n|3\mathbf{I}_n|\ldots|3^{k-1}\mathbf{I}_n] \in \mathbb{Z}_q^{n \times kn}$. Because $\mathbf{I}_n$ corresponds with the ring element $1 \in \mathcal{R}_q$, the gadget matrix $\mathbf{G}$ can be regarded as a row vector of the ring elements: $\mathbf{G} = [1, 3, \ldots 3^{k-1}] \in \mathcal{R}_q^{1 \times k}$.

Definition 2. *For any $\mathbf{A} \in \mathcal{R}_q^{1 \times (w+k)}$, and invertible $\mathbf{H} \in \mathcal{R}_q^{1 \times 1}$, a $\mathbf{G}$-trapdoor for $\mathbf{A}$ with $\mathbf{H}$ is a matrix $\mathbf{S} \in \mathcal{R}_q^{w \times k}$ such that $\mathbf{A}\begin{bmatrix}\mathbf{S}\\ \mathbf{I}_k\end{bmatrix} = \mathbf{H}\mathbf{G}$.*

The quality of a $\mathbf{G}$-trapdoor $\mathbf{S}$ is measured by the spectral norm $s_1(\mathbf{S})$. If $\mathbf{S} \leftarrow D_{\mathcal{R},s}^{w \times k}$, then we have $s_1(\mathbf{S}) = s\sqrt{n} \cdot O(\sqrt{w} + \sqrt{k} + \omega(\sqrt{\log n}))$ with overwhelming probability. Let $\mathcal{U}_w$ be the uniform distribution over w-dimensional ring elements. We introduce the following theorem.

Theorem 1.([18]). *There is a polynomial time algorithm* GenTrap$(\mathbf{A}', \mathbf{H}, s)$ *that on inputting a matrix $\mathbf{A}' \in \mathcal{R}_q^{1 \times w}$, $\mathbf{H} \in \mathcal{R}_q$, with parameter $s > \omega(\sqrt{\ln nw})$ outputs a matrix $\mathbf{A}'' \in \mathcal{R}_q^{1 \times k}$ and a $\mathbf{G}$-trapdoor $\mathbf{S} \in \mathcal{R}_q^{w \times k}$ for $\mathbf{A} = [\mathbf{A}', \mathbf{A}'']$ with $\mathbf{H} \in \mathcal{R}_q$ such that $s_1(\mathbf{S}) = s \cdot O(\sqrt{w} + \sqrt{k} + \omega(\sqrt{\log n}))$. In addition, if $w \geq 2(\lceil \log_2 q \rceil + 1)$, then with overwhelming probability over the choice of $\mathbf{A}' \leftarrow \mathcal{U}_w$, the distribution of $\mathbf{A}''$ is statistically close to uniform.*

We introduce the following lemma that any linear combination of $\mathbf{S}$ is also $\mathbf{G}$-trapdoor. For any matrix $X \in \mathcal{R}$, we write the sub-matrix as $X_{[i]}$.

Lemma 1.([18]). *For $i = 0, \ldots, d$, let $\mathbf{S}_{[i]} \in \mathcal{R}_q^{w \times k}$ be a $\mathbf{G}$-trapdoor for $[\mathbf{A}, \mathbf{A}_{[i]}]$ with $\mathbf{H}_{[i]} \in \mathcal{R}_q$, where $\mathbf{A}_{[i]} \in \mathcal{R}_q^{1 \times k}$. Then, any linear combination $\mathbf{S} = \sum_i y_i \cdot \mathbf{S}_{[i]}$ with $y_i \in \mathcal{R}_q$ is a $\mathbf{G}$-trapdoor for $[\mathbf{A}, \sum_i y_i \mathbf{A}_{[i]}]$ with $\mathbf{H} = \sum_i y_i \mathbf{H}_{[i]}$.*

Let us introduce a sampling algorithm from [34].

Corollary 1.([34]). *There is an efficient algorithm $\mathsf{SampleD}(\mathbf{A}, \mathbf{u}_0, \mathbf{S}, s)$ that, on inputting a matrix $\mathbf{A} \in \mathcal{R}_q^{1 \times (w+k)}$, syndrome $\mathbf{u}_0 \in \mathcal{R}_q$, $\mathbf{G}$-trapdoor $\mathbf{S} \in \mathcal{R}_q^{w \times k}$ for $\mathbf{A}$ with invertible $\mathbf{H} \in \mathcal{R}_q$, and parameter $s = \omega(\sqrt{\log n}) \cdot s_1(\mathbf{S})$, produces a sample statistically close to the distribution $D_{\Lambda^{\perp}_{\mathbf{u_0}}(\mathbf{A}),s}$, where $D_{\Lambda^{\perp}_{\mathbf{u_0}}(\mathbf{A}),s}$ is the discrete Gaussian distribution, the variance of which is s and center is $\mathbf{u_0}$.*

2.5 Trapdoor Commitments

We define a trapdoor commitment scheme [14]. Let $\mathsf{TCOM} = (\mathsf{KGen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ be a tuple of the following four algorithms: $\mathsf{KGen}^{\mathsf{tc}}$ is a PPT algorithm that takes as input security parameter 1^n and outputs a pair of keys, one public and one trapdoor $(pk, tk) \leftarrow \mathsf{KGen}^{\mathsf{tc}}(1^n)$; $\mathsf{Com}^{\mathsf{tc}}$ is a PPT algorithm that takes as input pk and m, selects a random $r \leftarrow \mathsf{COIN}^{\mathsf{com}}$ in which $r \in \mathbb{Z}_q$, and outputs a commitment $\mu = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$; $\mathsf{TCom}^{\mathsf{tc}}$ is a PPT algorithm that takes as input 1^n and tk and outputs $(\mu, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^n)$, where χ is auxiliary information; and $\mathsf{TCol}^{\mathsf{tc}}$ is a deterministic polynomial-time algorithm that takes as input tk, μ, χ, and m and outputs r such that $\mu = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$. For example, there are some concrete constructions of lattice-based commitment schemes [29, 6, 15]. We use implicitly them in this paper.

3 Our Intermediate Scheme with Mild Security

In general, the fully secure EUF-CMA signature scheme is constructed from some intermediate mildly secure scheme. We first construct our intermediate signature scheme with EUF-XRMA security from DM14. We apply two ideas to reduce the reduction loss: considering multiple tag collisions and changing the construction of tag sets.

3.1 Tags

Before we describe each idea in more detail, we introduce tags based on DM14. We identify each tag prefix $t = [t_0, \ldots, t_{i-1}] \in \mathcal{T}_i$ with a corresponding ring element $t(X) = \sum_{j<i} t_j X^j \in \mathcal{R}_q$ with binary coefficients $t_j \in \{0, 1\}$. We define the sets of tag prefixes $\mathcal{T}_i = \{0, 1\}^{C_i}$, where C_i is a monotonically increasing constant. For simplicity, we write a tag set to denote $\mathcal{T}_i$. For any full tag $t \in \mathcal{T} = \mathcal{T}_d$ and $i < d$, we write $t_{\leq i} \in \mathcal{T}_i$ for its prefix of length i and $t_{[i]}$ for the (ring) difference $t_{\leq i}(X) - t_{\leq i-1}(X) \in \mathcal{R}_q$. Figure 3 is an example that shows mod operations $t_{\leq i} = m \mod C_i$ when $C_i = i$. Then $t_{[i]}$ is obtained by computing the difference $t_{\leq i}(X) - t_{\leq i-1}(X)$. We demonstrate the following

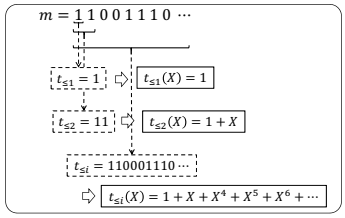

Fig. 3. Example of tags when $C_i = i$

lemma to prove the security of our signature scheme later in this paper. This lemma is almost the same as lemma 1 in [27], but its parameters are different from those of [27] to match the lattice setting. The proof of [27] cannot directly apply to this lemma, so we show the proof of this lemma here.

Lemma 2. *Let $Q = 2^{O(n)}$ and $\psi = \Omega(n)$. If $\#\mathcal{T} > \frac{2eQ}{\psi+1}$,*

$$\Pr[(\psi{+}1)\text{-fold}] := \Pr[\exists i_1, \ldots, i_{\psi+1 \in [Q]} \text{s.t. } t_{i_1} = \cdots = t_{i_{\psi+1}}]$$

is exponentially small in n, where $t_1, \ldots, t_Q$ are independently and uniformly chosen from $\mathcal{T}$ and e denotes the base of the natural logarithm.

Proof. We compute the probability of $\Pr[(\psi+1)\text{-fold}]$ where $\psi+1$ tags are the same from Q elements. We then apply Stirling's approximation and asymptotically estimate the probability.

$$\begin{aligned}
&\Pr[\exists i_1, \ldots, i_{\psi+1} \in [Q] \text{ s.t } t_{i_1} = \cdots = t_{i_{\psi+1}}] \\
&\leq \binom{Q}{\psi+1} \left(\frac{1}{\#\mathcal{T}}\right)^{\psi} \\
&= \frac{Q \cdot (Q-1) \cdots (Q-\psi)}{(\psi+1)!} \left(\frac{1}{\#\mathcal{T}}\right)^{\psi} \\
&\leq \frac{Q^{\psi+1}}{(\psi+1)!} \left(\frac{1}{\#\mathcal{T}}\right)^{\psi} \\
&\leq \frac{Q^{\psi+1}}{\sqrt{2\pi(\psi+1)}} \left(\frac{e}{\psi+1}\right)^{\psi+1} \left(\frac{1}{\#\mathcal{T}}\right)^{\psi} \quad \cdots (*) \\
&= \frac{e \cdot Q}{\sqrt{2\pi(\psi+1)} \cdot (\psi+1)} \left(\frac{e \cdot Q}{\#\mathcal{T}(\psi+1)}\right)^{\psi}.
\end{aligned}$$

Inequality $(*)$ holds by Stirling's approximation

$$\sqrt{2\pi x}\left(\frac{x}{e}\right)^x \leq x! \leq e\sqrt{x}\left(\frac{x}{e}\right)^x.$$

From $\psi = O(n)$ and $Q = 2^{O(n)}$,

$$\frac{e \cdot Q}{\sqrt{2\pi(\psi+1)} \cdot (\psi+1)} = \frac{2^{O(n)}}{O(n^{3/2})}.$$

Now, we set $\#\mathcal{T} > \frac{2eQ}{\psi+1}$ and $\frac{e\cdot Q}{\#\mathcal{T}(\psi+1)} < 1/2$. $\frac{e\cdot Q}{\sqrt{2\pi(\psi+1)}\cdot(\psi+1)}$ is a power of 2 order in n. Hence, $\Pr[(\psi+1)\text{-fold}]$ is exponentially small in n. □

The lemma above is a generalized birthday bound lemma, which often appears in the literature with ψ as a constant number, including [9]. In this case, ψ is not constant and Q is an exponential number, which lead to somewhat different results than those in [9, 18, 27].

3.2 Multiple tag collisions

If we can consider multiple tag collisions, the tag set will be smaller. For example, if the tag set is small, a tag collision will surely occur. On the contrary, if it is sufficiently large, almost no collision will occur. The simulator then uses the tag set so that the probability of tag collisions is negligible and guesses the solution among that tag set, which affects the reduction loss directly. From lemma 2, if we set the tag size $\#\mathcal{T} > \lfloor(2eQ)/(\psi+1)\rfloor$, the probability of ψ tag collisions is negligible. We then present the following key lemma. This key lemma is used as a basis for considering multiple tag collisions in the signature simulation of our signature. The key lemma shows that ψ different simultaneous equations have the same solution in vectors A and B of different sizes chosen randomly.

Lemma 3. *Let* $A = [A'|A''] = [a_1, \ldots, a_{w+k}] \in R_q^{1\times(w+k)}$ *and* $B = [b_1, \ldots, b_k] \in R_q^{1\times k}$. *For* $0 \le i, j \le \psi - 1$ *and* $\psi < k < w$, *there exist* $X \in R_q^{(w+k)\times 1}$ *and* $Y \in R_q^{k\times 1}$ *such that* $AX_\ell - BY_\ell = \cdots = AX_{\ell+\psi-1} - BY_{\ell+\psi-1}$ *and* $X_{\ell+i} \neq X_{\ell+j}$, $Y_{\ell+i} \neq Y_{\ell+j}$.

Proof. For $X_\ell = [x_1, \ldots, x_{w+k}]^T$ and $Y_\ell = [y_1, \ldots, y_k]^T$, let

$$AX_\ell - BY_\ell = v_0.$$

Now we show that $AX_{\ell+i} - BY_{\ell+i} = v_0$. For uniformly chosen $r_{\ell+i} \leftarrow R_q$ and random matrices $Z \in R_q^{w\times 1}$ and $Z' \in R_q^{k\times 1}$, we set $X_{\ell+i}$ and $Y_{\ell+i}$

$$X_{\ell+i} = X_\ell - r_{\ell+i}\left[B^T|Z\right]^T \in R_q^{(w+k)\times 1},$$
$$Y_{\ell+i} = Y_\ell - r_{\ell+i}\left[A'^T + Z'\right] \in R_q^{k\times 1}.$$

From $\psi < k < w$, let $w = ck + d$ for $c \in \mathbb{N}$, $d < k \in \mathbb{N}$. So we have

$$A = [a_1, \cdots, a_k, a_{k+1}, \cdots, a_{ck}, \cdots, a_{ck+d}].$$

We divide A for simplicity as follows:

$$\begin{aligned} A_1 &= [a_1, \cdots, a_k], \\ A_2 &= [a_{k+1}, \cdots, a_{k+k}], \\ &\vdots \\ A_c &= [a_{(c-1)k+1}, \cdots, a_{(c-1)k+k}], \\ A_{c+1} &= [a_{ck+1}, \ldots, a_{ck+d}]. \end{aligned}$$

For $1 \leq i \leq \psi$, we let $X_{\ell+i}, Y_{\ell+i}$ by using X_ℓ, Y_ℓ as follows.

$$X_{\ell+i} = X_\ell - r_{\ell+i} \begin{bmatrix} B^T \\ \vdots \\ B^T \\ b_1 \\ \vdots \\ b_d \end{bmatrix} \in R_q^{(w+k)\times 1}, \tag{1}$$

$$Y_{\ell+i} = Y_\ell - r_{\ell+i} \left(A_1^T + A_2^T + \cdots + A_c^T + \begin{bmatrix} A_{c+1}^T \\ \mathbf{0} \end{bmatrix} \right) \in R_q^{k\times 1}. \tag{2}$$

Note that in the second term of equation (1), B^T is aligned c vertically,and from the relation $w = ck + d$, only d vectors of B are aligned. Then, from (1), (2),

$$\begin{aligned} & AX_{\ell+i} - BY_{\ell+i} \\ = & AX_\ell - BY_\ell - r_{\ell+i} \Big(A_1 B^T + A_2 B^T + \cdots + A_c B^T \\ & + A_{c+1}[b_1, \ldots, b_d]^T - BA_1^T - BA_2^T - \cdots - BA_c^T - B \begin{bmatrix} A_{c+1}^T \\ \mathbf{0} \end{bmatrix} \Big) \\ = & AX_\ell - BY_\ell \\ = & v_0. \end{aligned}$$

Therefore, for $0 \leq i, j \leq \psi - 1$, we get

$$AX_\ell - BY_\ell = \cdots = AX_{\ell+\psi-1} - BY_{\ell+\psi-1}.$$

Finally, we estimate the probability that $X_{\ell+i} = X_{\ell+j}$ and $Y_{\ell+i} = Y_{\ell+j}$ happen. Since $r_{\ell+i}$ is an uniformly randomness, the probability will be exponentially small. Therefore we get $AX_\ell - BY_\ell = \cdots = AX_{\ell+\psi-1} - BY_{\ell+\psi-1}$ and $X_{\ell+i} \neq X_{\ell+j}, Y_{\ell+i} \neq Y_{\ell+j}$ with overwhelming probability. □

3.3 Changing tag construction

DM14 makes the tag sets as $\{0,1\}^{\lfloor \alpha c^i \rfloor}$. In proposed scheme with property 1, we take over their tag setting, so we can also write our proposed scheme with property 1 as proposed scheme with $C_i = \lfloor \alpha c^i \rfloor$. We then make tag sets with small space by applying existing reduction technique [27]. If we can select a small target tag set in the security proof, we can make reduction loss tighter. Kajita et al. [27] improved the reduction loss in trade-off with the public key length by changing the way the domain of the tag. Thus, we then make the tag sets as $\{0,1\}^i$. Although the total number of elements in the tags is as same as DM14, we extend the number of tag sets instead of increasing the number of elements in the tag sets. It is the optimal case that the number of elements in tag sets is minimized at the cost of the number of tag sets because we can select

a certain tag sets considering tag collisions. The increased number of tag sets affects the size of verification keys from $O(\log n)$ to $O(n)$ because the size is commensurate with the number of tag sets. Note that this approach does not affect the security proof because the only target tag set which is carefully selected is used in the security proof. We apply this reduction technique [27] and write the signature scheme as proposed scheme with property 2 or proposed scheme with $C_i = i$. The only difference between our proposed scheme with two properties is the tag-generation parameter C_i, so it can be easily switched by changing C_i.

3.4 Construction

We construct our proposed mildly secure signature scheme (hereafter, SIG_0). SIG_0 is similar to DM14's non-adaptively secure signature scheme [18]. The main differences between SIG_0 and DM14 are the generation of tags from messages and that the tag-generation parameter C_i is variable. Figure 4 illustrates SIG_0. Let k be an arbitrary system parameter. We let $w = 2\lceil \log_2 q \rceil + 2$, $q = 3^k$, and $s = n^{3/2} \cdot \omega(\log n)^{3/2}$ as system parameters. Let the algorithm BtoR in Sign and Vrfy be a function that converts an nk-bit string into a k-dimension vector in $\mathcal{R}_q$. Note that to sign a message m, SIG_0 generates $\{t_{\leq 1}, \ldots, t_{\leq d}\}$ and $\{t_{[1]}, \ldots, t_{[d]}\}$, from m. Now we describe two core sub-algorithms [18, 34] used in our scheme: GenTrap and SampleD.

GenTrap: Let Gaussian parameter $s > \omega(\sqrt{\ln nw})$. For $i = 0, \ldots, d$, according to Theorem 1 and Definition 2, we get $S_{[i]} \leftarrow D_{\mathcal{R},s}^{w \times k}$ from Gaussian distribution with parameter s.We compute $\mathbf{A}_{[\mathbf{i}]}$ as follows;

$$\begin{aligned} & \mathbf{A}_{[i]} \begin{bmatrix} \mathbf{S}_{[\mathbf{i}]} \\ \mathbf{I}_k \end{bmatrix} = \mathbf{H}_{[\mathbf{i}]}\mathbf{G} \\ \iff & \mathbf{A}'\mathbf{S}_{[\mathbf{i}]} + \mathbf{A}_{[i]} = \mathbf{H}_{[\mathbf{i}]}\mathbf{G} \\ \therefore \quad & \mathbf{A}_{[i]} = \mathbf{H}_{[\mathbf{i}]}\mathbf{G} - \mathbf{A}'\mathbf{S}_{[\mathbf{i}]} \end{aligned} \tag{3}$$

At the signing stage, we apply linear combinations by Lemma 1 for the equation (3). For $t_{[i]} \in R_q$, we compute $\mathbf{H}_\mathbf{t}, \mathbf{S}_\mathbf{t}, \mathbf{A}_\mathbf{t}$ as follows;

$$\mathbf{A}_t = [\mathbf{A}' | \mathbf{A}_{[0]} + \sum_{i=1}^{d} t_{[i]} \mathbf{A}_{[i]}]$$

$$\mathbf{H}_t = \mathbf{H}_{[0]} + \sum_{i=1}^{d} t_{[i]} \mathbf{H}_{[i]}$$

$$\mathbf{S}_t = \mathbf{S}_{[0]} + \sum_{i=1}^{d} t_{[i]} \mathbf{S}_{[i]}$$

Then we get

$$\mathbf{A}_t \begin{bmatrix} \mathbf{S}_\mathbf{t} \\ \mathbf{I}_k \end{bmatrix} = \mathbf{H}_\mathbf{t}\mathbf{G}.$$

$\mathsf{KGen}(n)$	$\mathsf{Sign}(vk, sk, m)$	$\mathsf{Vrfy}(vk, m, \boldsymbol{\sigma})$
$\mathbf{A}' \leftarrow \mathcal{R}_q^{1\times w}$	$t_{\leq 0} = 1$	$t_{\leq 0} = 1$
$\mathbf{U} \leftarrow \mathcal{R}_q^{1\times k}$	For $i = 1$ to d	For $i = 1$ to d
$\mathbf{v_0} \leftarrow \mathcal{R}_q$	$t_{\leq i} = m \mod C_i$	$t_{\leq i} = m \mod C_i$
$\{\mathbf{H_{[i]}}\}_{i=0}^{d} \leftarrow \mathcal{R}_q$	$t_{[i]} = (t_{\leq i} - t_{\leq i-1})X^{i-1}$	$t_{[i]} = (t_{\leq i} - t_{\leq i-1})X^{i-1}$
for $i = 0$ to d do	$\mathbf{A}_t = [\mathbf{A}'\|\mathbf{A}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{A}_{[i]}]$	$\mathbf{m} = \mathsf{BtoR}(m)$
$(\mathbf{A_{[i]}}, \mathbf{S_{[i]}}) \leftarrow \mathsf{GenTrap}(\mathbf{A}', \mathbf{H}, s)$	$\mathbf{H}_t = \mathbf{H}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{H}_{[i]}$	compute $\mathbf{A}_t, \mathbf{u}_0$
$\mathbf{A}_{[i]} \leftarrow \mathcal{R}_q^{1\times k}$	$\mathbf{S}_t = \mathbf{S}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{S}_{[i]}$	if $\|\|\boldsymbol{\sigma}\|\| \leq s\sqrt{n(w+k)}$
vk=$(\mathbf{A}', \{\mathbf{A_{[i]}}, \mathbf{H_{[i]}}\}_{\mathbf{i=0}}^{\mathbf{d}}, \mathbf{U}, \mathbf{v_0})$	$\mathbf{m} = \mathsf{BtoR}(m)$	and $\mathbf{A}_t\boldsymbol{\sigma} = \mathbf{u}_0$
$sk = \{\mathbf{S_{[i]}}\}_{\mathbf{i=0}}^{\mathbf{d}}$	$\mathbf{u}_0 = \mathbf{Um} + \mathbf{v_0}$	return 1
return (vk, sk)	$\boldsymbol{\sigma} \leftarrow \mathsf{SampleD}(\mathbf{A}_t, \mathbf{H}_t, \mathbf{S_t}, \mathbf{u}_0, s)$	else
	return $\boldsymbol{\sigma}$	return 0

Fig. 4. SIG_0: EUF-XRMA-secure signature scheme under ring-SIS assumption

SampleD: SampleD [34] is a sampling algorithm that outputs signatures. We explain the necessary equations and the final form of the signature. For $s = \omega(\sqrt{\log n}) \cdot s_1(\mathbf{S_t})$ according to Corollary 1, we choose randomness $\mathbf{p_1} \leftarrow D^{w}_{\mathcal{R}_\Pi, s}$ and $\mathbf{p_2} \leftarrow D^{k}_{\mathcal{R}_\Pi, s}$ from Gaussian distribution with s and get $\mathbf{p} = \begin{bmatrix}\mathbf{p_1}\\ \mathbf{p_2}\end{bmatrix} \in R_q^{(w+k)\times 1}$. This randomness $\mathbf{p}$ is called as a perturbation parameter. We set $w = \mathbf{Gp_2}$ and $w' = \mathbf{A}'(\mathbf{p_1} - \mathbf{S_t p_2})$. For $u_0 \in R_q$, we define v as follows;

$$v = \mathbf{H_t}^{-1}(u_0 - w') - w = \mathbf{H_t}^{-1}(u_0 - \mathbf{A_t p}) \tag{4}$$

Then we perform the Gaussian sampling with s such that

$$\mathbf{Gz} = v \mod q$$

and get $\mathbf{z} \in R_q^k$. Finally SampleD outputs

$$\boldsymbol{\sigma} = \begin{bmatrix}\mathbf{S_t}\\ \mathbf{I_k}\end{bmatrix}\mathbf{z} + \mathbf{p} \in R_q^{(w+k)\times 1}.$$

Correctness: The correctness of SIG_0 is verified in the same manner of DM14 as follows. Because $s = n^{3/2} \cdot \omega(\log n)^{3/2}$, the signature $\boldsymbol{\sigma}$ produced during the signature generation process follows the distribution $D_{\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}_t), s}$ and has a length of at most $s\sqrt{n(w \times k)}$ with overwhelming probability. From (4), (4), (5), and (5),

$$\begin{aligned}\mathbf{A_t}\boldsymbol{\sigma} &= \mathbf{A_t}\left(\begin{bmatrix}\mathbf{S_t}\\ \mathbf{I_k}\end{bmatrix}\mathbf{z} + \mathbf{p}\right) = \mathbf{H_t G z} + \mathbf{A_t p}\\ &= \mathbf{H_t H_t^{-1}}(\mathbf{u_0} - \mathbf{A_t p}) + \mathbf{A_t p} = \mathbf{u_0}.\end{aligned}$$

Thus, $\boldsymbol{\sigma}$ is accepted by the verification algorithm.

3.5 Security Analysis

Let $(m, \chi) \leftarrow \mathsf{MsgGen}$ be the algorithm based on lattices in the EUF-XRMA experiment that runs $(\mu, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^n)$ and outputs a commitment μ as a message m.

Theorem 2. *Under the* ring-SIS$_{w,q,\beta}$ *assumption for* $\beta = \tilde{O}(n^{7/2})$, SIG_0 *is EUF-XRMA secure. More precisely, if there exists an attacker* $\mathcal{A}$ *against EUF-XRMA of* SIG_0 *that runs in time T, makes at most Q queries where* $Q = 2^{O(n)}$ *and succeeds with probability* $\epsilon \geq 2^{-O(n)}$*, then there exists an algorithm* $\mathcal{B}$ *that runs in time* $T' = T + \mathrm{poly}(n)$ *and solves* ring-SIS$_{w,q,\beta}$ *with probability* $\epsilon' = \Omega((\frac{\psi+1}{4eQ})^c) \cdot \epsilon$ *for* $C_i = \lfloor \alpha c^i \rfloor$ *or* $\epsilon' = \Omega(\frac{\psi+1}{4eQ}) \cdot \epsilon$ *for* $C_i = i$ *, where* ψ *is the number of tag-collisions and e denotes the base of the natural logarithm.*

The security proof of Theorem 2 is different in the manner of multiple tag collisions and the tag-generation method from that of DM14 and success probability of the simulation due to tag-generation parameter C_i.

Proof. Suppose that there exists a PPT $\mathcal{A}$ against SIG_0 and MsgGen. We demonstrate that we can construct an algorithm $\mathcal{B}$ that uses $\mathcal{A}$ as an internal sub-algorithm to solve the ring-SIS problem.

Setup: $\mathcal{B}$ receives a ring-SIS challenge $\mathbf{A}' \in \mathcal{R}_q^{1\times w}$. $\mathcal{B}$ then runs MsgGen to receive $\{m^{(j)}, \{t^{(j)}_{[i]}\}_{i=0}^{d}\}_{j=1}^{Q} \leftarrow \mathsf{MsgGen}(1^n)$ as follows. Let us define $\mathcal{M} := \{m^{(j)}\}_{j=1}^{Q}$ and $\mathcal{T}_i := \{0,1\}^{C_i}$ for $i = 0, \ldots, d$. For $j = 1, \ldots, Q$, $\mathcal{B}$ selects message $m^{(j)} \in \{0,1\}^{nk}$ uniformly at random. Then, for $i = 0, \ldots, d$ and $c > 1$, let

$$t^{(j)}_{\leq i} = \begin{cases} 0 & \text{if } i = 0 \\ m^{(j)} \mod C_i & \text{if } i \geq 1 \end{cases}$$
$$t^{(j)}_{[i]} = t^{(j)}_{\leq i}(X) - t^{(j)}_{\leq i-1}(X) \in \mathcal{R}_q$$

$\mathcal{B}$ sets i^* to be as small as possible such that $i^* > \lfloor (2eQ)/(\psi+1) \rfloor$. If $\#\mathcal{T}_{i^*} > \lfloor (2eQ)/(\psi+1) \rfloor$, the probability that event $(\psi+1)$-fold occurs is exponentially small if Q tags are independently and uniformly chosen from $\mathcal{T}_{i^*}$, due to Lemma 2. Let us denote as $(\psi+1)$-fold$^{\mathrm{real}}$ the event that $(\psi+1)$-fold occurs on a tag in $\mathcal{T}_{i^*}$ when $t^{(j)}_{\leq i^*}$ are selected in accordance with the distribution of MsgGen. We show that the statistical distance between the distribution of tags computed by the signed message and uniform distribution is negligible.

Claim. $\Pr[(\psi+1)\text{-fold}^{\mathrm{real}}] = \Pr[(\psi+1)\text{-fold}^{\mathrm{ideal}}] + 2^{-O(n)}$.

Proof of Claim. Let m be a message outputted by MsgGen, which is distributed over R_q. By construction , the distribution of $t^* = m \mod C_i$ is statistically close to the uniform distribution over T_{i^*}, where C_i is the tag-generation parameter. Its distance is bounded by $2^{-O(n)}$. Although independent Q messages are considered, the distance should be still $2^{-O(n)}$. □

$\mathcal{B}$ randomly selects $t^*_{\leq i^*} \xleftarrow{\$} \mathcal{T}_{i^*}$ and can solve the ring-SIS challenge when $\mathcal{A}$ outputs a forged pair $(m^\diamond, \boldsymbol{\sigma}^\diamond)$ such that $t^*_{\leq i^*} = m^\diamond \mod C_{i^*}$. Let

$$\mathcal{M}' := \{m \in \mathcal{M} | t^*_{\leq i^*} = t^{(j)}_{\leq i^*}\}.$$

If $\#\mathcal{M}' \geq \psi + 1$, $\mathcal{B}$ aborts; otherwise, it sets the verification key parameters as follows:

$$\mathbf{H}_{[i]} = \begin{cases} 0 \in \mathcal{R}_q & \text{if i} > \text{i}^*, \\ 1 \in \mathcal{R}_q & \text{if } 1 \leq \text{i} \leq \text{i}^*, \\ -t^*_{\leq i^*} & \text{if i} = 0. \end{cases}$$

For $s' = \omega(\sqrt{\log n})$, $\mathcal{B}$ runs $(\mathbf{A}_{[i]}, \mathbf{S}_{[i]}) \leftarrow \mathsf{GenTrap}(\mathbf{A}', \mathbf{H}_{[i]}, s')$. From Lemma 1, because we have $\mathbf{H}_t = \mathbf{H}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{H}_{[i]} = -t^*_{[i^*]} + \sum_{i=1}^{i^*} t_{[i]} = -t^*_{\leq i^*} + t_{\leq i^*}$, $\mathbf{A}_t \begin{bmatrix} \mathbf{S}_t \\ \mathbf{I} \end{bmatrix} = \mathbf{H}_t\mathbf{G}$ holds for

$$\begin{aligned} \mathbf{S}_t &= \mathbf{S}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{S}_{[i]}, \\ \mathbf{H}_t &= -t^*_{\leq i^*} + t_{\leq i^*}, \\ \mathbf{A}_t &= [\mathbf{A}'|\mathbf{A}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{A}_{[i]}]. \end{aligned}$$

Simulation of keys and signatures: To exploit a forgery, $\mathcal{B}$ selects $\mathbf{S}_\mathbf{U} \leftarrow D^{w\times k}_{\mathcal{R},s'}$. The spectrum norm of $\mathbf{S}_\mathbf{U}$ satisfies $s_1(\mathbf{S}_\mathbf{U}) = \sqrt{n} \cdot \omega(\log n)$. We then have $\mathbf{U} = \mathbf{A}'\mathbf{S}_\mathbf{U}$.

If $t^*_{\leq i^*} \neq t^{(j)}_{\leq i^*}$, $\mathcal{B}$ can run the signing algorithm $\boldsymbol{\sigma}^{(j)} \leftarrow \mathsf{Sign}(sk, m^{(j)})$ because $\mathbf{H}_t = -t^*_{\leq i^*} + t_{\leq i^*} \neq 0$ as the same of DM14.

Otherwise, i.e., $t^*_{\leq i^*} = t^{(j)}_{\leq i^*}$, $\mathbf{H}_t = -t^*_{\leq i^*} + t_{\leq i^*} = 0$ holds. $\mathcal{B}$ must simulate signatures from at most ψ distinct messages. We set $\mathbf{v_0} = \mathbf{A}_t\sigma^{(\ell)} - \mathbf{U}m^{(\ell)}$ for $1 \leq \ell \leq Q$, where $\mathbf{A}_t := [a_1, \ldots, a_{k+w}]$, $\mathbf{U} := [u_1, \ldots, u_k]$. From $\psi < k \leq w$, we set $w = ck + d$ for $c \in \mathbb{N}, d < k \in \mathbb{N}$. For $r^{(\ell+i)} \leftarrow R_q$, we set

$$\sigma^{(\ell+i)} = \sigma^{(\ell)} - r^{(\ell+i)} \begin{bmatrix} \mathbf{U}^T \\ \vdots \\ \mathbf{U}^T \\ u_1 \\ \vdots \\ u_d \end{bmatrix} \in R_q^{(w+k)\times 1},$$

$$m^{(\ell+i)} = m^{(\ell)} - r^{(\ell+i)} \left(\begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix} + \begin{bmatrix} a_{k+1} \\ \vdots \\ a_{k+k} \end{bmatrix} + \cdots + \begin{bmatrix} a_{ck+1} \\ \vdots \\ a_{ck+d} \\ \mathbf{0} \end{bmatrix} \right) \in R_q^{k\times 1}.$$

Then $\mathcal{B}$ selects $m^{(j^*)}$ at random from $\mathcal{M}'$ and sets $m^* = m^{(j^*)}$. For the selected j^*, $\mathcal{B}$ sets $\boldsymbol{\sigma}^* = \boldsymbol{\sigma}^{(j^*)}$.

$\mathcal{B}$ sets $vk = (\mathbf{A}', \mathbf{A}_{[0]}, \ldots, \mathbf{A}_{[d]}, \mathbf{U}, \mathbf{v_0})$. These simulated keys are indistinguishable from real keys. $\mathcal{B}$ feeds $(vk, \{m^{(j)}, \boldsymbol{\sigma}^{(j)}, \{t^{(j)}_{[i]}\}^d_{i=0}\}^Q_{j=1})$ to $\mathcal{A}$.

Correctness when $t^*_{\leq i^*} \neq t^{(j)}_{\leq i^*}$ As defined, from (4), (4), (5), and (5), we have

$$\begin{aligned}\mathbf{A}_t \sigma_j &= \mathbf{A}_t \left(\begin{bmatrix} \mathbf{S}_t \\ \mathbf{I_k} \end{bmatrix} \mathbf{z}_j + \mathbf{p} \right) = \mathbf{H}_t \mathbf{G} \mathbf{z}_j + \mathbf{A}_t \mathbf{p} \\ &= \mathbf{H}_t \mathbf{H}_t^{-1} (u_0 - \mathbf{A}_t \mathbf{p}) + \mathbf{A}_t \mathbf{p} = u_0.\end{aligned}$$

Correctness when $t^*_{\leq i^*} = t^{(j)}_{\leq i^*}$ According to Lemma 3,

$$\begin{aligned}u_0 &= \mathbf{U} m^{(\ell)} + v_0 = \mathbf{U} m^{(\ell)} + \mathbf{A}_t \sigma^{(\ell)} - \mathbf{U} m^{(\ell)} = \mathbf{A}_t \sigma^{(\ell)} \\ u_0 &= \mathbf{U} m^{(\ell+1)} + v_0 = \mathbf{U} m^{(\ell+1)} + \mathbf{A}_t \sigma^{(\ell)} - \mathbf{U} m^{(\ell)} = \mathbf{A}_t \sigma^{(\ell+1)} \\ &\vdots \\ u_0 &= \mathbf{U} m^{(\ell+\psi)} + v_0 = \mathbf{U} m^{(\ell+\psi)} + \mathbf{A}_t \sigma^{(\ell)} - \mathbf{U} m^{(\ell)} = \mathbf{A}_t \sigma^{(\ell+\psi)}\end{aligned}$$

Therefore, all simulated signatures are indistinguishable from real signatures.

$\mathcal{A}$'s forgery: Given $(vk, \{m^{(j)}, \boldsymbol{\sigma}^{(j)}, \{t^{(j)}_{[i]}\}_{i=0}^{d}\}_{j=1}^{Q})$ from $\mathcal{B}$, $\mathcal{A}$ generates a forged signature $(m^\diamond, \boldsymbol{\sigma}^\diamond)$ and feeds it to $\mathcal{B}$.

Exploiting the forgery: $\mathcal{A}$ outputs a forgery $\boldsymbol{\sigma}^\diamond$ for a message $m^\diamond$ of its selection with a probability of at least ϵ. The simulator hopes that $t^\diamond_{\leq i^*} = t^*_{\leq i^*}$ is fulfilled with probability $1/|\mathcal{T}_{i^*}|$. If $t^\diamond_{\leq i^*} \neq t^*_{\leq i^*}$, $\mathcal{B}$ aborts; otherwise, $\mathcal{B}$ computes $\mathbf{A}^\diamond_{\mathbf{t}}$, $u^\diamond_0$ and obtains $\boldsymbol{\sigma} \leftarrow \mathsf{SampleD}(\mathbf{A}_t, u_0, \mathbf{S}, s)$. Because $\mathbf{A}_{t^\diamond} \boldsymbol{\sigma}^\diamond = u^\diamond_0$ holds, $\mathcal{B}$ has $\mathbf{v_0} = \mathbf{A}_{t^\diamond} \boldsymbol{\sigma}^\diamond - u^\diamond_0$. Similarly for $\boldsymbol{\sigma}^*$, $\mathcal{B}$ has $\mathbf{v_0} = \mathbf{A}_{t^*} \boldsymbol{\sigma}^*_1 - u^*_0$. Therefore, $\mathbf{A}_{t^*} \boldsymbol{\sigma}^* - u^*_0 = \mathbf{A}_{t^\diamond} \boldsymbol{\sigma}^\diamond - u^\diamond_0$. Because the condition $t^\diamond_{\leq i^*} = t^*_{\leq i^*}$ ensures $\mathbf{H}_{t^*} = \mathbf{H}_{t^\diamond} = 0$, we derive

$$[\mathbf{A}| - \mathbf{A}\mathbf{S}_{t^*}| - \mathbf{A}\mathbf{S}_{\mathbf{U}}] \cdot \begin{bmatrix} \boldsymbol{\sigma}^*_u \\ \boldsymbol{\sigma}^*_\ell \\ m^* \end{bmatrix} = \mathbf{v_0} = [\mathbf{A}| - \mathbf{A}\mathbf{S}_{t^\diamond}| - \mathbf{A}\mathbf{S}_{\mathbf{U}}] \cdot \begin{bmatrix} \boldsymbol{\sigma}^\diamond_u \\ \boldsymbol{\sigma}^\diamond_\ell \\ m^\diamond \end{bmatrix},$$

where $\boldsymbol{\sigma} = (\boldsymbol{\sigma}_u, \boldsymbol{\sigma}_\ell)$ for the computation. In particular we obtain $\mathbf{A}\mathbf{w} = \mathbf{0}$ for

$$\mathbf{w} = (\boldsymbol{\sigma}^*_u - \boldsymbol{\sigma}^*_\ell - (\mathbf{S}_{t^*} \cdot \boldsymbol{\sigma}^\diamond_u - \mathbf{S}_{t^\diamond} \cdot \boldsymbol{\sigma}^\diamond_\ell) - \mathbf{S}_{\mathbf{U}}(m^* - m^\diamond)).$$

Because $\mathbf{w}$ has at least $\omega(n)$ min-entropy, the probability of $\mathbf{w} = \mathbf{0}$ is $2^{-\Omega(n)}$.

Size of the extracted ring-SIS solution: Because $\mathbf{s}^*$ and $\mathbf{s}^\diamond$ are valid signatures, $||\mathbf{s}^*||, ||\mathbf{s}^\diamond|| \leq n^2 w \cdot \omega(\log n)^{3/2}$. For any tag $t \in \mathcal{T}$, $s_1(\mathbf{S}_t) \leq n^3/2 \cdot \omega(\log n)$. Additionally, $||m^*||, ||m^\diamond|| \leq O(\sqrt{nk})$ and $\mathbf{S}_{\mathbf{U}} \leq \sqrt{n} \cdot \omega(\log n)$. Combining all these bounds, we obtain

$$||\mathbf{w}|| \leq n^{7/2} \cdot \log n \cdot \omega(\log n)^{3/2}.$$

Success probability of the simulation: We denote ϵ_m, ϵ_{nur}, $\epsilon_{t^\diamond=t^*}$, and $\epsilon_{\mathbf{w}=0}$ as follows: ϵ_m is the probability that events $\#\mathcal{M}' \geq \psi + 1$ occur and is exponentially small; $\epsilon_{nur} = 1/2^{\Omega(n)}$ is the advantage of $\mathcal{A}$ that distinguishes between uniformly random distributed tags and simulated tags; $\epsilon_{t^\diamond=t^*}$ is the probability that the forged tag corresponds to the target tag , that is, $1/\#\mathcal{T}_{i^*}$; and $\epsilon_{\mathbf{w}=0}$ is the probability that the ring-SIS solution $\mathbf{w} = 0$ and is exponentially small. After $\mathcal{B}$ feeds all information, messages, signatures, and tags as auxiliary information, the adversary $\mathcal{A}$ returns the forgery $\boldsymbol{\sigma}^\diamond$ for a fresh message $m^\diamond$. If the tag $t^\diamond_{\leq i^*}$ for the forgery corresponds the target tag $t^*_{\leq i^*}$, $\mathcal{B}$ can solve the ring-SIS challenge with probability $1/|\mathcal{T}_{i^*}|$. Therefore, for the advantage of the ring-SIS problem ϵ',

$$\begin{aligned}\epsilon' &\geq (1 - \epsilon_m - \epsilon_{nur}) \cdot \epsilon_{t^\diamond=t^*}(1 - \epsilon_{\mathbf{w}=0}) \cdot \epsilon \\ &\geq \frac{1}{\#\mathcal{T}_{i^*}}\epsilon.\end{aligned}$$

In accordance with Lemma 2, $\mathcal{B}$ chooses $\#\mathcal{T}_{i^*}$ such that $\#\mathcal{T}_{i^*-1} < \frac{2eQ}{\psi+1} < \#\mathcal{T}_{i^*}$ for each case of C_i.

If $C_i = \lfloor \alpha c^i \rfloor$ for $c > 1$ and $\alpha \geq \frac{1}{c-1}$, $\alpha c^i \leq C_i + 1$ holds, then $C_{i^*} \leq \alpha c^{i^*} = c\alpha c^{i^*-1} \leq c(C_{i^*-1} + 1)$. $\mathcal{B}$ sets $\#\mathcal{T}_{i^*}$ as

$$\#\mathcal{T}_{i^*} = 2^{C_{i^*}} \leq 2^{c(C_{i^*-1}+1)} = (2 \cdot 2^{C_{i^*-1}})^c = (2 \cdot \#\mathcal{T}_{i^*-1})^c \leq \left(\frac{4eQ}{\psi+1}\right)^c.$$

Therefore, we get the success probability $\epsilon' \geq \frac{1}{\#\mathcal{T}_{i^*}}\epsilon = \Omega\left(\left(\frac{\psi+1}{4eQ}\right)^c\right)\epsilon$. If $C_i = i$, $\mathcal{B}$ sets $\#\mathcal{T}_{i^*}$ as

$$\#\mathcal{T}_{i^*} = 2^{i^*} \leq 2 \cdot 2^{i^*-1} = 2\mathcal{T}_{i^*-1} \leq \frac{4eQ}{\psi + 1}.$$

Therefore, $\mathcal{B}$ can solve the ring-SIS challenge with success probability $\epsilon' \geq \frac{1}{\#\mathcal{T}_{i^*}}\epsilon = \Omega\left(\frac{\psi+1}{4eQ}\right)\epsilon$. □

4 Our Scheme with Full Security

In this section, we demonstrate the construction of our fully EUF-CMA-secure signature scheme from SIG_0 by applying a generic conversion technique of Abe et al.using trapdoor commitments TCOM [1] as in Kajita et al. [27]. We call TCOM a trapdoor commitment scheme if the following conditions hold.

4.1 Conditions of TCOM

Hiding. For the pk generated with $\mathsf{KGen}^{\mathsf{tc}}(1^n)$, and any $m, m' \in \mathcal{M}_n$, *statistical hiding* holds if the following ensembles are statistically indistinguishable in n:

$$\left\{(\mu, m, r) \mid \mu = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r); r \leftarrow \mathsf{COIN}^{\mathsf{com}}\right\}$$

$$\overset{s}{\approx}\left\{(\mu', m', r') \mid \mu' = \mathsf{Com}^{\mathsf{tc}}_{pk}(m'; r'); r' \leftarrow \mathsf{COIN}^{\mathsf{com}}\right\}.$$

Computationally binding. For any polynomial-time adversary $\mathcal{A}$,

$$\epsilon^{\mathrm{bind}} := \Pr\begin{bmatrix}(m_1, m_2, r_1, r_2) \leftarrow \mathcal{A}(pk); \\ (pk, tk) \leftarrow \mathsf{KGen}^{\mathsf{tc}}(1^n) : \\ \mathsf{Com}^{\mathsf{tc}}_{pk}(m_1; r_1) = \mathsf{Com}^{\mathsf{tc}}_{pk}(m_2; r_2) \wedge (m_1 \neq m_2)\end{bmatrix} = \mathsf{negl}(n).$$

Trapdoor property. The algorithm $\mathsf{KGen}^{\mathsf{tc}}$ for generating pk also outputs a trapdoor tk. There is an efficient algorithm $\mathsf{TCom}^{\mathsf{tc}}$ that, on inputting tk, pk, outputs a commitment μ, and an algorithm $\mathsf{TCol}^{\mathsf{tc}}$ that, on inputting any m, produces r such that $\mu = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$. The distribution of μ computed with $\mathsf{TCom}^{\mathsf{tc}}$ is statistically indistinguishable from that of commitments computed with $\mathsf{Com}^{\mathsf{tc}}$,

$$\left\{(\mu, m, r) \mid \mu = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r); r \leftarrow \mathsf{COIN}^{\mathsf{com}}\right\}$$
$$\overset{s}{\approx}\left\{(\mu, m, r) \mid (\mu, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^n); r = \mathsf{TCol}^{\mathsf{tc}}_{tk}(\mu, \chi, m)\right\}.$$

4.2 Construction

Let SIG_1 be our signature scheme constructed by applying TCOM to SIG_0, as illustrated in Fig. 5. In the signing and verification algorithms of SIG_1, commitments μ are regarded as messages. The correctness of SIG_1 can be demonstrated in the same manner as that of SIG_0.

4.3 Security Analysis

We demonstrate that SIG_1 is EUF-CMA secure with TCOM by constructing adversary $\mathcal{B}^{\mathrm{bind}}$, which breaks the computationally binding of TCOM, or adversary $\mathcal{B}^{\mathrm{euf-xrma}}_{\mathsf{SIG}_0}$, which breaks the EUF-XRMA security. We then show the following theorem. Note that the following theorem does not depend on the tag-generation parameter C_i.

Theorem 3. *If* $\mathsf{TCOM} = (\mathsf{KGen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ *is a trapdoor commitment and* SIG_0 *is EUF-XRMA secure, then* SIG_1 *is EUF-CMA secure.*

Proof. Let $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ be the adversary that can break the EUF-XRMA security of SIG_0, and let $\mathcal{B}^{\mathrm{bind}}$ be the adversary that can break computationally binding for TCOM. Let $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}_1}$ be the adversary that can break EUF-CMA security of SIG_1. Let $\epsilon^{\text{EUF-XRMA}}_{\mathsf{SIG}_0} = \mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0, \mathcal{B}}(n)$ be an advantage of $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$, ϵ^{bind} be an advantage of $\mathcal{B}^{\mathrm{bind}}$, and $\epsilon^{\text{EUF-CMA}}_{\mathsf{SIG}_1} = \mathsf{Adv}^{\text{EUF-CMA}}_{\mathsf{SIG}_1, \mathcal{A}}(n)$ be an advantage of $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}_1}$. We write $\mathcal{B}^{\text{EUF-XRMA with TCOM}}_{\mathsf{SIG}_0}$ as the adversary against EUF-XRMA security with TCOM of SIG_0. We write the verification key and signing key of SIG_1 as (vk, sk) and those of SIG_0 as (vk_0, sk_0). From the view of $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}_1}$, $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ and $\mathcal{B}^{\mathrm{bind}}$ are statistically indistinguishable. We now show that if a $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}_1}$ that can break EUF-CMA security of SIG_1 exists, then $\mathcal{B}^{\text{EUF-XRMA with TCOM}}_{\mathsf{SIG}_0}$ or $\mathcal{B}^{\mathrm{bind}}$ exists.

$\mathsf{KGen}(n)$
$\mathbf{A}' \leftarrow \mathcal{R}_q^{1\times w}$
$\mathbf{U} \leftarrow \mathcal{R}_q^{1\times k}$
$\mathbf{v_0} \leftarrow \mathcal{R}_q$
$\{\mathbf{H_{[i]}}\}_{i=0}^{d} \leftarrow \mathcal{R}_q$
for $i = 0$ to d do
$(\mathbf{A_{[i]}}, \mathbf{S_{[i]}}) \leftarrow \mathsf{GenTrap}(\mathbf{A}', \mathbf{H}, s)$
$\mathbf{A}_{[i]} \leftarrow \mathcal{R}_q^{1\times k}$
$(tk, pk) \leftarrow \mathsf{KGen}^{\mathsf{tc}}(n)$
$vk = (\mathbf{A}', \{\mathbf{A_{[i]}}, \mathbf{H_{[i]}}\}_{\mathbf{i=0}}^{\mathbf{d}}, \mathbf{U}, \mathbf{v_0}, pk)$
$sk = \{\mathbf{S_{[i]}}\}_{\mathbf{i=0}}^{\mathbf{d}}$
return (vk, sk)

$\mathsf{Sign}(vk, sk, m)$
$r \leftarrow \mathsf{COIN}^{\mathsf{com}}$
$\mu = \mathsf{Com}_{pk}^{\mathsf{tc}}(m; r)$
$t_{\leq 0} = 1$
For $i = 1$ to d
$t_{\leq i} = \mu \mod C_i$
$t_{[i]} = (t_{\leq i} - t_{\leq i-1})X^{i-1}$
$\mathbf{A}_t = [\mathbf{A}'|\mathbf{A}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{A}_{[i]}]$
$\mathbf{H}_t = \mathbf{H}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{H}_{[i]}$
$\mathbf{S}_t = \mathbf{S}_{[0]} + \sum_{i=1}^{d} t_{[i]}\mathbf{S}_{[i]}$
$\boldsymbol{\mu} = \mathsf{BtoR}(\mu)$
$\mathbf{u}_0 = \mathbf{U}\boldsymbol{\mu} + \mathbf{v_0}$
$\boldsymbol{\sigma} \leftarrow \mathsf{SampleD}(\mathbf{A}_t, \mathbf{H}_t, \mathbf{S_t}, \mathbf{u}_0, s)$
return $\boldsymbol{\sigma}$

$\mathsf{Vrfy}(vk, m, \boldsymbol{\sigma})$
$\mu = \mathsf{Com}_{pk}^{\mathsf{tc}}(m; r)$
$t_{\leq 0} = 1$
For $i = 1$ to d
$t_{\leq i} = m \mod C_i$
$t_{[i]} = (t_{\leq i} - t_{\leq i-1})X^{i-1}$
$\mathbf{m} = \mathsf{BtoR}(m)$
compute $\mathbf{A}_t, \mathbf{u}_0$
if $||\boldsymbol{\sigma}|| \leq s\sqrt{n(w+k)}$
and $\mathbf{A}_t\boldsymbol{\sigma} = \mathbf{u}_0$
return 1
else
return 0

Fig. 5. SIG_1: EUF-CMA-secure signature scheme with TCOM

Setup: We consider $\mathsf{TCom}_{tk}^{\mathsf{tc}}$ as MsgGen of EUF-XRMA. Then, commitments are generated with auxiliary information such that $(\mu_i, r_i') \leftarrow \mathsf{TCom}_{tk}^{\mathsf{tc}}(1^n)$. The adversary $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ receives the verification key vk_0, commitments μ_i, and signatures $\boldsymbol{\sigma}_i$ of SIG_0 for $1 \leq i \leq Q$ and auxiliary information $\rho_i = (pk, tk, r_i')$, where pk is the public key, tk is the trapdoor key for TCOM, and commitment μ_i satisfies $\mu_i = \mathsf{Com}_{pk}(x_i; r_i')$ for $x_i \in \mathcal{M}_n$. $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ sets $vk = (vk_0, pk)$ and sends vk to $\mathcal{A}_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$.

Signing: $\mathcal{A}_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$ makes Q signing queries. For $1 \leq i \leq Q$, $\mathcal{A}_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$ gives a message m_i to $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$. Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ computes $r_i = \mathsf{TCol}_{tk}^{\mathsf{tc}}(\mu_i, \chi_i, m_i)$, where r_i satisfies $\mu_i = \mathsf{Com}_{pk}^{\mathsf{tc}}(m_i; r_i)$. In accordance with the statistical hiding property of trapdoor commitments, from the view of $\mathcal{A}_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$, the r that is generated by both $\mathsf{COIN}^{\mathsf{com}}$ and $\mathsf{TCol}_{tk}^{\mathsf{tc}}$ are statistically indistinguishable. $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ then returns $(\boldsymbol{\sigma}_i, r_i)$ corresponding to m_i. The signatures that $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ first received as input are regarded as those of SIG_1 since messages can be just replaced with commitments.

Forgery of $\mathcal{A}_{\mathsf{SIG}_1}^{EUF\text{-}CMA}$: $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ receives a forgery $(m^*, \boldsymbol{\sigma}^*, r^*)$ of SIG_1 from $\mathcal{A}_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$, where $m^* \notin \{m_1, \ldots, m_q\}$. $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ then computes commitment $\mu^* = \mathsf{Com}_{pk}^{\mathsf{tc}}(m^*; r^*)$.

Case 1: breaking EUF-XRMA security of $\mathbf{SIG_0}$ In this case, $\mu^* \notin \{\mu_1, \ldots, \mu_Q\}$, $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ outputs $(\mu^*, \boldsymbol{\sigma}^*)$. This means the adversary succeeds in breaking the EUF-XRMA with TCOM security of SIG_0. This goes against the fact that no adversary who breaks the EUF-XRMA security of SIG_0 exists in Theorem 2.

Case 2: breaking computationally binding In this case, $\mu^* \in \{\mu_1, \ldots, \mu_Q\}$, $\mathcal{B}^{\text{bind}}$ outputs (m^*, r^*, m_i, r_i) such that $(\mu^* = \mu_i) \cap (m^* \neq m_i)$ for $1 \leq i \leq Q$. This means $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ succeeds in breaking the computationally binding for trapdoor commitment as $\mathcal{B}^{\text{bind}}$.

Table 2. Comparison between our proposed scheme and DM14

Scheme	Tag collisions	$\lvert\mathcal{T}_i\rvert$	d	$\lvert vk\rvert$	Reduction loss
DM14	1	$2^{\lfloor \alpha c^i \rfloor}$	$\lceil \log_c(\log_2(\frac{2Q^2}{\epsilon}))\rceil$	$O(\log n)$	$(\frac{4Q^2}{\epsilon})^c$
SIG_1 with $C_i = \lfloor \alpha c^i \rfloor$	ψ	$2^{\lfloor \alpha c^i \rfloor}$	$\lceil \log_c(\log_2(\frac{2eQ}{\psi+1}))\rceil$	$O(\log n)$	$(\frac{4eQ}{\psi+1})^c$
SIG_1 with $C_i = i$	ψ	2^i	$\lceil \log_2(\frac{2eQ}{\psi+1})\rceil$	$O(n)$	$\frac{4eQ}{\psi+1}$

Analysis: Suppose that SIG_1 is EUF-CMA secure. Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with TCOM}}$ breaks EUF-XRMA security when $\mu^* \notin \{\mu_1, \ldots, \mu_q\}$, or $\mathcal{B}^{\text{bind}}$ breaks the computationally binding for trapdoor commitments when $\mu^* \in \{\mu_1, \ldots, \mu_Q\}$. Therefore, $\epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}}$ is bounded by the sum of $\epsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}}$ and ϵ^{bind}. Hence,

$$\epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}} \leq \epsilon^{\text{bind}} + \epsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}}.$$

□

4.4 Reduction loss

We discuss the reduction loss in this section. For the advantage of the ring-SIS problem $\epsilon^{\text{ring-SIS}}$, in accordance with Theorems 2,

$$\epsilon^{\text{ring-SIS}} = \frac{1}{\#\mathcal{T}_{i^*}} \cdot \epsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}}.$$

Because $\epsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}} \geq \epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}} - \epsilon^{\text{bind}}$ from Theorem 3,

$$\epsilon^{\text{ring-SIS}} \geq \frac{1}{\#\mathcal{T}_{i^*}} \cdot \left(\epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}} - \epsilon^{\text{bind}}\right).$$

If $C_i = \lfloor \alpha c^i \rfloor$, since $\#\mathcal{T}_{i^*} = \Omega\left(\left(\frac{\psi+1}{4eQ}\right)^c\right)$,

$$\epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}} = O\left(\left(\frac{4eQ}{\psi+1}\right)^c\right) \cdot \epsilon^{\text{ring-SIS}} + \epsilon^{\text{bind}},$$

if $C_i = i$, since $\#\mathcal{T}_{i^*} = \Omega\left(\frac{\psi+1}{4eQ}\right)$,

$$\epsilon_{\mathsf{SIG}_1}^{\text{EUF-CMA}} = O\left(\frac{4eQ}{\psi+1}\right) \cdot \epsilon^{\text{ring-SIS}} + \epsilon^{\text{bind}}.$$

Since the advantage of computationally binding is negligible and $\psi = \Omega(n)$, the whole reduction loss to the ring-SIS problem is $O\left(\left(\frac{Q}{n}\right)^c\right)$ if $C_i = \lfloor \alpha c^i \rfloor$ or $O\left(\frac{Q}{n}\right)$ if $C_i = i$. We give a comparison between our proposed signature scheme with each C_i and DM14 in Table 2. The reduction loss is related to ψ and Q, and there is an asymptotic relation between them, $\psi = O(\log(Q))$. Consequently, we can eliminate ϵ from the reduction loss of DM14, $O\left(\left(\frac{Q^2}{\epsilon}\right)^c\right)$.

5 Conclusion

We developed a short lattice-based signature scheme under the ring-SIS assumption based on DM14. Our proposed signature scheme has a short signature size of $O(1)$, achieves a verification key size of $O(\log n)$, and reduction loss of $O\left(\left(\frac{Q}{n}\right)^c\right)$ when tag-generation parameter $C_i = \lfloor \alpha c^i \rfloor$. Alternately, our proposed signature scheme achieves a verification key size of $O(n)$ and reduction loss of $O\left(\frac{Q}{n}\right)$ when $C_i = i$. Its reduction loss is the tightest among those of known short lattice-based signature schemes with signing keys of $O(1)$ only under the standard assumption (i.e., without pseudorandom functions) in the standard model. We also hope that this paper will contribute to the development of security proofs in the standard model for lattice tag-based signatures.

References

1. M.Abe, N.Chase, B.David, M.Kohlweiss, R.Nishimaki, and M.Ohkubo, Constant-size structure-preserving signatures: Generic constructions and simple assumptions, Journal of Cryptology 29(4), pp. 833-878, Springer, 2016.
2. M.Ajtai, Generating hard instances of lattice problems, In STOC, pp. 99-108, ACM, 1996.
3. M.Ajtai and C.Dwork, A public-key cryptosystem with worst-case/average-case equivalence, In STOC, pp. 284-293, ACM, 1997.
4. J.Alperin-Sheriff, Short Signatures with Short Public Keys from Homomorphic Trapdoor Functions, In PKC, pp. 236-255, Springer, 2015.
5. R. E. Bansarkhani, and J. Buchmann, Towards lattice based aggregate signatures. In International Conference on Cryptology in Africa (pp. 336-355). Springer, Cham, 2014.
6. C.Baum, I.Damgård, V.Lyubashevsky, S.Oechsner, and C.Peikert. More efficient commitments from structured lattice assumptions. In SCN, pp. 368–385. Springer, 2018.
7. D.Boneh, and M.Franklin, Identity-based encryption from the Weil pairing, In CRYPTO , pp. 213-229, Springer, 2001.
8. O.Blazy, S.A.Kakvi, E.Kiltz, and J.Pan, Tightly-secure Signatures from Chameleon Hash Functions, In PKC, pp. 256-279, Springer, 2015.
9. F.Böhl, D.Hofheinz, T.Jager, J.Koch, J.H.Seo, and C.Striecks, Practical Signatures from Standard Assumptions, In EUROCRYPT, pp. 461-485, Springer, 2013.
10. X.Boyen, Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More, In PKC, pp. 499-517, Springer, 2010.
11. X.Boyen, and Q.Li, Towards Tightly Secure Lattice Short Signature and Id-Based Encryption. In ASIACRYPT pp.404-434, Part II, Springer, 2016.
12. D.Cash, D.Hofheinz, E.Kiltz, and C.Peikert, Bonsai trees, or how to delegate a lattice basis. In EUROCRYPT, pp. 523-552, Springer, 2010.

13. B.Chevallier-Mames, and M.Joye, A practical and tightly secure signature scheme without hash function. In CT-RSA, pp. 339-356, Springer, 2007.
14. I.Damgård, Efficient concurrent zero-knowledge in the auxiliary string model. In EUROCRYPT, pp. 418-430, Springer, 2000.
15. I.Damågrd, C.Orlandi, A.Takahashi, and M.Tibouchi, Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices. In Cryptology ePrint Archive, Report 2020/1110, 2020.
16. J. Ding, M. Chen, A. Petzoldt, D. Schmidt, and B. Yang, "Rainbow - algorithm specification and documentation." In Technical Report, NIST, 2019. https://csrc.nist.gov/Projects/post-quantumcryptography/round-3-submissions, Accessed: March. 10, 2021.
17. L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS–Dilithium: Digital signatures from module lattices." In Technical Report, NIST, 2020, https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions, Accessed: March. 10, 2021.
18. L.Ducas, and D.Micciancio, Improved Short Lattice Signature in the Standard Model. In CRYPTO, pp. 335-352, Springer, 2014.
19. P.A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "Falcon: Fast-Fourier lattice-based compact signatures over NTRU", In Technical Report, NIST, 2020. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions,
Accessed: March. 10, 2021.
20. S.Goldwasser, S.Micali, and R.L.Rivest, A Digital Signature Scheme Secure against Adaptive Chosen-Message Attacks. In Journal of Computer Vol.17(2), pp. 281-308, SIAM, 1988.
21. O.Goldreich, Foundations of Cryptography, Volume II - Basic Applications, Cambridge University Press, 2004.
22. C.Gentry, C.Peikert, and V.Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, In STOC, pp. 197-206, ACM, 2008.
23. D.Hofheinz, T.Jager, and E.Knapp, Waters signatures with optimal security reduction, In PKC, pp. 66-83, Springer, 2012.
24. S.Hohenberger, and B.Waters, Realizing hash-and-sign signatures under standard assumptions. In EUROCRYPT, pp. 333-350, Springer, 2009.
25. S.Hohenberger, and B.Waters, Short and stateless signatures from the RSA assumption, In CRYPTO, pp. 654-670, Springer, 2009.
26. Z. Jing, An efficient homomorphic aggregate signature scheme based on lattice. In Mathematical Problems in Engineering, 2014.
27. K. Kajita, K. Ogawa, and E. Fujisaki, A constant-size signature scheme with a tighter reduction from the CDH assumption, In IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 103(1), 141-149, 2020.
28. K.Kajita, K.Ogawa, K.Nuida, T.Takagi, Short Lattice Signatures in the Standard Model with Efficient Tag Generation, In ProvSec, pp. 85-102, Springer, 2020.
29. A.Kawachi, K.Tanaka, and K.Xagawa, Concurrently secure identification schemes based on the worst-case hardness of lattice problems, In ASIACRYPT, pp. 372-389, Springer, 2008.
30. X. Lu, W. Yin, Q. Wen, Z. Jin, and W. Li, A lattice-based unordered aggregate signature scheme based on the intersection method. In IEEE Access, 6, 33986-33994, 2018.
31. V.Lyubashevsky and D.Micciancio, Asymptotically efficient lattice-based digital signatures, In TCC, pp. 37-54, Springer, 2008.
32. V.Lyubashevsky, D.Micciancio, C.Peikert, and A.Rosen, SWIFFT: A modest proposal for FFT hashing, In FSE, pp. 54-72, Springer, 2008.

33. D.Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. In Computational Complexity Conference(CCC), 16(4), pp. 365-411, Schloss Dagstuhl, 2007.
34. D.Micciancio, and C.Peikert, Trapdoors for Lattices: simpler, Tighter, Faster, Smaller, In EUROCRYPT, pp. 700-718, Springer, 2012.
35. National Institute of Standards and Technology, "Post-quantum cryptography," 2019. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography, Accessed: March. 10, 2021.
36. National Institute of Standards and Technology, "Post-quantum cryptography Round 3 submissions," 2020. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions, Accessed: March. 10, 2021.
37. C.Peikert, An efficient and parallel Gaussian sampler for lattices, In CRYPTO, pp. 80-97, Springer, 2010.
38. S.Schage, Tight proofs for signature schemes without random oracles, In EUROCRYPT, pp. 189-206, Springer, 2011.
39. P.W.Shor, Algorithms for quantum computation: Discrete logarithms and factoring, In FOCS, pp. 124-134, IEEE, 1994.
40. Z. Wang, and Q. Wu, A practical lattice-based sequential aggregate signature. In International Conference on Provable Security, pp. 94-109. Springer, Cham, 2019.
41. P. Zhang, J. Yu, and T. Wang, A homomorphic aggregate signature scheme based on lattice. In Chinese Journal of Electronics, 21(4), pp. 701-704, 2012.