A Constant-Size Signature Scheme with a Tighter Reduction from the CDH Assumption

Kaisei Kajita[1], Kazuto Ogawa[1], Eiichiro Fujisaki[2]

[1] Japan Broadcasting Corporation, Tokyo, Japan
{kajita.k-bu, ogawa.k-cm}@nhk.or.jp
[2] Japan Advanced Institute of Science and Technology, Ishikawa, Japan
fujisaki@jaist.ac.jp

Abstract. We present a signature scheme with the tightest security-reduction among known constant-size signature schemes secure under the computational Diffie-Hellman (CDH) assumption. It is important to reduce the security-reduction loss of a cryptosystem, which enables choosing of a smaller security parameter without compromising security; hence, enabling constant-size signatures for cryptosystems and faster computation. The tightest security reduction far from the CDH assumption is $\mathcal{O}(q)$, presented by Hofheinz et al., where q is the number of signing queries. They also proved that the security loss of $\mathcal{O}(q)$ is optimal if signature schemes are "re-randomizable". In this paper, we revisit the non-re-randomizable signature scheme proposed by Böhl et al. Their signature scheme is the first that is fully secure under the CDH assumption and has a compact public key. However, they constructed the scheme with polynomial-order security-reduction loss. We first constructed a new existentially unforgeable againt extended random-message attack (EUF-XRMA) secure scheme based on Böhl et al.'s scheme, which has a tighter security reduction of $\mathcal{O}(q/d)$ to the CDH assumption, where d is the number of group elements in a verification key. We then transformed the EUF-XRMA secure signature scheme into an existentially unforgeable against adaptively chosen-message attack (EUF-CMA) secure one using Abe et al.'s technique. In this construction, no pseudorandom function, which results in increase of reduction loss, is used, and the above reduction loss can be achieved. Moreover, a tag can be generated more efficiently than Böhl et al.'s signature scheme, which results in smaller computation. Consequently, our EUF-CMA secure scheme has a tighter security reduction to the CDH assumption than any previous schemes. [1]

keywords Digital signatures, the CDH assumption, Trapdoor commitment, a Tight security reduction

[1] This is a revised version of the LNCS version of [23], where there are many technical bugs. We have fixed the bugs in this version

1 Introduction

1.1 Background

Digital signatures are the most elemental cryptographic primitives that guarantee authenticity of electronic documents and are analogous to pen-and-ink signatures on physical documents. In digital signatures, each signer has a pair of secret (signing) and public (verification) keys. A signer signs documents by using one secret key, and authenticity of a signature is publicly verifiable with the public key. Digital signatures are widely used in the real world. For example, it is used in transport layer security and e-commerce and so on.

The performance of cryptographic primitives is evaluated by reduction loss to a certain difficult problem. The (security) reduction is a particular way of using a mathematical proof to ensure that a cryptographic primitive is secure. It shows that breaking the primitive is at least as difficult as breaking the difficult problem. Reduction loss is the gap in difficulty between breaking the primitive and breaking the difficult problem. When there is approximately no security-reduction loss, it is called *tight security*. Strictly speaking, if a t-time adversary attacks the scheme with success probability ε, then a t'-time algorithm can be constructed to break some difficult problem with success probability $\varepsilon' = \varepsilon/\theta$ and $t' = k \cdot t + \mathcal{O}(t)$. A cryptographic scheme is tightly secure if θ is a small constant. The constant θ measures the security loss of the security reduction of our primitives from the underlying assumption. In particular θ does not depend on other parameters under the adversary control (e.g. the number of queries, the scheme's security parameter and adversary's own success probability).

When the parameter θ is a small constant only depends on a small polynomial of the security parameter, the cryptographic scheme is called *almost tightly secure*. It is important to reduce the security-reduction loss of a cryptosystem, which enables the choosing of as small a security parameter without compromising security as possible; hence, enabling small security parameters for cryptosytems, i.e., signatures and verification keys, and fast computations of signature generation and verification, etc.

1.2 Related Works

There are many provable digital signature schemes [2, 10, 27, 22, 4, 19, 6, 14, 8]. The security of signature schemes first can only be proven in the random oracle model. Signature schemes in the random oracle model have heuristic security arguments based on the random oracle [16]. Then digital signatures in the standard model are developed. With these schemes, there are two major problems used for security proof, decisional problem, i.e. the decisional Diffie-Hellman (DDH) problem, and search problem, i.e., the Computational Diffie-Hellman (CDH) problem. Generically, search problems are harder than decisional problems, namely, breaking the CDH problem is harder than breaking the DDH problem.

Constant-Size Signature If a signature consists of a (small) constant number of group elements, the size of the signature is called *constant-size*. We discuss constant-size signature schemes in the standard model from now. The digital signatures with a security reduction to decisional problems has been extensively studied last years and its reduction loss to the DDH problem is achieved $\mathcal{O}(l)$, where l is the bit length of a message [12, 18]. There are a few digital signatures secure under the hardness of search problems. Waters proposed a scheme [27] that is efficient and provably secure under the CDH assumption in the standard model. Some digital signatures under the CDH assumption based on Waters' signature scheme have been developed [22, 20, 6, 26, 7]. However, their reduction loss to the CDH problem are not so tight. The loss of security reductions on Waters' signature scheme is $\mathcal{O}(8(l+1)q)$, where q is the number of adversarial signature queries. The technique called programmable hash functions (PHFs) [21] improves the tightness of the security reduction to $\mathcal{O}(\sqrt{l}q)$. To the best of our knowledge, the tightest security reduction to the CDH problem from a constant-size signature scheme is $\mathcal{O}(q)$, presented by Hofheinz et al [20]. They proposed a re-randomizable signature scheme by applying an error-correcting code to Waters' signature scheme. They also proved that the reduction loss of $\mathcal{O}(q)$ is optimal if signature schemes are re-randomizable.

In spite of many of these previous studies, constant-size signatures with a tight reduction to the CDH problem in the standard model remain unknown. If it is not limited to these condition, there are some signature schemes with a tight reduction. Unless a signature is constant-size, there exists a signature scheme with a tight reduction from the CDH assumption was proposed by [8]. Unless a signature scheme is based on the CDH assumption, there exists a constant-size signature scheme with a tight reduction [11]. Unless a signature scheme is in the standard model, there exists a constant signature scheme with a tight reduction [24].

However these either have not constant-size signatures (e.g. $\mathcal{O}(\kappa)$ times the number of group elements in the CDH assumption) [25] or are based on strong assumption (e.g. strong RSA, strong DH) [11], where κ is the security parameter. Although there exist signature schemes with a tight reduction to search problem, they either are based on the random oracle model or have a non-constant size signature. Tree-based signature schemes achieve a tight reduction to search problem but their signature size is not constant. This is an open problem that obtaining a tightly secure and short (i.e. constant-size) signature scheme under the search assumptions (e.g., CDH). In this paper, we focus on the security reduction of constant-size signature scheme can be obtained from the CDH assumption.

1.3 Our Contribution

We present a signature scheme with a tighter security reduction than known constant-size (in the sense that the signature contains constant number of group elements or vectors) signature schemes under the CDH assumption. In this paper, we revisit the non-re-randomizable signature scheme proposed by Böhl et al. [7]. Their scheme has compact public keys at the price of a loose security-reduction

Scheme	Origin	VK Size	Sig. Size	Reduction Loss
Waters	new	$\mathcal{O}(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$\mathcal{O}(\kappa q)$
HK	Waters	$\mathcal{O}(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$\mathcal{O}(\sqrt{\kappa} q)$
HJK	Waters	$\mathcal{O}(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$\mathcal{O}(q)$
BHJKS	new	$\mathcal{O}(\log_c \kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$\mathcal{O}\left(\frac{2^{2+\frac{c}{d}} q^{\frac{c}{d}+c}}{\varepsilon^{\frac{c}{d}}}\right)$
Seo	BHJKS	$\omega(1)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$\mathcal{O}(\kappa q)$
Ours	BHJKS	$\mathcal{O}(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$\mathcal{O}(\frac{\kappa}{q})$

Table 1. Constant-size signature scheme under the CDH assumption in the standard model: κ is the security parameter, $\tau_{\mathbb{G}}$ is the size of group element, $\tau_{\mathbb{F}_p}$ is the size of the exponent, q is the maximum bound of the signing queries, c and d are constants, ε is the success probability of the adversary.

loss. We address that there is a trade-off between public key size and a security-reduction loss in their scheme. Moreover, without a pseudo-random generator and adopting a generic transformation from the scheme with extended random-message-attack security to that with chosen-message-attack security [1], we can obtain a signature scheme with the reduction loss of $\mathcal{O}(q/d)$, where d is the number of group elements in a verification key.

2 Preliminaries

For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \ldots, n\}$. We let $\mathsf{negl}(\kappa)$ denote an unspecified function $f(\kappa)$ such that $f(\kappa) = \kappa^{-\omega(1)}$, saying that such a function is negligible in κ. 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 result of this experiment to the variable y, i.e., $y = \mathcal{A}(x; r)$. Let $X = \{X_\kappa\}_{\kappa \in \mathbb{N}}$ and $Y = \{Y_\kappa\}_{\kappa \in \mathbb{N}}$ be probability ensembles such that each X_κ and Y_κ are random variables ranging over $\{0,1\}^\kappa$. The statistical distance between X_κ and Y_κ is $\mathsf{Dist}(X_\kappa, Y_\kappa) \triangleq \frac{1}{2} \cdot |\Pr_{s \in \{0,1\}^\kappa}[X = s] - \Pr_{s \in \{0,1\}^\kappa}[Y = s]|$. We say that two probability ensembles, X and Y, are statistically indistinguishable in κ, denoted as $X \overset{s}{\approx} Y$, if $\mathsf{Dist}(X_\kappa, Y_\kappa) = \mathsf{negl}(\kappa)$. Let $\mathcal{A}$ and $\mathcal{B}$ be PPT algorithms that both take as input $x \in \{0,1\}^*$. We write $\{\mathcal{A}(x)\}_{\kappa \in \mathbb{N},\, x \in \{0,1\}^\kappa} \overset{s}{\approx} \{\mathcal{B}(x)\}_{\kappa \in \mathbb{N},\, x \in \{0,1\}^\kappa}$ to denote $\{\mathcal{A}(x_\kappa)\}_{\kappa \in \mathbb{N}} \overset{s}{\approx} \{\mathcal{B}(x_\kappa)\}_{\kappa \in \mathbb{N}}$ for every sequence $\{x_\kappa\}_{\kappa \in \mathbb{N}}$ such that $|x_\kappa| = \kappa$.

2.1 Digital Signatures

We use the standard definition of digital signature schemes. 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) $\kappa \in \mathbb{N}$, KGen, the key-generation algorithm, takes as input security parameter 1^κ and outputs a pair of verification and signing keys, (vk, sk). The signing algorithm Sign, takes as input (vk, sk) and

m and produces σ. The verification algorithm Vrfy, takes as input vk, m, and σ, and outputs a verification result bit. For completeness, it is required that for any (vk, sk) pair generated with $\mathsf{KGen}(1^\kappa)$ and for any $m \in \{0,1\}^*$, it holds $\mathsf{Vrfy}(vk, m, \mathsf{Sign}(sk, m)) = 1$.

tag-based signatures A tag-based signature scheme $\mathsf{SIG}_t = (\mathsf{KGen}_t, \mathsf{Sign}_t, \mathsf{Vrfy}_t)$ with message space $\mathcal{M}_\lambda$ and tag space $\mathcal{T}_\lambda$ consists of three PPT algorithms. Key-generation $(vk, sk) \leftarrow \mathsf{KGen}_t(1^\lambda)$ takes as input a security parameter 1^λ and outputs a pair of verification and signing keys (vk, sk). The signing algorithm $\sigma \leftarrow \mathsf{Sign}_t(sk, m, t)$ computes σ on input sk, m, and tag t. The verification algorithm $\mathsf{Vrfy}_t(vk, m, \sigma, t) \in \{0,1\}$ takes vk, m, σ, and t, and outputs a verification result bit. For correctness, we require that for any $\lambda \in \mathbb{N}$, all $(vk, sk) \leftarrow \mathsf{KGen}_t(1^\lambda)$, $m \in \mathcal{M}_\lambda$, $t \in \mathcal{T}_\lambda$, and $\sigma \leftarrow \mathsf{Sign}_t(sk, m, t)$, $\mathsf{Vrfy}_t(vk, m, \sigma, t) = 1$.

Re-Randomizable Signatures Intuitively, re-randomizable signatures [20] have a property that, given vk, m, and valid σ, one can efficiently generate a new σ' that is distributed uniformly over the set of all possible signatures for m under vk.

Formally, let $\mathsf{SIG} = (\mathsf{KGen}, \mathsf{Sign}, \mathsf{Vrfy})$ be a signature scheme. Let us denote the set of σ for m that can be verified correctly under vk by

$$\Sigma(vk, m) = \{\sigma \mid \mathsf{Vrfy}(vk, m, \sigma) = 1\}.$$

We say that SIG is re-randomizable if there is a PPT algorithm *Rerand* such that for all (vk, m, σ) with $\mathsf{Vrfy}(vk, m, \sigma) = 1$, the output distribution of $Rerand(vk, m, \sigma)$ is identical to uniform distribution over $\Sigma(vk, m)$.

2.2 Trapdoor Commitments

We now define a trapdoor commitment scheme [13]. Let $\mathsf{TCOM} = (\mathsf{Gen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ be a tuple of the following four algorithms. The $\mathsf{Gen}^{\mathsf{tc}}$ algorithm is a PPT algorithm that takes as input security parameter κ and outputs a pair of public and trapdoor keys (pk, tk). The $\mathsf{Com}^{\mathsf{tc}}$ algorithm is a PPT algorithm that takes as input pk and m, selects a random $r \leftarrow \mathsf{COIN}^{\mathsf{com}}$, where $\mathsf{COIN}^{\mathsf{com}}$ represents the internal random number 0 or 1, and outputs a $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$. The $\mathsf{TCom}^{\mathsf{tc}}$ algorithm is a PPT algorithm that takes as input tk and outputs $(\psi, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^\kappa)$. The $\mathsf{TCol}^{\mathsf{tc}}$ algorithm is a deterministic polynomial-time algorithm that takes as input $(tk, \psi, \chi, \hat{m})$ and outputs $\hat{r} \in \{0,1\}$ such that $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(\hat{m}; \hat{r})$.

We call TCOM a trapdoor commitment scheme if the following two conditions hold.

Condition 1 ***Trapdoor Collision.*** *For the pk generated with $\mathsf{Gen}^{\mathsf{tc}}(1^\kappa)$, and all $m \in \{0,1\}^{\lambda_m(\kappa)}$, the following ensembles are statistically indistinguishable in*

κ:

$$\Big\{(\psi, m, r) \,|\, r \leftarrow \mathsf{COIN}^{\mathsf{com}}; \psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)\Big\}$$
$$\overset{\mathrm{s}}{\approx}\Big\{(\psi, m, r) \,|\, (\psi, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^\kappa); r = \mathsf{TCol}^{\mathsf{tc}}_{tk}(\psi, \chi, m)\Big\}.$$

Condition 2 ***Computational Binding.*** *For any PPT adversary $\mathcal{A}$,*

$$\varepsilon^{\text{comp-bind}} = \Pr\left[\begin{array}{l} pk \leftarrow \mathsf{Gen}^{\mathsf{tc}}(1^\kappa);\ (m_1, m_2, r_1, r_2) \leftarrow \mathcal{A}(pk) : \\ \mathsf{Com}^{\mathsf{tc}}_{pk}(m_1; r_1) = \mathsf{Com}^{\mathsf{tc}}_{pk}(m_2; r_2) \,\wedge\, (m_1 \neq m_2) \end{array}\right] = \mathsf{negl}(\kappa).$$

2.3 Security class of digital signatures

EUF-CMA A digital signature scheme SIG is said to be existentially unforgeable against adaptively chosen-message attack (EUF-CMA) [17], if for any $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$, where $\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ is defined in Fig. 1.

EUF-XRMA A SIG is said to be existentially unforgeable against extended random-message attack (EUF-XRMA) [1] with respects to the message generator MsgGen, a PPT algorithm that takes as input a message-generation key gk and outputs m, if for any $\mathcal{A}$ and any positive integer n bounded by a polynomial in κ, $\mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$, where $\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ is defined in Fig. 2, and $\mathcal{Q}_m = \{m_1, \ldots, m_n\}$.

2.4 Bilinear Groups

Let $\mathcal{G}$ be a PPT algorithm that, on input of a security parameter 1^κ, outputs a description of bilinear groups $(\mathbb{G}, \mathbb{G}_T, e, q, g)$ [9] such that $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order q, g is a generator of $\mathbb{G}$, and a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ satisfies the following properties:

- (Bilinear:) for any $g, h \in \mathbb{G}$ and any $a, b \in \mathbb{Z}_q$, $e(g^a, h^b) = e(g, h)^{ab}$,
- (Non-degenerate:) $e(g, g)$ has order q in $\mathbb{G}_T$, and
- (Efficiently computable:) $e(\cdot, \cdot)$ is efficiently computable.

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

Fig. 1. Experiment with EUF-CMA. $\mathsf{Sign}_{sk}(\cdot)$ is a signing oracle with respect to sk that takes m and returns $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$ and records m to $\mathcal{Q}_m$, which is initially an empty list.

$$
\begin{array}{|l|}
\hline
\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa): \\
\quad (vk, sk) \leftarrow \mathsf{KGen}(1^\kappa);\ gk \leftarrow \mathsf{Setup}(1^\kappa) \\
\quad \text{For } \forall i \in [n], \\
\qquad (m_i, w_i) \leftarrow \mathsf{MsgGen}(gk);\ \sigma_i \leftarrow \mathsf{Sign}_{sk}(m_i) \\
\quad (m^*, \sigma^*) \leftarrow \mathcal{A}(vk, \{m_i, \sigma_i, w_i\}_{i=1}^n) \\
\quad \text{If } m^* \in \mathcal{Q}_m, \text{ then return } 0 \\
\quad \text{Return } \mathsf{Vrfy}(vk, m^*, \sigma^*). \\
\hline
\end{array}
$$

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

2.5 Computational Diffie-Hellman Assumption

Let g be a group generator of $\mathbb{G}$. We say that the CDH assumption [26] holds if for any PPT algorithm $\mathcal{A}$ the following advantage

$$
\begin{aligned}
\mathsf{Adv}^{CDH}_{\mathcal{A}}(\kappa) &:= Pr\big[\mathcal{A}(q, \mathbb{G}, g, g^\alpha, g^\beta) \rightarrow g^{\alpha\beta} | \alpha, \beta \xleftarrow{\$} \mathbb{Z}_q, g \xleftarrow{\$} \mathbb{G}\big] \\
&= \varepsilon^{CDH}
\end{aligned}
$$

is negligible function in the security parameter κ.

2.6 Pseudorandom Functions

For any set $\mathcal{S}$ a pseudorandom function (PRF) [5] with a range $\mathcal{S}$ is an efficiently computable function $\mathsf{PRF}^{\mathcal{S}} : \{0,1\}^\kappa \times \{0,1\}^* \rightarrow \mathcal{S}$. We may write $\mathsf{PRF}^{\mathcal{S}}_\kappa(x)$ for $\mathsf{PRF}^{\mathcal{S}}(\kappa, x)$ with a key $\kappa \in \{0,1\}^*$. Additionally we require that

$$
\mathsf{Adv}^{\mathsf{prf}}_{\mathsf{PRF}^{\mathcal{S}},\mathcal{A}}(\kappa) := \Big|\Pr\big[\mathcal{A}^{\mathsf{PRF}}_\kappa(\cdot) = 1 \text{ for } \kappa \leftarrow \{0,1\}^*\big] - \Pr[\mathcal{A}^{\mathcal{U}}_{\mathcal{S}}(\cdot) = 1]\Big| = \varepsilon^{\mathsf{PRF}}
$$

is negligible in κ where $\mathcal{U}$ is a truly uniform function to $\mathcal{S}$. We often write PRF, which is omitted from $\mathcal{S}$.

2.7 Scheme of Böhl et al.

We now revisit the signature scheme [7] proposed by Böhl et al. They present a new paradigm for the construction of efficient signature schemes secure under standard computational assumptions. First, they define a mild security for signature schemes that is much easier to achieve than full security. We consider EUF-CMA security as full security. They present efficient mildly secure schemes under the CDH assumption in pairing-friendly groups. Concretely, they construct an EUF-dnaCMA secure signature scheme by using a SIG_t, which is EUF-dnaCMA$^*_{\mathrm{d}}$ secure, and a PRF, which is a PRF. Moreover, they applied trapdoor commitment and modified the EUF-dnaCMA secure signature scheme and achieved an EUF-CMA secure signature scheme under the CDH assumption. Therefore, they constructed a full secure signature scheme generically from a mildly secure signature one. They constructed the signature scheme that is secure against non-adaptive attack by using PRFs. Pseudorandom functions affect security-reduction loss. In their security proof, they use the *confined guessing* technique. They choose an appropriately sized tag set, where their signature simulation is done.

Theorem 1. *If* PRF *is a PRF and a* SIG_t *is* EUF-dnaCMA$^*_\mathrm{d}$ *secure, then there is an* EUF-dnaCMA$^*_\mathrm{d}$ *secure* SIG*. Concretely, let* $\mathcal{A}$ *be a PPT adversary against a SIG with at most q signature queries and having advantage* $\varepsilon := \mathsf{Adv}^{\text{EUF-dnaCMA}}_{\mathsf{SIG}_t,\mathcal{A}}(\kappa)$*. Then there exists an* EUF-dnaCMA$^*_\mathrm{d}$ *adversary* $\mathcal{A}'$ *against the* SIG_t *that makes* $q'(\kappa) \leq 2 \cdot \{\frac{2 \cdot q^{d+1}}{\varepsilon(\kappa)}\}^{c/d} + l \cdot q$ *signature queries and has advantage* $\varepsilon' := \mathsf{Adv}^{\text{EUF-dnaCMA}^*_\mathrm{d}}_{\mathsf{SIG}_t,\mathcal{A}'}(\kappa)$ *and PRF distinguisher with advantage* $\varepsilon_{\mathsf{PRF}}$ *such that*

$$\varepsilon' \geq \varepsilon/2 - \varepsilon^{\mathsf{PRF}} - \frac{p'(\kappa)}{|\mathcal{M}_k|}$$

for infinitely large κ*, where* $p'(\kappa)$ *is a suitable polynomial and* $\mathcal{M}_k$ *denotes the message space.*

Lemma 1. *Let* T *be a tag set with* $|T| = n$*. Let* $t_1, \ldots, t_q$ *be* q *independent random variables taken uniformly random from* T*. Then, the probability that there exist* $d+1$ *pairwise distinct indices* $i_1, \ldots, i_{d+1}$ *such that* $t_{i_1} = \cdots = t_{i_{d+1}}$ *is upper bounded by* $\frac{q^{d+1}}{n^d}$*.*

Theorem 2. *The* SIG_t *is* EUF-dnaCMA$^*_\mathrm{d}$ *secure if the CDH assumption holds in* $\mathbb{G}$*. Let* $\mathcal{A}$ *be a PPT adversary on* SIG_t *with advantage* $\varepsilon := \mathsf{Adv}^{\text{EUF-dnaCMA}^*_\mathrm{d}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ *with at most q random messages along with signatures. Then, it can be used to solve the CDH problem with probability of at least* ε/q'*, where* q' *denotes the number of distinct tags queried by* $\mathcal{A}$*.*

Theorem 3. *If the CDH assumption holds in* $\mathbb{G}$*, then the signature scheme with trapdoor commitments* $\mathsf{SIG}^{\mathcal{B}}_t$ *is* EUF-CMA *secure. Let* $\mathcal{A}$ *be a PPT adversary on* $SIG^{\mathcal{B}}_t$ *with advantage* $\varepsilon := \mathsf{Adv}^{\text{EUF-dnaCMA}^*_\mathrm{d}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ *querying for q random messages along with signatures. Then, it can be used to solve the CDH problem with probability of at least* $\frac{2^{2+\frac{c}{d}} \cdot q^{c+\frac{c}{d}}}{\varepsilon^c d+1-2\varepsilon^c d(\varepsilon_{\mathsf{PRF}}+\varepsilon^{\text{comp-bind}})}$*, where* $\varepsilon_{\mathsf{PRF}}$ *and* $\varepsilon^{\text{comp-bind}}$ *correspond to the advantages for breaking the* PRF *and computational binding, respectively, and* $c > 1$ *denotes a granularity parameter in which the size of tag spaces is defined by* $T^i = 2^{\lceil c^i \rceil}$*.*

There are some changes of notation between our signature scheme and Böhl et al.'s signature scheme. We omit these proofs. Please visit [7] for details of these proofs.

3 Proposal: Modified Mildly Secure Signature Scheme

We modify Böhl et al.'s signature scheme and reduced it to the CDH assumption more efficiently. We first construct an EUF-XRMA secure signature scheme under the CDH assumption based on Böhl et al.'s signature scheme [7].

– Böhl et al. transformed EUF-dnaCMA$_{\mathrm{d}}^{*}$ secure signature schemes to EUF -CMA secure ones. We first construct a EUF-XRMA secure signature scheme based on theirs. We transform it to an EUF-CMA secure signature scheme with trapdoor commitments using Abe et al.'s technique[1]. In this way, we construct a new *non*-re-randomizable signature scheme since re-randomizable signature scheme has a property that bounds of security-reduction loss to the CDH problem is $\mathcal{O}(q)$.
– We construct this signature scheme without a PRF. In an experiment with EUF-XRMA security, messages are generated by a message generator MsgGen instead of the PRF. The PRF affects security-reduction loss, but the MsgGen does not. Consequently, the security-reduction loss of our scheme improves when PRF disappears.
– In Böhl et al.'s signature scheme, the tag space is divided into $|T_j| = 2^{\lceil c^j \rceil}$. While in our construction, we make the tag space stepwise $|T_j| = 2^j$ and set a tag by using modulo operation $t^{(j)} = m \mod 2^j$, where m is generated by the MsgGen. We can choose the size of the tag set T_j adequately and prepare T_j to be as small as possible so that any q signatures can be produced from q messages.
– We evaluate the condition under which an identical tag t is generated from distinct messages ms in the signature simulation more strictly. In Böhl et al.'s lemma 1, the probability of condition $\Pr[(d+1)\text{-fold}]$ is negligible. Since we change the parameter size of tag sets and the number of tag collisions d, we evaluate the lemma again with the parameter d, which results in exponentially small $\Pr[(d+1)\text{-fold}]$.

3.1 Construction

SIG_0 is an EUF-XRMA secure signature scheme under the CDH assumption and described in Fig.3. Tag sets are generated along with the following tag-making rule. Each T_j is set as $\{0,1\}^j$ $(1 \leq j \leq l)$, and each tag in T_j is determined as $t_i^{(j)} = m_i \mod 2^j$ for $1 \leq i \leq q$ by using an m_i. This scheme does not require a PRF, unlike that by Böhl et al. [7]. In the EUF-XRMA experiment, messages $\{m_i\}_{i=1}^n$ are generated by MsgGen uniformly. Thus, tag $t^{(j)}$ is also distributed uniformly. We assume that $\mathbb{G}$ and $\mathbb{G}_T$ are groups of prime orders and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is an efficiently computable non-degenerate bilinear map. We let $l = \omega(\log \kappa)$ and $d = O(\kappa)$ for public parameters.

3.2 Security Analysis

We first show the following lemma used in the security proof of SIG_0 then prove that SIG_0 is secure under the CDH assumption.

Lemma 2. *Let T be a set with $|T| = n$. Let $t_1, \ldots, t_q$ be q independent random variables, taken uniformly random from T. Then, let $q = O(poly(\kappa))$, $d = O(\kappa)$. For $n > \frac{e \cdot q}{d+1}$,*

$$\Pr[\exists i_1, \ldots, i_{d+1} \in [q] \mid t_{i_1} = \cdots = t_{i_{d+1}}]$$

is exponentially small in κ, where e is the base of the natural logarithm.

$\mathsf{KGen}(1^\kappa)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vrfy}(vk, m, \sigma)$
set $\mathbb{G}$ $\ s.t.\ \lvert\mathbb{G}\rvert = p$	$r \leftarrow \mathbb{Z}/p\mathbb{Z}$	For $j := 1$ to ℓ do
$T^{(j)} = \{0,1\}^j$	$u(m) = \sum_{i=0}^{d} u_i^{m^i}$	$t^{(j)} = m \mod 2^j$.
$\alpha \leftarrow \mathbb{Z}_p$	$T^{(j)} = \{0,1\}^j$	If $e(\sigma_0, g)$
$(g, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}) \leftarrow \mathbb{G}$	$t^{(j)} = m \mod 2^j$	$\neq e(u(m), g^\alpha)e(z(m)h, \sigma_1)$
$sk = \alpha$	$z(m) = \prod_{j=1}^{l} z_j^{t^{(j)}}$	return 0
$vk = (g, g^\alpha, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l})$	$\sigma_0 = u(m)^\alpha (z(m)h)^r$	else
return (vk, sk)	$\sigma_1 = g^r$	return 1
	return $\sigma = (\sigma_0, \sigma_1)$	

Fig. 3. SIG_0: EUF-XRMA-secure signature scheme under the CDH assumption

Proof.

$$
\begin{aligned}
&\Pr[\exists i_1, \ldots, i_{d+1} \in [q] \mid t_{i_1} = \cdots = t_{i_{d+1}}] \\
&= {}_q\mathrm{C}_{d+1} \left(\frac{1}{n}\right)^d \\
&= \frac{q!}{(q-(d+1))!(d+1)!} \left(\frac{1}{n}\right)^d \\
&= \frac{q \cdot (q-1) \cdots (q-d)}{(d+1)!} \left(\frac{1}{n}\right)^d \\
&\leq \frac{q^{d+1}}{(d+1)!} \left(\frac{1}{n}\right)^d \quad \cdots (*) \\
&\leq \frac{q^{d+1}}{\sqrt{2\pi(d+1)}} \left(\frac{e}{d+1}\right)^{d+1} \left(\frac{1}{n}\right)^d \quad \cdots (**) \\
&= \frac{e \cdot q}{\sqrt{2\pi(d+1)}(d+1)} \left(\frac{e \cdot q}{n(d+1)}\right)^d
\end{aligned}
$$

where Inequation $**$ holds by Stirling's approximation

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

Now, we set $n > \frac{eq}{d+1}$ then $\frac{e \cdot q}{n(d+1)} < 1$ and $\frac{e \cdot q}{\sqrt{2\pi(d+1)}(d+1)}$ is polynomial in κ.

Hence, $\Pr[\exists i_1, \ldots, i_{d+1} \in [q] \mid t_{i_1} = \cdots = t_{i_{d+1}}]$ is exponentially small in κ. $\square$

Böhl et al. assumed that d is constant and showed that the probability $\Pr[\exists i_1, \ldots, i_{d+1} \in [q] \mid t_{i_1} = \cdots = t_{i_{d+1}}]$ is bounded by $\frac{q^{d+1}}{n^d}$. However, d is not necessarily constant. When assuming $d = \mathcal{O}(\kappa)$, $(d+1)!$ in Inequation $*$, which is also in the proof of lemma 1, cannot be ignored. Lemma 2 shows that the $(d+1)$-fold probability is exponentially small when q tags $\{t_i^{(j)}\}_{i=1}^{q}$ are chosen from T_j. This is a key lemma since this probability affects reduction loss.

This modification makes the vk size increased but our security reduction tighter than that of Böhl et al.'s scheme.

Theorem 4. *If the CDH assumption holds in $\mathbb{G}$, then SIG_0 is EUF-XRMA secure. Concretely, let $\mathcal{A}$ be a PPT adversary against SIG_0 with advantage $\varepsilon^{\text{EUF-XRMA}}$ $:=\mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ and let $\mathcal{A}$ have at most q random messages and their corresponding signatures. Then, another adversary $\mathcal{B}$, which can solve the CDH problem with probability of at least $\mathcal{O}(\frac{d}{q})$, can be constructed using $\mathcal{A}$.*

Proof. Suppose that there exists an $\mathcal{A}$ that has at most q random messages and corresponding signatures, and outputs a valid forged signature with probability $\varepsilon^{\text{EUF-XRMA}}$. We show that we can construct another adversary $\mathcal{B}$ that uses $\mathcal{A}$ as an internal sub-algorithm to solve the CDH problem.

Let $\varepsilon^{\text{EUF-XRMA}}$ be $\mathcal{B}$'s advantage in the EUF-XRMA experiment.

Setup Adversary $\mathcal{B}$ receives a CDH challenge $(g, g^{\alpha}, g^{\beta}) \in \mathbb{G}^3$ as an instance of the CDH problem. It then generates q random messages $m_i \leftarrow \mathsf{MsgGen}(gk)$; $gk \leftarrow \mathsf{Setup}(1^{\kappa})$ for $1 \le i \le q$, defines tag sets $T^{(j)} = \{0,1\}^j$, and generates tags $t_i^{(j)} \in T^{(j)}$ from message m_i,

$$t_i^{(j)} = m_i \bmod 2^j \quad \text{for } 1 \le i \le q,\ 1 \le j \le l.$$

Note that $t_i^{(j)}$ is not t_i to the j-th power, and $l = \omega(\log_2 \kappa)$. $\mathcal{B}$ chooses the challenge instance j^* such that the probability of a $(d+1)$- tag collision Pr[$(d+1)$-fold] is exponentially small, i.e.,

$$\Pr[\{\exists i_1, \ldots, i_{d+1}\} \subseteq [q] : t_{i_1}^{(j^*)} = \cdots = t_{i_{d+1}}^{(j^*)} \mid \forall i \in [q] : t_i^{(j^*)} \leftarrow T^{(j^*)}]$$

is exponentially small such that $|T^{(j^*)}|$ is polynomial in κ. Thus, $j^* := \lfloor \log(\frac{e \cdot q}{d+1}) \rfloor$ $+1$ for $|T^{(j^*)}| = \lfloor (e \cdot q/(d+1) \rfloor + 1$ is an index that fulfills these conditions (see lemma 2).

Adversary $\mathcal{B}$ chooses $\tilde{t} \in T^{(j^*)}$ randomly and $m_{i_1}, \ldots, m_{i_d}$ such that $t_{i_1}^{(j^*)} = \cdots = t_{i_d}^{(j^*)} = \tilde{t}$. It can choose at most d messages $m_{i_1}, \ldots, m_{i_d}$ which have the same tag $\tilde{t}$ with probability 1, except exponentially small probability according to Lemma 2. It then constructs a polynomial:

$$f(X) = \prod_{i=1}^{d} (X - m_i) = \sum_{i=0}^{d} \mu_i X^i \ \in \ \mathbb{Z}_p[X] \ ,$$

where coefficients $(\mu_0, \ldots, \mu_d)$ in $\mathbb{Z}_p$ and $f(X) = 1$ for $d = 0$. Note that $f(X) = 0$ for $m_i, \ldots, m_{i_d}$. Adversary $\mathcal{B}$ chooses random exponents $(r_0, \ldots, r_d, x_{z_1}, \ldots, x_{z_l},$ $x_h) \in \mathbb{Z}_p$, where the index $z_1, \ldots, z_l \subseteq [l]$, and defines

$$r(X) = \sum_{i=0}^{d} r_i X^i,$$

$$u(X) = (g^{\beta})^{f(X)} g^{r(X)},$$
$$z(X) = (g^{\beta})^{\tilde{t}} g^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}}} \mid t^{(j)} = X \mod 2^j,$$

using the instance of the CDH problem.

Adversary $\mathcal{B}$ then generates a vk. Concretely, $\mathcal{B}$ chooses $\check{t} \in T^{(j^*)}$ such that $\tilde{t} \neq \check{t}$ and generates coefficients μ_i and h as follows:

$$u_i = (g^{\beta})^{\mu_i} g^{r_i} \ (i = 0, \ldots, d),$$
$$h = (g^{\beta})^{-\check{t}} g^{x_h}.$$

Moreover, $\mathcal{B}$ chooses g^{α} from the CDH instance and generates a $vk = (g, g^{\alpha}, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}, h)$.

Adversary $\mathcal{B}$ then creates q signatures $\sigma_1, \ldots, \sigma_q$ for q messages $m_1, \ldots, m_q$. Let $\hat{t}$ be a tag for a message $\hat{m}$. For $\hat{m} \in \{m_1, \ldots, m_q\}$, let $\hat{t} = \hat{m} \mod 2^{j^*}$. If $\tilde{t} \neq \hat{t}$, then $f(\hat{m}) \neq 0$ since $f(X)$ does not have $m_{i_1}, \ldots, m_{i_d}$ as a root, which maps to $\tilde{t}$. There are two cases according to the value of $\tilde{t}$; $\tilde{t} = \hat{t}$ or $\tilde{t} \neq \hat{t}$.

When $\hat{t} = \tilde{t}$, then $\mathcal{B}$ chooses a random $r \leftarrow \mathbb{Z}_p$ and computes a signature $\hat{\sigma} = (\hat{\sigma}_0, \hat{\sigma}_1)$ as follows:

$$\hat{\sigma}_0 = (g^{\alpha})^{r(\hat{m})} (z(\hat{m})h)^r,$$
$$\hat{\sigma}_1 = g^r.$$

From the definition of SIG_0, $\hat{\sigma}_0 = u(\hat{m})^{\alpha} (z(\hat{m})h)^r, g^r)$. In fact,

$$\begin{aligned}\hat{\sigma}_0 &= (u(\hat{m})^{\alpha} (z(\hat{m})h)^r, g^r) \\ &= \left((g^{\beta})^{f(\hat{m})} g^{r(\hat{m})}\right)^{\alpha} (z(\hat{m})h)^r.\end{aligned}$$

In case that $\hat{t} = \tilde{t}$, $f(\hat{m}) = 0$. Then

$$\hat{\sigma}_0 = (g^{\alpha})^{r(\hat{m})} (z(\hat{m})h)^r.$$

When $\tilde{t} \neq \hat{t}$, then $\mathcal{B}$ chooses a random $r \leftarrow \mathbb{Z}_p$ and computes a signature $\hat{\sigma} = (\hat{\sigma}_0, \hat{\sigma}_1)$ as follows:
Let $S = g^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}} + x_h}$, $\hat{r} = \frac{-\alpha f(\hat{m})}{\tilde{t} - \check{t}} \mod p$, $r' \leftarrow \mathbb{Z}_p$, and $r = \hat{r} + r' \mod p$.

$$\hat{\sigma}_0 = (g^{\alpha})^{r(\hat{m})} (g^{\beta})^{r'(\tilde{t} - \check{t})} S^r$$
$$\hat{\sigma}_1 = g^r.$$

Note that $r \in \mathbb{Z}_p$ is uniformly distributed since r' is chosen at random.

From the definition of SIG_0, $\hat{\sigma}_0 = u(\hat{m})^{\alpha} (z(\hat{m})h)^r, g^r)$. In fact,

$$\begin{aligned}\hat{\sigma}_0 &= u(\hat{m})^{\alpha} (z(\hat{m})h)^r \\ &= (g^{\beta f(\hat{m}) + r(\hat{m})})^{\alpha} \{(g^{\beta})^{\tilde{t}} g^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}}} (g^{\beta})^{-\check{t}} g^{x_h}\}^r \\ &= (g^{\beta f(\hat{m}) + r(\hat{m})})^{\alpha} \{g^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}}} (g^{\beta})^{(\tilde{t} - \check{t})} g^{x_h}\}^r\end{aligned}$$

$$
\begin{aligned}
&= (g^{\alpha})^{r(\hat{m})} (g^{r})^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}} + x_h} (g^{\alpha\beta})^{f(\hat{m})} (g^{\beta})^{(r' - \frac{\alpha f(\hat{m})}{\tilde{t} - t^*})(\tilde{t} - \check{t})} \\
&= (g^{\alpha})^{r(\hat{m})} (g^{r})^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}} + x_h} (g^{\alpha\beta})^{f(\hat{m})} (g^{\beta})^{r'(\tilde{t} - t^*)} (g^{\alpha\beta})^{-f(\hat{m})} \\
&= (g^{\alpha})^{r(\hat{m})} (g^{r})^{\sum_{j=1}^{l} x_{z_j}^{t^{(j)}} + x_h} (g^{\beta})^{r'(\tilde{t} - t^*)} \\
&= (g^{\alpha})^{r(\hat{m})} (g^{\beta})^{r'(\tilde{t} - t^*)} S^{r}.
\end{aligned}
$$

$\mathcal{B}$ then sends $(vk, \{m_i, \sigma_i\}_{i=1}^{q})$ to $\mathcal{A}$.

Forgery Adversary $\mathcal{A}$ receives q message and signature pairs $(m_1, \sigma_1), \ldots, (m_q, \sigma_q)$ from $\mathcal{B}$. After that, $\mathcal{A}$ generates a forged signature $\sigma^* = (\sigma_0^*, \sigma_1^*)$ on m^* and returns (m^*, σ^*) to $\mathcal{B}$.

Solution of the CDH problem Adversary $\mathcal{B}$ derives the solution of the CDH problem using (m^*, σ^*).

When $\mathcal{A}$ succeeds in the forgery, $m^* \notin \{m_1, \ldots, m_q\}$; hence $f(m^*) \neq 0$. Adversary $\mathcal{B}$ then calculates a tag t^* of m^*. If $t^* \neq \tilde{t}$, then it aborts; otherwise, it outputs the solution of the CDH problem $g^{\alpha\beta}$ as follows:

$$
\left(\frac{\sigma_0^*}{(g^{\alpha})^{r(m^*)} (\sigma_1^*)^{(\sum_{j=1}^{l} x_{z_j} {}^{t^{(j)}} + x_h)}} \right)^{-f(m^*)} = g^{\alpha\beta}.
$$

The simulation of $\mathcal{B}$ is perfect, and $\mathcal{A}$ is given the same environment as a real attack.

Claim The q signature and message pairs (m_i, σ_i) sent to $\mathcal{A}$ are valid.

Proof of Claim. Let $(m_1, \sigma_1), \ldots, (m_q, \sigma_q)$ be the message and signature pairs that $\mathcal{A}$ received. Adversary $\mathcal{A}$ verifies these signatures using $vk = (g, g^{\alpha}, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}, h)$.

The pairs that $\mathcal{A}$ received are classified into two groups according to the tag of message $\hat{t} = \hat{m} \mod 2^{j^*}$. One group is $\hat{t} = \tilde{t}$ and the other is $\hat{t} \neq \tilde{t}$.

Regarding the group that has $\hat{t} = \tilde{t}$, $\hat{\sigma} = (\hat{\sigma}_0, \hat{\sigma}_1) = ((g^{\alpha})^{r(\hat{m})} (z(\hat{m})h)^{r}, g^{r})$. The signature $\hat{\sigma}$ is verified as follows:

$$
\begin{aligned}
e(\hat{\sigma}_0, g) &= e\left((g^{\alpha})^{r(\hat{m})} (z(\hat{m})h)^{r}, g \right) \\
&= e\left((g^{\alpha})^{r(\hat{m})}, g \right) e\left((z(\hat{m})h)^{r}, g \right) \\
&= e\left((g^{\alpha})^{r(\hat{m}) + \beta f(\hat{m})}, g \right) e\left((z(\hat{m})h)^{r}, g \right) \\
&= e\left(g^{r(\hat{m}) + \beta f(\hat{m})}, g \right)^{\alpha} e\left((z(\hat{m})h), g \right)^{r} \\
&= e\left(g^{r(\hat{m}) + \beta f(\hat{m})}, g^{\alpha} \right) e\left((z(\hat{m})h), g^{r} \right)
\end{aligned}
$$

$$= e\left(u(\hat{m}), g^{\alpha}\right)e(z(\hat{m})h, \hat{\sigma}_1)\,.$$

Regarding the group that has $\hat{t} \neq \tilde{t}$, $\hat{\sigma} = (\hat{\sigma}_0, \hat{\sigma}_1) = ((g^{\alpha})^{r(\hat{m})}(g^{\beta})^{r'(\tilde{t}-\check{t})}S^r, g^r)$. The signature $\hat{\sigma}$ is verified as follows:

$$\begin{aligned}
e(\hat{\sigma}_0, g) &= e\left((g^{\alpha})^{r(\hat{m})}(g^{\beta})^{r'(\tilde{t}-t^*)}S^r, g\right)\\
&= e\left((g^{\alpha})^{r(\hat{m})}(g^{\beta})^{(r+\frac{\alpha f(\hat{m})}{(\tilde{t}-t^*)})(\tilde{t}-t^*)}(g^r)^{\sum_{j=1}^{l} x_{z_j}^{t(j)}+x_h}, g\right)\\
&= e\left((g^{\alpha})^{r(\hat{m})+\beta f(\hat{m})}(g^r)^{\beta(\tilde{t}-t^*)+\sum_{j=1}^{l} x_{z_j}^{t(j)}+x_h}, g\right)\\
&= e\left((g^{\alpha})^{r(\hat{m})+\beta f(\hat{m})}, g\right) e\left((g^r)^{\beta(\tilde{t}-t^*)+\sum_{j=1}^{l} x_{z_j}^{t(j)}+x_h}, g\right)\\
&= e\left(g^{r(\hat{m})+\beta f(\hat{m})}, g\right)^{\alpha} e\left(g^{\beta(\tilde{t}-t^*)+\sum_{j=1}^{l} x_{z_j}^{t(j)}+x_h}, g\right)^{r}\\
&= e\left(g^{r(\hat{m})+\beta f(\hat{m})}, g^{\alpha}\right) e\left((g^{\beta})^{\tilde{t}+\sum_{j=1}^{l} x_{z_j}^{t(j)}}(g^{\beta})^{-t^*+x_h}, g^r\right)\\
&= e(u(\hat{m}), g^{\alpha})e(z(\hat{m})h, \hat{\sigma}_1).
\end{aligned}$$

Both groups satisfy the equation

$$e(\hat{\sigma}_0, g) = e\left(u(\hat{m}), g^{\alpha}\right)e(z(\hat{m})h, \hat{\sigma}_1)\,.$$

□

Analysis Let *success* be the event that $\mathcal{B}$ outputs a CDH solution $g^{\alpha\beta}$. In this simulation, $\mathcal{B}$ can extract $g^{\alpha\beta}$ from the forgery if $\tilde{t} = t^*$. This probability $\Pr[\tilde{t} = t^*]$ is

$$\Pr[\tilde{t} = t^*] = \frac{1}{|T^{(j^*)}|} = \frac{1}{\lfloor \frac{e\cdot q}{d+1} \rfloor + 1}.$$

However, if no tag $t_i^{(j^*)} \in T^{(j^*)}$ has at most d-fold collisions, $\mathcal{B}$ can not extract $g^{\alpha\beta}$ from the forgery since $f(m^*) \neq 0$. Moreover, there is a gap in tag distribution $1/2^{\mathcal{O}(\kappa)}$ between mod 2^j computation and uniform distribution, where $j \leq d \leq \mathcal{O}(\kappa)$. Hence,

$$\begin{aligned}
\Pr[\mathit{success}] &= \frac{1}{\lfloor \frac{e\cdot q}{d+1} \rfloor + 1}\varepsilon^{\text{EUF-XRMA}} - \Pr[d+1\text{-fold}] - \frac{1}{2^{\mathcal{O}(\kappa)}}\\
&= \mathcal{O}\left(\frac{d}{q}\right)\varepsilon^{\text{EUF-XRMA}}.
\end{aligned}$$

□

4 EUF-CMA Full Security Scheme

In this section, we discuss the construction of a fully EUF-CMA secure scheme from SIG_0 by applying trapdoor commitment TCOM.

4.1 Construction

We describe SIG in Fig. 4.

$\mathsf{KGen}(1^\kappa)$	$\mathsf{Sign}(sk, m)$	$\mathsf{Vrfy}(vk, m, \sigma, r)$
set $\mathbb{G}$ $s.t.$ $\lvert\mathbb{G}\rvert = p$	$r \leftarrow \mathsf{COIN}^{\mathsf{com}}$, $s \leftarrow \mathbb{Z}/p\mathbb{Z}$	$\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$
$\alpha \leftarrow \mathbb{Z}_p$	$\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$	For $i := 1$ to ℓ do
$(g, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}) \leftarrow \mathbb{G}$	$u(\psi) = \prod_{i=0}^{d} u_i^{\psi^i}$	$t^{(j)} = \psi \mod 2^j$
$sk = \alpha$	For $j := 1$ to ℓ do	If $e(\tilde{\sigma_0}, g)$
$vk = (g, h, g^\alpha, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l})$	$t^{(j)} = \psi \mod 2^j$	$\neq e(u(\psi), g^\alpha) e(z(\psi)h, \tilde{\sigma_1})$
$(tk, pk) \leftarrow \mathsf{Gen}^{\mathsf{tc}}(1^\kappa)$	$z(\psi) = \prod_{j=1}^{l} z_j^{t^{(j)}}$	return 0
return (vk, sk, tk, pk)	$\tilde{\sigma_0} = u(\psi)^\alpha (z(\psi)h)^s$	else
	$\tilde{\sigma_1} = g^s$	return 1
	return $(\sigma = (\tilde{\sigma_0}, \tilde{\sigma_1}), r)$	

Fig. 4. SIG: EUF-CMA-secure signature scheme with TCOM under the CDH assumption

Remark 1. One can construct TCOM such that ψ can be seen in an element in $\mathbb{Z}/p\mathbb{Z}$ (except for one element). In addition, $\psi \leftarrow \mathsf{Com}^{\mathsf{tc}}_{pk}(m)$ is (almost) uniformly distributed over $\mathbb{Z}/p\mathbb{Z}$ for any m. The latter condition is needed to transform an EUF-XRMA secure signature scheme to an EUF-CMA secure one. For example, let $\mathbb{G}$ be the group defined over the super-singular elliptic curve $y^2 = x^3 + b$ on $\mathbb{F}_p$, where $p = 2 \pmod 3$. Then, there is the one-to-one encoding, called map-to-point, from $\mathbb{G}^\times (= \mathbb{G} \backslash \{\mathcal{O}\})$ to $\mathbb{Z}/p\mathbb{Z}$ [3].

Lemma 3. *The signature scheme* SIG (Fig. 4) *is non-re-randomizable.*

Proof. Let $vk = (g, g^\alpha, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}, h)$ be a given vk, and let m and $(\sigma = (\tilde{\sigma_0}, \tilde{\sigma_1}),\ r)$ be valid messages for signatures, i.e., σ satisfies

$$e(\tilde{\sigma_0}, g) = e(u(\psi), g^\alpha) e(h \prod_{j=1}^{l} z_j^{t^{(j)}}, \tilde{\sigma_1}). \tag{1}$$

The set of all σs satisfying (1) is therefore identical to the set

$$\Sigma(vk, m) = \{(u(\psi))^\alpha (z(\psi)h)^s, g^s; s \in \mathbb{Z}_p, r \leftarrow \mathsf{COIN}^{\mathsf{com}}\}.$$

Consider an algorithm *Rerand* taking as input vk, σ, and message m. We assume that *Rerand* samples $s' \leftarrow \mathbb{Z}_p$ and returns $\sigma' = (\sigma'_0, \sigma'_1)$ distributed uniformly over $\Sigma(sk, m)$. However, since *Rerand* cannot generate $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(x; r)$; $r \leftarrow \mathsf{COIN}^{\mathsf{com}}$, there is no *Rerand* that returns the new signature σ' distributed uniformly over the set of all possible signatures for m. Hence, SIG is non-re-randomizable. $\square$

4.2 Security Analysis

Theorem 5. *Let* $\mathsf{TCOM} = (\mathsf{Gen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ *be a trapdoor commitment and* SIG_0 *be* EUF-XRMA *secure. Then,* SIG *is* EUF-CMA *secure. Moreover, let* $\varepsilon^{\text{EUF-CMA}}_{\mathsf{SIG}} = \mathsf{Adv}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ *be an advantage of an* EUF-CMA *adversary for* SIG*,* $\varepsilon^{\text{EUF-XRMA}}_{\mathsf{SIG}_0} = \mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0,\mathcal{B}}(\kappa)$ *be an advantage of an* EUF-XRMA *adversary for* SIG_0*, and* $\varepsilon^{\text{comp-bind}}$ *be an advantage of a computational binding adversary. Then,* $\varepsilon^{\text{EUF-CMA}}_{\mathsf{SIG}}$ *can be bounded by* $\varepsilon^{\text{EUF-XRMA}}_{\mathsf{SIG}_0} + \varepsilon^{\text{comp-bind}}$.

Proof Let $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ be the adversary against EUF-XRMA security of SIG_0 and $\mathcal{B}^{\text{comp-bind}}$ be the adversary against computational binding for TCOM and $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}}$ be the adversary against EUF-CMA security of SIG.

As we can regard commitments as input in SIG_0 instead of messages, the adversary $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ who can breaks EUF-XRMA security of SIG_0 can break EUF-XRMA with TCOM for SIG_0. According to Theorem 4, if the CDH assumption holds in $\mathbb{G}$, then SIG_0 is EUF-XRMA secure with TCOM. We write $\mathcal{B}^{\text{EUF-XRMA with }\mathsf{TCOM}}_{\mathsf{SIG}_0}$ as the adversary against EUF-XRMA security with TCOM of SIG_0.

Now we show that if the adversary $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}}$ who can break EUF-CMA security of SIG exists, then the adversaries $\mathcal{B}^{\text{EUF-XRMA with }\mathsf{TCOM}}_{\mathsf{SIG}_0}$ who can break EUF-XRMA security with TCOM for SIG_0 or $\mathcal{B}^{\text{comp-bind}}$ who can break computational binding for TCOM exist. Then we compare their advantages $\varepsilon^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ and $\varepsilon^{\text{comp-bind}}$ with $\varepsilon^{\text{EUF-CMA}}_{\mathsf{SIG}}$. We consider a EUF-XRMA with TCOM game and two cases; when queried commitments $\{\psi_1, \ldots, \psi_q\}$ contains challenge commitment ψ^*, $\mathcal{B}^{\text{EUF-XRMA with }\mathsf{TCOM}}_{\mathsf{SIG}_0}$ breaks EUF-XRMA security with TCOM (**Case 1**) and when $\psi_1, \ldots, \psi_q$ do not contain ψ^*, $\mathcal{B}^{\text{coomp-bind}}$ breaks computational binding (**Case 2**). Here, we write the verification key and signing key of SIG as (vk, sk) and those of SIG_0 as (vk_0, sk_0). From the view of the adversary $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}}$, it is statistically indistinguishable that view made by the adversary $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ and the adversary $\mathcal{B}^{\text{comp-bind}}$. According to **Case 1** and **Case 2**, the advantage of $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}}$ can be bounded by the sum of the advantages of $\mathcal{B}^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ and $\mathcal{B}^{\text{comp-bind}}$.

We construct the adversary $\mathcal{B}^{\text{EUF-XRMA with }\mathsf{TCOM}}$ with advantage of $\varepsilon^{\text{EUF-XRMA}}_{\mathsf{SIG}_0}$ or $\mathcal{B}^{\text{comp-bind}}$ with advantage of $\varepsilon^{\text{comp-bind}}$ by using the adversary $\mathcal{A}^{\text{EUF-CMA}}_{\mathsf{SIG}}$.

Setup We consider $\mathsf{TCom}^{\mathsf{tc}}_{tk}$ as MsgGen of EUF-XRMA, then commitments are generated with auxiliary information such that

$$(\psi_i, \overline{r}_i) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^k).$$

The adversary $\mathcal{B}^{\text{EUF-XRMA with }\mathsf{TCOM}}_{\mathsf{SIG}_0}$ receives the verification key vk_0, commitments ψ_i, signatures σ_i of SIG_0 for $1 \leq i \leq q$ and auxiliary information w_i,

$$w_i = (pk, tk, \overline{r}_i),$$

where pk is the public key, tk is the trapdoor key for TCOM, and commitment ψ_i satisfies that

$$\psi_i = \mathsf{Com}_{pk}(x_i; \overline{r}_i)$$

for $x_i \in \mathcal{M}$. $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCom}}$ sets

$$vk = (vk_0, pk)$$

and send vk to $\mathcal{A}_{\mathsf{SIG}}^{\text{EUF-CMA}}$.

Signing $\mathcal{A}_{\mathsf{SIG}}^{\text{EUF-CMA}}$ makes q signing queries. For $1 \leq i \leq q$, $\mathcal{A}_{\mathsf{SIG}}^{\text{EUF-CMA}}$ gives a message m_i to $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$. Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ computes

$$r_i = \mathsf{TCol}_{tk}^{\mathsf{tc}}(\psi_i, \overline{r}_i, m_i),$$

where r_i satisfies

$$\psi_i = \mathsf{Com}_{pk}^{\mathsf{tc}}(m_i; r_i).$$

Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ returns (σ_i, r_i) corresponding to m_i. Here, the signatures which $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ firstly received as input in this game are regarded as that of SIG since messages can be just replaced by commitments.

Forgery of $\mathcal{A}_{\mathsf{SIG}}^{\text{EUF-CMA}}$ $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ receive a forgery (m^*, σ^*, r^*) of SIG from $\mathcal{A}_{\mathsf{SIG}}^{\text{EUF-CMA}}$, where $m^* \notin \{m_i, \dots, m_q\}$. Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ computes commitment

$$\psi^* = \mathsf{Com}_{pk}^{\mathsf{tc}}(m^*; r^*).$$

Case 1: breaking EUF-XRMA security of SIG_0 In this case that $\psi^* \notin \{\psi_1, \dots, \psi_q\}$, $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ outputs (ψ^*, σ^*). This means the adversary succeeds in breaking EUF-XRMA with TCOM security of SIG_0. This goes against the fact that any adversary who breaks the EUF-XRMA security of SIG_0 does not exists in Theorem 4.

Case 2: breaking computational binding In the case that $\psi^* \in \{\psi_1, \dots, \psi_q\}$, $\mathcal{B}^{\text{comp-bind}}$ outputs (m^*, r^*, m_i, r_i) such that

$$(\psi^* = \psi_i) \cap (m^* \neq m_i)$$

for $1 \leq i \leq q$. This means $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ succeeds in breaking computational binding for trapdoor commitment as $\mathcal{B}^{\text{comp-bind}}$.

Analysis

Supposed that SIG is EUF-CMA secure. Then $\mathcal{B}_{\mathsf{SIG}_0}^{\text{EUF-XRMA with } \mathsf{TCOM}}$ breaks EUF-XRMA security when $\psi^* \notin \{\psi_1, \dots, \psi_q\}$ or $\mathcal{A}^{\text{comp-bind}}$ breaks computational binding for trapdoor commitments when $\psi^* \in \{\psi_1, \dots, \psi_q\}$. Therefore $\varepsilon_{\mathsf{SIG}}^{\text{EUF-CMA}}$ is bounded by sum of $\varepsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}}$ and $\varepsilon^{\text{comp-bind}}$. Hence,

$$\varepsilon_{\mathsf{SIG}}^{\text{EUF-CMA}} \leq \varepsilon^{\text{comp-bind}} + \varepsilon_{\mathsf{SIG}_0}^{\text{EUF-XRMA}}.$$

$\square$

5 Discussion

The reduction loss of Böhl et al.'s signature scheme is

$$\varepsilon^{\text{CDH}} \geq |\frac{1}{T^{(j^*)}}| \left(\varepsilon^{\text{EUF-CMA}} - \varepsilon^{\mathsf{PRF}} - Pr[d+1\text{-fold}]\right),$$

where $|T^{(j^*)}|$ is the size of tag sets. In our scheme, $T^{(j^*)} = \mathcal{O}(\frac{q}{d})$ since its tag space is $|T^{(j^*)}| := \lfloor (d+1)/e \cdot q \rfloor + 1$. The advantage regarding PRF $\varepsilon^{\mathsf{PRF}}$ is $\frac{1}{2^{\mathcal{O}(\kappa)}}$, which is the gap between the case in which tags are chosen uniformly and that in which tags are generated as $t^j = m \mod 2^j$. In Böhl et al.'s scheme, the key lemma is as follows:

$$\Pr[d+1\text{-}-\text{fold}] = \Pr[\exists i_1, \ldots, i_{d+1} \in [q] \mid t_{i_1} = \cdots = t_{i_{d+1}}] \leq \frac{q^{d+1}}{n^d}.$$

Since they assumed that the size of d is constant, the evaluation was sufficient. However, we assume $d = \mathcal{O}(\kappa)$; thus, we evaluate the probability more strictly. According to Theorem 4, 5,

$$\begin{aligned} \varepsilon^{\text{CDH}} &\geq |\frac{1}{T^{(j^*)}}| \left(\varepsilon^{\text{EUF-XRMA}} - \frac{1}{2^{\mathcal{O}(\kappa)}} - Pr[d+1\text{-fold}]\right) \qquad (2)\\ &\geq \mathcal{O}\left(\frac{d}{q}\right) \cdot \varepsilon^{\text{EUF-XRMA}} \\ &\geq \mathcal{O}\left(\frac{d}{q}\right) \cdot \left(\varepsilon^{\text{EUF-CMA}} - \varepsilon^{\text{comp-binding}}\right) \end{aligned}$$

Hence,

$$\varepsilon^{\text{EUF-CMA}} \leq \mathcal{O}\left(\frac{q}{d}\right) \cdot \varepsilon^{\text{CDH}} + \varepsilon^{\text{comp-binding}}. \qquad (3)$$

Computational binding is reduced to the discrete logarithm problem. The whole security-reduction loss to the CDH problem, a search problem, is $\mathcal{O}(q/d)$.

The tag set of Böhl et al.'s scheme is chosen from a sparse tag set whose size is $2^{\lfloor c^j \rfloor}$, where c is constant. Our tag set size is 2^j, which is appropriate to choose a small T^{j^*} such that $|T^{j^*}| > \frac{e \cdot q}{d+1}$. On the other hand, d is constant in Böhl et al.'s scheme, while $d = \mathcal{O}(\kappa)$ in our scheme. The size of the vk increases according to the size of d. Hence, the vk size of our scheme is larger than that of Böhl et al.'s scheme. That is, although the vk size is larger than that of Böhl et al.'s scheme, our scheme achieves a constant-size signature with a tighter reduction.

6 Conclusion

The optimal security-reduction loss to the CDH problem from a constant-size signature scheme is $\mathcal{O}(q)$ if signature schemes are re-randomizable. We proposed a constant-size non-re-randomizable signature scheme that is secure under the CDH assumption with tighter security-reduction than ever constant-size signature schemes. Particularly, its security reduction, $\mathcal{O}(q/d)$ is the tightest thus far.

References

1. Abe, M., Chase, M., David, B., Kohlweiss, M., Nishimaki, R., and Ohkubo, M. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. Journal of Cryptology, 29(4), 833-878. 2016.
2. Boneh, D., Boyen, X. Efficient selective-ID secure identity-based encryption without random oracles. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 223-238). Springer, Berlin, Heidelberg. 2004.
3. Boneh, D., and Franklin, M. Identity-based encryption from the Weil pairing. In Annual International Cryptology Conference (pp. 213-229). Springer Berlin Heidelberg. 2001.
4. Boyen, X. Lattice Mixing and Vanishing Trapdoors: A Framework for Fully Secure Short Signatures and More. In Public Key Cryptography (Vol. 6056, pp. 499-517). 2010
5. Boyle, E., Goldwasser, S., and Ivan, I. Functional signatures and pseudorandom functions. In International Workshop on Public Key Cryptography (pp. 501-519). Springer Berlin Heidelberg. 2014.
6. Böhl, F., Hofheinz, D., Jager, T., Koch, J., Seo, J. H., and Striecks, C. Practical signatures from standard assumptions. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 461-485). Springer Berlin Heidelberg. 2013.
7. Böhl, F., Hofheinz, D., Jager, T., Koch, J., and Striecks, C. Confined guessing: New signatures from standard assumptions. Journal of Cryptology, 28(1), 176-208. 2015.
8. Blazy, O., Kakvi, S. A., Kiltz, E., and Pan, J. Tightly-Secure Signatures from Chameleon Hash Functions. In Public Key Cryptography (pp. 256-279). 2015.
9. Boneh, D., Mironov, I., and Shoup, V. A secure signature scheme from bilinear maps. In CT-RSA (Vol. 2612, pp. 98-110). 2003.
10. Chevallier-Mames, B. An efficient CDH-based signature scheme with a tight security reduction. In Annual International Cryptology Conference (pp. 511-526). Springer Berlin Heidelberg. 2005.
11. Chevallier-Mames, B., Joye, M. A practical and tightly secure signature scheme without hash function. In CT-RSA (Vol. 4377, pp. 339-356). 2007.
12. Chen, J., and Wee, H. Fully,(almost) tightly secure IBE and dual system groups. In Advances in Cryptology CRYPTO 2013 (pp. 435-460). Springer Berlin Heidelberg. 2013.
13. Damgrd, I. Efficient concurrent zero-knowledge in the auxiliary string model. In Advances in Cryptology—EUROCRYPT 2000 (pp. 418-430). Springer Berlin/Heidelberg. 2000.
14. Ducas, L., and Micciancio, D. Improved short lattice signatures in the standard model. In International Cryptology Conference (pp. 335-352). Springer, Berlin, Heidelberg. 2014.
15. Goldreich, O. Foundation of cryptography (in two volumes: Basic tools and basic applications). 2001.
16. Goh, E. J., Jarecki, S. A signature scheme as secure as the Diffie-Hellman problem. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 401-415). Springer, Berlin, Heidelberg. 2003.
17. Goldwasser, S., Micali, S., and Rivest, R. L. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 17(2), 281-308. 1988.

18. Hofheinz, D. Algebraic Partitioning: Fully Compact and (almost) Tightly Secure Cryptography. In TCC (A1) (pp. 251-281). 2016.
19. Hofheinz, D., Jager, T. Tightly Secure Signatures and Public-Key Encryption. In Crypto (Vol. 7417, pp. 590-607). 2012.
20. Hofheinz, D., Jager, T., and Knapp, E. Waters signatures with optimal security reduction. In International Workshop on Public Key Cryptography (pp. 66-83). Springer Berlin Heidelberg. 2012.
21. Hofheinz, D., and Kiltz, E. Programmable hash functions and their applications. Journal of Cryptology, 25(3), 484-527. 2012.
22. Hohenberger, S. and Waters, B. Realizing hash-and-sign signatures under standard assumptions. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 333-350). Springer Berlin Heidelberg. 2009.
23. Kajita, k., Ogawa, K., and Fujisaki, E. A Constant-Size Signature Scheme with Tighter Reduction from CDH Assumption. In International Conference on Information Security (pp. 137-154). Springer international Publishing. 2017
24. Katz, J., Wang, N. Efficiency improvements for signature schemes with tight security reductions. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 155-164). 2003.
25. Schge, S. Tight Proofs for Signature Schemes without Random Oracles. In Eurocrypt (Vol. 6632, pp. 189-206). ISO 690. 2011.
26. Seo, J. H. Short Signatures from Diffie-Hellman, Revisited: Sublinear Public Key, CMA Security, and Tighter Reduction. IACR Cryptology ePrint Archive, 2014, 138. 2014.
27. Waters, B. Efficient identity-based encryption without random oracles. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 114-127). Springer Berlin Heidelberg. ISO 690. 2005

Appendix

EUF-dnaCMA A SIG is said to be existentially unforgeable against distinct-message non-adaptively chosen-message attack (EUF-dnaCMA) [6, 7], if for any $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-dnaCMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{EUF-dnaCMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$. $\mathsf{Expt}^{\text{EUF-dnaCMA}}_{\mathsf{SIG},\mathcal{A}}$ (κ) is the experiment with EUF-dnaCMA and refer to [7].

EUF-dnaCMA$^*_{\mathbf{d}}$ A tag-based signature scheme SIG_t is said be EUF-dnaCMA with d-fold tag-collisions (EUF-dnaCMA$^*_{\mathrm{d}}$) [6, 7], if for any $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-dnaCMA}^*_{\mathrm{d}}}_{\mathsf{SIG}_t,\mathcal{A}}(\kappa)$ $:= \Pr[\mathsf{Expt}^{\text{EUF-dnaCMA}^*_{\mathrm{d}}}_{\mathsf{SIG}_t,\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$, where $\mathsf{Expt}^{\text{EUF-dnaCMA}^*_{\mathrm{d}}}_{\mathsf{SIG}_t,\mathcal{A}}(\kappa)$ is the experiment with EUF-dnaCMA$^*_{\mathrm{d}}$ and refer to [7]. Note that we call d a tag-collision parameter; it affects key and signature sizes, and the security reduction. The d-fold tag-collisions means that the same tag t_i is chosen for d different signed messages.