PAPER Special Section on Cryptography and Information Security

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

Kaisei KAJITA[†a)], *Nonmember*, Kazuto OGAWA[†], *and* Eiichiro FUJISAKI[††], *Members*

SUMMARY We present a constant-size signature scheme under the CDH assumption. It has a tighter security reduction than any other constant-size signature scheme with a security reduction to solving some intractable search problems. Hofheinz, Jager, and Knapp (PKC 2012) presented a constant-size signature scheme under the CDH assumption with a reduction loss of $O(q)$, where q is the number of signing queries. They also proved that the reduction loss of $O(q)$ is optimal in a black-box security proof. To the best of our knowledge, no constant-size signature scheme has been proposed with a tighter reduction (to the hardness of a search problem) than that proposed by Hofheinz et al., even if it is not re-randomizable. We remark that our scheme is not re-randomizable. We achieve the reduction loss of $O(q/d)$, where d is the number of group elements in a public key.

key words: *digital signature, CDH assumption, trapdoor commitment, tight security reduction*

1. Introduction

1.1 Background

Digital signatures are one of the most elemental cryptographic primitives that guarantee authenticity of electronic documents. When using a digital signature scheme, 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. They are used in transport layer security (TLS), e-commerce, and Cryptocurrency among others.

The performance of cryptographic primitives can be evaluated by *reduction loss* to a certain difficult problem. The security reduction is a particular way of a mathematical proof to ensure that a cryptographic primitive is secure. It shows that breaking the primitive is at least as difficult as solving the difficult problem. Reduction loss is the gap in difficulty between breaking the primitive and solving the difficult problem. When there is approximately no security-reduction loss, it is called *tightly secure*. More strictly speaking, if a t-time adversary attacks the scheme with success probability ε, then a t'-time algorithm can be constructed to solve some difficult problem with success probability ε'. A cryptographic scheme is tightly secure if $\varepsilon' \approx \varepsilon/\theta$ and $t' \approx t$. The constant θ measures the security loss of the reduction of the primitives from the underlying assumption and does not depend on other parameters under the adversary's control (e.g., the number of queries, the scheme's security parameter, and the adversary's own success probability). In this paper, we focus on the security-reduction of signature schemes. It is important to reduce the reduction loss of a cryptosystem, which enables the choosing of as small a security parameter as needed without compromising security as much as possible; hence, enabling small security parameters for cryptosystems, i.e., signatures and verification keys, and fast computations of signature generation and verification, etc.

1.2 Related Work

There are many provably secure digital signature schemes [3], [4], [6], [8], [10], [14], [19], [22], [27]. The security of signature schemes was first discussed in the random oracle model. Those signature schemes have heuristic security arguments [16]. Then digital signatures in the standard model were developed [3]. Those schemes use two major problems for security proofs; decisional problems, e.g., the decisional Diffie-Hellman (DDH) problem, and search problem, e.g., the Computational Diffie-Hellman (CDH) problem. Generically, search problems are more difficult than decisional problems, namely, solving the CDH problem is more difficult than solving the DDH problem. 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 on. The digital signatures that can be reduced to decisional problems have been extensively studied, and their reduction loss $O(l)$ to the DDH problem has been achieved, where l is the bit length of a message [12], [18]. On the other hand, there are a few digital signatures secure under the difficulty of CDH problems. We show them in Table 1. Waters proposed a signature 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 the Waters signature scheme have been developed [6], [7], [20], [22], [26]. However, their reduction loss to the CDH problem is not so tight. The reductions loss of the Wa-

Manuscript received March 18, 2019.
Manuscript revised June 18, 2019.

[†] The authors are with the Science and Technology Research Laboratories, Japan Broadcasting Corporation, Tokyo, 157-8310 Japan.

[††] The author is with the School of Information Science, Japan Advanced Institute of Science and Technology (JAIST), Nomi-shi, 923-1292 Japan.

[*] This paper is the revised version of the paper that appeared in the 20th Information Security Conference (ISC2017), Ho Chi Minh, Vietnam, Nov. 2017 [23]. This revised one has fixed many mistakes in the previous one.

a) E-mail: kajita.k-bu@nhk.or.jp

DOI: 10.1587/transfun.2019CIP0015

Table 1 Constant-size signature schemes under the CDH assumption in the standard model: κ is the security parameter, $\tau_{\mathbb{G}}$ is the size of the 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 satisfying $c > 1$, and ε is the success probability of the adversary. $\omega(1)$ means any strictly increasing function in κ; e.g., $\log\log\kappa$.

Scheme	Verification key size	Signature size	Reduction loss
Wat05 [27]	$O(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$O(\kappa q)$
HK08 [21]	$O(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$O(\sqrt{\kappa}q)$
HJK12 [20]	$O(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}}$	$O(q)$
BHJ+13 [6], BHJ+15 [7]	$O(\log_c \kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$O\left(\frac{2^{2+\frac{c}{d}} q^{\frac{c}{d}+c}}{\varepsilon^{\frac{c}{d}}}\right)$
Seo14 [26]	$\omega(1)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$O(\kappa q)$
Ours	$O(\kappa)\tau_{\mathbb{G}}$	$2\tau_{\mathbb{G}} + \tau_{\mathbb{F}_p}$	$O(\frac{q}{d})$

ters signature scheme is $O(8(l+1)q)$, 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 $O(\sqrt{l}q)$. As far as we know, the tightest security reduction to the CDH problem from known constant-size signature schemes is $O(q)$, presented by Hofheinz et al. [20]. They proposed a re-randomizable signature scheme (shown in Sect. 2.1) by applying an error-correcting code to the Waters signature scheme. They also proved that the reduction loss of $O(q)$ is optimal if signature schemes are re-randomizable.

Böhl et al. presented a new paradigm for the construction of signature schemes in standard computational assumptions [6], [7]. They present an efficient mildly secure scheme based on the CDH assumption in pairing-friendly groups. Moreover, they apply trapdoor commitment and some modification and achieve EUF-CMA security of the signature scheme if the CDH assumption holds. In their construction, pseudorandom functions, which affect the security-reduction loss, are used to achieve security against a non-adaptive attack. Their security proof uses a "confined guessing" technique, which is a new proof technique by using tags. After that, Seo proposed the signature scheme [26] with a short verification key and the same security reduction as the Waters signatures by improving Böhl et al.'s signature scheme.

In spite of many of these splendid previous studies, constant-size signatures with a tight reduction to the CDH problem in the standard model remain undeveloped. If conditions are relaxed, there are some signature schemes with a tight reduction. For example, the tree-based signature scheme [8] achieves a tight reduction to search problems but its signature size is not constant. Besides, there exists a non constant-size signature scheme with a tight reduction from the strong RSA assumption [11]. Unless a signature scheme is in the standard model, there exists a constant-size signature scheme with a tight reduction in the random oracle model [24]. So it is open to give a constant-size signature scheme under the difficulty of a search problem with a tight reduction.

1.3 Our Contributions

In general, the fully secure EUF-CMA signature scheme is constructed from some mildly secure schemes. Böhl et al. construct the EUF-CMA secure scheme from the schemes that are secure in mild security models by using generic transformation. In this paper, in order to achieve the EUF-CMA security, we use an existential unforgeability against the extended random message attack (EUF-XRMA security) presented by Abe et al. [1] as mild security. The exact definition of the EUF-XRMA security will be described in Sect. 2.2. Intuitively, in the EUF-XRMA security, messages are generated uniformly by a message generator with auxiliary information. Our signature scheme is constructed as follows: first, we construct an EUF-XRMA secure signature scheme, and then, we convert it to an EUF-CMA signature scheme by using a method given in [1]. Interestingly, the underlying signature scheme in [1] is slightly more secure than EUF-XRMA. Indeed, it is secure even if messages are not randomly chosen. In our scheme, however, the underlying scheme is just EUF-XRMA secure–it is not secure unless messages are randomly chosen. To the best of our knowledge, our proposal is the first scheme that essentially needs the conversion of [1] from EUF-XRMA security to EUF-CMA security.

We present a signature scheme with a tighter security reduction than known constant-size (i.e., the signature contains a constant number of group elements) signature schemes under the CDH assumption. We modify the Böhl et al.'s signature scheme and reduce its security to the CDH assumption more efficiently. Their scheme has compact public keys at the price of a loose security-reduction loss. We find out that there is a trade-off between public key size and a security-reduction loss in their scheme. Moreover, by removing a pseudorandom generator and using a generic transformation from the scheme with extended random-message-attack security to that with chosen-message-attack security shown in [1], we can obtain a signature scheme with the reduction loss of $O(q/d)$, where d is the number of group elements in a verification key.

2. Preliminaries

For $n \in \mathbb{N}$, $[n]$ denotes the set $\{1, \ldots, n\}$. $a \overset{\$}{\leftarrow} A$ denotes sampling a uniformly and randomly from a finite set A. $\mathsf{negl}(\kappa)$ denotes 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 $\mathsf{Dist}(X_\kappa, Y_\kappa) \triangleq \frac{1}{2}\sum_{s\in\{0,1\}^\kappa} |\Pr[X_\kappa = s] - \Pr[Y_\kappa = s]|$. We write $X \equiv Y$ if $\mathsf{Dist}(X_\kappa, Y_\kappa) = 0$.

2.1 Digital Signatures

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) $\kappa \in \mathbb{N}$, KGen, the key-generation algorithm, takes as input security parameter 1^κ and outputs a pair of verification and signing keys, (vk, sk). Here let $\mathcal{M}_\kappa$ be message space. The signing algorithm Sign takes as input (vk, sk) and a message $m \in \mathcal{M}_\kappa$ and produces a signature σ. The verification algorithm Vrfy takes as input vk, m, and σ, and outputs a verification result bit. For correctness, it is required that for any (vk, sk) pair generated with $\mathsf{KGen}(1^\kappa)$ and for any $m \in \mathcal{M}_\kappa$, it holds $\mathsf{Vrfy}(vk, m, \sigma) = 1$, where $\sigma = \mathsf{Sign}(sk, m)$.

Re-Randomizable Signatures: Intuitively, re-randomizable signatures [20] have a property that, given vk, m, and valid σ, one can efficiently generate a new signature σ' that is distributed properly over the set of all possible signatures on 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 of $\mathsf{Rerand}(vk, m, \sigma)$ is distributed over $\Sigma(vk, m)$ identically to that of $\mathsf{Sign}(sk, m)$.

2.2 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 PTT $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$, where $\mathsf{Expt}^{\text{EUF-CMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ is defined in Fig. 1.

EUF-XRMA: Let MsgGen is a PPT algorithm, called the message generator, which takes as input security parameter 1^κ and outputs $m \in \mathcal{M}_\kappa$ and auxiliary information w. A digital signature scheme SIG is said to be existentially unforgeable against extended random-message attack (EUF-XRMA) [1] with respect to MsgGen, if for any PPT $\mathcal{A}$, $\mathsf{Adv}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) := \Pr[\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa) = 1] = \mathsf{negl}(\kappa)$, where $\mathsf{Expt}^{\text{EUF-XRMA}}_{\mathsf{SIG},\mathcal{A}}(\kappa)$ is defined in Fig. 2.

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

Fig. 1 The EUF-CMA experiment. $\mathsf{Sign}_{sk}(\cdot)$ is a signing oracle with respect to sk. It takes as input m and returns $\sigma \leftarrow \mathsf{Sign}_{sk}(m)$, and then, records m to Q_m which is initially an empty list.

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

Fig. 2 The EUF-XRMA experiment. $Q_m = \{m_1, \ldots, m_q\}$.

2.3 Cryptographic Tools

Trapdoor Commitments: We define a trapdoor commitment scheme, following [13]. Let $\mathsf{TCOM} = (\mathsf{KGen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ be a tuple of the four algorithms. $\mathsf{KGen}^{\mathsf{tc}}$ is a PPT algorithm that takes as input security parameter 1^κ and outputs a pair of public and trapdoor keys $(pk, tk) \leftarrow \mathsf{KGen}^{\mathsf{tc}}(1^\kappa)$. $\mathsf{Com}^{\mathsf{tc}}$ is a PPT algorithm that takes as input pk and m, selects a random $r \leftarrow \mathsf{COIN}^{\mathsf{com}}$, where $r \in \mathbb{Z}/p\mathbb{Z}$, and outputs a commitment $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$. $\mathsf{TCom}^{\mathsf{tc}}$ is a PPT algorithm that takes as input 1^κ and tk, and outputs $(\psi, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^\kappa)$, where χ is auxiliary information. $\mathsf{TCol}^{\mathsf{tc}}$ is a deterministic polynomial-time algorithm that takes as input tk, ψ, χ and $\hat{m}$, and outputs $\hat{r} \in \mathbb{Z}/p\mathbb{Z}$ such that $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(\hat{m}; \hat{r})$.

We say that TCOM is a trapdoor commitment scheme if the following conditions holds, perfect hiding, computational binding, and trapdoor property.

Perfect Hiding. For any pk generated with $\mathsf{KGen}^{\mathsf{tc}}(1^\kappa)$, and any $m, m' \in \mathcal{M}_\kappa$, the following random variables are identical.

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

Computational Binding. For any PPT $\mathcal{A}$,

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

Trapdoor Property. For any pk generated with $\mathsf{KGen}^{\mathsf{tc}}(1^\kappa)$,

$$\left\{(\psi, m, r) \mid \psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r);\ r \leftarrow \mathsf{COIN}^{\mathsf{com}}\right\}$$
$$\equiv \left\{(\psi, m, r) \mid (\psi, \chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^\kappa);\ r = \mathsf{TCol}^{\mathsf{tc}}_{tk}(\psi, \chi, m)\right\}.$$

Bilinear Groups: Let $\mathcal{G}$ be a bilinear group generator [9] that, on input of a security parameter κ, outputs a description of bilinear groups $(\mathbb{G}, \mathbb{G}_T, e, p, g)$ such that $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of prime order p, 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 $a, b \in \mathbb{Z}/p\mathbb{Z}$, $e(g^a, h^b) = e(g, h)^{ab}$,

- (Non-degenerate:) $e(g,g)$ has order p in $\mathbb{G}_T$, and
- (Efficiently computable:) $e(\cdot,\cdot)$ is efficiently computable.

Computational Diffie-Hellman Assumption: Let $\mathcal{G}$ be a bilinear group generator, that on input of a security parameter κ, outputs a cyclic group. We say that the CDH assumption holds if for any polynomial-time algorithm $\mathcal{A}$ the following advantage is negligible function in κ:

$$\varepsilon^{\mathsf{cdh}} := \Pr\left[\begin{array}{l}(\mathbb{G},\mathbb{G}_T,e,p,g) \leftarrow \mathcal{G}(\kappa)\,;\,(\alpha,\beta) \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z} \;: \\ \mathcal{A}(\mathbb{G},p,g,g^{\alpha},g^{\beta}) = g^{\alpha\beta}\end{array}\right]$$
$$= \mathsf{negl}(\kappa).$$

3. Mildly Secure Signature Scheme and Message Generator

We propose a signature scheme SIG_0 and a message generator MsgGen. We later prove that SIG_0 is EUF-XRMA secure with respect to MsgGen under the CDH assumption. SIG_0 is similar to the non-adaptively secure signature scheme built in the optimized CDH-based signature scheme in [7]. The main differences from theirs are that $d = O(\kappa)$ instead of constant, and that tags, $t^{(1)},\ldots,t^{(l)}$ are made in a different manner.

We describe SIG_0 in Fig. 3. Its correctness is described in Appendix A. We let $l = \omega(\log_2 \kappa)$ and $d = O(\kappa)$. Let us define $T_j = \{0,1\}^j$ for $1 \le j \le l$. For $a, b \in \mathbb{Z}/p\mathbb{Z}$, we define

$$t^{(j)} = ((am+b) \bmod p) \bmod 2^j \qquad (1)$$

for $1 \le j \le l$, where $m \in \mathbb{Z}/p\mathbb{Z}$ is a message to be signed. We note that to sign a single message m, SIG_0 generates l tags, $t^{(1)},\ldots,t^{(l)}$, from m.

We now define MsgGen used in the later theorems.

Let $p = 2 \pmod 3$ and $E : y^2 = x^3 + 1$. We know that $E/\mathbb{F}_p$ is a super-singular elliptic curve defined over $\mathbb{F}_p$ of order $\#E/\mathbb{F}_p = p + 1$. Now we additionally assume that $p = \ell q' - 1$ where $q'(> 3)$ is a prime. We can assume that $\ell = 6$. Define $\mathbb{G}'$ as a cyclic sub-group in $E/\mathbb{F}_p$ of order q. Since $\mathbb{G}'$ is cyclic of prime order q', it is easy to construct a trapdoor commitment scheme TCOM on $\mathbb{G}'$. Let $\psi = (x,y) \in \mathbb{F}_p \times \mathbb{F}_p$ be an affine encoding of an element in $\mathbb{G}'$. Then, the map $\rho : \mathbb{G}' \hookrightarrow \mathbb{F}_p$, defined by $\rho(\psi) = y$, is injective. We now define $(m,w) \leftarrow \mathsf{MsgGen}$ as the algorithm that runs $(\psi,\chi) \leftarrow \mathsf{TCom}^{\mathsf{tc}}_{tk}(1^{\kappa})$ and outputs $(m,w) := (\rho(\psi),\chi)$. We note that it is not clear that elements of $\rho(\psi)$ is uniformly distributed in $[0,p-1]$. To prove Theorem 2, tags $t^{(j)}$ should be distributed uniformly in T_j. Therefore, we use the universal hashing technique to distribute $t^{(j)} = H(\rho(\psi)) \bmod 2^j$ almost uniformly in T_j, which is the reason why we add $a, b \in \mathbb{Z}/p\mathbb{Z}$ into vk. We remark that although we explicitly provide a candidate of $\mathbb{G}'$, one can use any cyclic group $\mathbb{G}'$ if (1) the DL problem on $\mathbb{G}'$ is believed to be hard, and (2) there is an efficiently computable injective map from $\mathbb{G}'$ to $\mathbb{Z}/p\mathbb{Z}$ such that $\log(p) - \log(\#\mathbb{G}') = \text{const}$, where p denotes the order of the bilinear group $\mathbb{G}$ in the proposed signature scheme.

We provide a useful lemma.

Lemma 1: Let T be a finite set. Let $q = O(poly(\kappa))$ and $d = O(\kappa)$. If $\#T > \frac{e\cdot q}{d+1}$,

$$\Pr[(d+1)\text{-fold}^{\mathsf{ideal}}] := \Pr[\exists i_1,\ldots,i_{d+1} \in [q] \text{ s.t } t_{i_1} = \cdots = t_{i_{d+1}}]$$

is exponentially small in κ, where $t_1,\ldots,t_q$ are independently and uniformly chosen from T and e denotes the base of the natural logarithm.

Proof. Let $n = \#T$.

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

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

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

Now, we set $n > \frac{eq}{d+1}$ then $\frac{e\cdot q}{n(d+1)} < 1$, and $\frac{e\cdot q}{\sqrt{2\pi(d+1)}\cdot(d+1)}$ is polynomial in κ. Hence, $\Pr[\exists i_1,\ldots,i_{d+1} \in [q] \text{ s.t } t_{i_1} = \cdots = t_{i_{d+1}}]$ is exponentially small in κ. □

The lemma above with constant d is known as a generalized birthday bound lemma, which often appears in the literature, including [6], [26]. In our case, d is not constant, which leads to somehow different consequence from [6], [26]. For constant d, the probability $\Pr[(d+1)\text{-fold}] = O(\frac{q^{d+1}}{n^d})$, because $(d+1)!$ is still constant. For $d = O(\kappa)$, however, $(d+1)!$ cannot be ignored. By using Stirling's approximation with suitable parameter selection, we have the result mentioned above.

3.1 EUF-XRMA Security

Theorem 2: Let MsgGen be a message generator mentioned above. Then SIG_0 is EUF-XRMA secure with respect to MsgGen under the CDH assumption on $\mathbb{G}$. Here, the reduction loss is $O(\frac{q}{d})$, where q is the number of queries of the adversary.

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

```
KGen($1^\kappa$)
    $(\mathbb{G}, \mathbb{G}_T, e, p, g) \leftarrow \mathcal{G}(\kappa)$
    $a, b, \alpha \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z}\ (H(x) := (ax + b) \bmod p)$
    $(g, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}) \overset{\$}{\leftarrow} \mathbb{G}$
    $vk = (H, g, g^\alpha, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l})$
    $sk = (\alpha, vk)$
    return $(vk, sk)$
```

```
Sign($sk, m$)
    $r \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z}$
    $u(m) = \prod_{i=0}^{d} u_i^{m^i}$
    For $j := 1$ to $l$ do
    $t^{(j)} = H(m) \bmod 2^j$
    $z(m) = \prod_{j=1}^{l} z_j^{t^{(j)}}$
    $\sigma_0 = u(m)^\alpha (z(m)h)^r$
    $\sigma_1 = g^r$
    return $\sigma = (\sigma_0, \sigma_1)$
```

```
Vrfy($vk, m, \sigma$)
    For $j := 1$ to $l$ do
    $t^{(j)} = H(m) \bmod 2^j$
    If $e(\sigma_0, g)$
      $\neq e(u(m), g^\alpha) e(z(m)h, \sigma_1)$
    return 0
      else
    return 1
```

Fig. 3 SIG$_0$: the EUF-XRMA secure signature scheme under the CDH assumption.

Setup.

$\mathcal{B}$ receives a CDH challenge $(g, g^\alpha, g^\beta) \in \mathbb{G}^3$. $\mathcal{B}$ then runs MsgGen to receive $\{(m_i, w_i)\}_{i=1}^{q}$. Let us define $\mathcal{M} := \{m_i\}_{i=1}^{q}$ and $T_j := \{0, 1\}^j$ for $j \in [l]$. $\mathcal{B}$ picks up randomly $a, b \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z}$ and define $H : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ as $H(m) = (am + b) \bmod p$. $\mathcal{B}$ sets j^* to be the smallest j^* such that $j^* > \lfloor \log_2(\frac{e \cdot q}{d+1}) \rfloor + 1$. We note that $\#T_{j^*}$ is polynomial in κ. Since $\#T_{j^*} > \lfloor (e \cdot q/(d + 1) \rfloor + 1$, The probability that event $(d + 1)$-fold happens is exponentially small if q tags are independently and uniformly chosen from T_{j^*}, due to Lemma 1.

$\mathcal{B}$ randomly chooses $\tilde{t} \overset{\$}{\leftarrow} T_{j^*}$. To jump into the conclusion, $\mathcal{B}$ can solve the CDH problem when $\mathcal{A}$ outputs forged pair (m^*, σ^*) such that $\tilde{t} = H(m^*) \bmod 2^{j^*}$. Let

$$\mathcal{M}' := \{m \in \mathcal{M} \,|\, \tilde{t} = H(m) \mod 2^{j^*}\}.$$

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

Let $d' = \#\mathcal{M}'$. By definition, $d' \leq d$. $\mathcal{B}$ makes a polynomial $f(X)$ of degree d' such that $f(m) = 0$ for all $m \in \mathcal{M}'$. If $d' = 0$, define $f(X) \equiv 1$. By polynomial expansion, we have

$$f(X) = \sum_{k=0}^{d'} \mu_k X^k$$

for some coefficients, $\mu_0, \ldots, \mu_{d'} \in \mathbb{Z}/p\mathbb{Z}$.

$\mathcal{B}$ then chooses randomly and independently $r_0, \ldots, r_d$, $x_1, \ldots, x_l, x_h \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z}$. $\mathcal{B}$ sets h as

$$h = (g^\beta)^{-\tilde{t}} g^{x_h}.$$

For $0 \leq k \leq d$, $\mathcal{B}$ sets u_k as

$$u_k = (g^\beta)^{\mu_k} g^{r_k},$$

where $\mu_k = 0$ for $d' < k$. $\mathcal{B}$ sets $z_1, \ldots, z_l$ as

$$z_j = g^{x_j} \text{ for } 1 \leq j \leq l,\ j \neq j^*,$$
$$z_{j^*} = g^\beta g^{x_{j^*}}$$

$\mathcal{B}$ finally chooses $a, b \overset{\$}{\leftarrow} \mathbb{Z}/p\mathbb{Z}$ and sets up $vk = (a, b, g, g^\alpha, h, \{u_k\}_{k=0}^{d}, \{z_j\}_{j=1}^{l})$. For the sake of convenience, we define $r(X)$, $\gamma(X)$ as follows;

$$r(X) := \sum_{k=0}^{d} r_k X^k,$$

$$\gamma(X) := x_h + \sum_{j=1}^{l} x_i t^{(j)}.$$

Let $t := H(X) \bmod 2^{j^*}$. Then, we have

$$u(X) = \prod_{k=0}^{d} u_k^X = (g^\beta)^{f(X)} g^{r(X)}, \tag{2}$$

$$z(X)h = (g^\beta)^{t-\tilde{t}} g^{\gamma(X)}. \tag{3}$$

Hence, the signature on message m holds, for $r \in \mathbb{Z}/p\mathbb{Z}$,

$$\sigma_0 = \left((g^\beta)^{f(m)} g^{r(m)}\right)^\alpha \left((g^\beta)^{t-\tilde{t}} g^{\gamma(m)}\right)^r, \tag{4}$$

$$\sigma_1 = g^r. \tag{5}$$

Here, note that $f(X), r(X), \gamma(X)$ are all known polynomials for $\mathcal{B}$ and kept for the signature simulation.

Signature simulation.

$\mathcal{B}$ creates q signatures $\sigma_1, \ldots, \sigma_q$ for q messages in $\mathcal{M}$.

Let $m \in \mathcal{M}$ be a message to be signed. Set $t := H(m) \bmod 2^{j^*}$. Note that t is the tag for message m in T_{j^*}.
Case 1 ($t = \tilde{t}$): By definition, $f(m) = 0$. Therefore, by Eq. (4), it holds that

$$\sigma_0 = (g^\alpha)^{r(m)} (z(m)h)^r,$$
$$\sigma_1 = g^r.$$

Therefore, it is obvious that $\mathcal{B}$ computes (σ_0, σ_1) on m.
Case 2 ($t \neq \tilde{t}$): Then, it holds that $f(m) \neq 0$. Let $r = \frac{-\alpha f(m)}{t-\tilde{t}}$ (mod p). By simple calculation and the equations, (4) and (5), it holds that

$$\begin{aligned}
\sigma_0 &= \left((g^\beta)^{f(m)} g^{r(m)}\right)^\alpha \left((g^\beta)^{t-\tilde{t}} g^{\gamma(m)}\right)^r \\
&= (g^{\alpha\beta})^{f(m)} (g^\alpha)^{r(m)} \left((g^\beta)^{t-\tilde{t}} g^{\gamma(m)}\right)^r \\
&= (g^{\alpha\beta})^{f(m)} (g^\beta)^{(t-\tilde{t}) \cdot \frac{-\alpha f(m)}{t-\tilde{t}}} (g^\alpha)^{r(m)} g^{\gamma(m) r} \\
&= (g^\alpha)^{r(m)} g^{\gamma(m) r} \\
&= (g^\alpha)^{r(m)} (g^\alpha)^{\frac{-f(m)\gamma(m)}{t-\tilde{t}}}.
\end{aligned}$$

As above, $\mathcal{B}$ can compute σ_0. To make a signature with the proper distribution, $\mathcal{B}$ just sets $r = \frac{-\alpha f(m)}{t-\tilde{t}} + r'$ (mod p), where $r' \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$. It is obvious that r is uniformly distributed over $\mathbb{Z}/p\mathbb{Z}$ since r' is uniformly chosen. $\mathcal{B}$ then sets (σ_0, σ_1) as

$$\begin{aligned}\sigma_0 &= (g^{\alpha})^{r(m)}(g^{\alpha})^{\frac{-f(m)\gamma(m)}{t-\tilde{t}}}(z(m)h)^{r'},\\ \sigma_1 &= (g^{\alpha})^{\frac{-f(m)}{t-\tilde{t}}}g^{r'}.\end{aligned}$$

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

A's stage.

Given $(vk, \{m_i, \sigma_i, w_i\}_{i=1}^{q})$ from $\mathcal{B}$, $\mathcal{A}$ runs following its strategy. Consider the case that $\mathcal{A}$ successfully produces a forged signature $\sigma^* = (\sigma_0^*, \sigma_1^*)$ on a fresh message $m^* \notin \mathcal{M}$.

Solving the CDH problem.

When $\mathcal{A}$ succeeds to forge (m^*, σ^*), it holds that $f(m^*) \neq 0$ by construction. $\mathcal{B}$ then check the tag $t^* = H(m^*) \mod 2^{j^*}$. If $t^* \neq \tilde{t}$, then B aborts; otherwise, it outputs the solution of the CDH problem $g^{\alpha\beta}$ as follows:

$$\left(\frac{\sigma_0^*}{(g^{\alpha})^{r(m^*)}(\sigma_1^*)^{\gamma(m^*)}}\right)^{1/f(m^*)} = g^{\alpha\beta}.$$

Security Analysis.

By construction, it is obvious that the simulated verification key and signatures are properly distributed conditioned that $(d+1)$-fold doesn't happen on chosen tag $\tilde{t} \in T_{j^*}$, i.e., $\#\mathcal{M}' \leq d$, where $\mathcal{M}' := \{m \in \mathcal{M} \,|\, \tilde{t} = H(m) \bmod 2^{j^*}\}$. Let us denote by $(d+1)\text{-fold}^{\mathsf{real}}$ the event that $(d+1)$-fold happens on some tag in T_{j^*} when $t_1^{(j)}, \ldots, t_q^{(j)}$ in T_{j^*} are chosen according to the distribution of MsgGen. Then, the forging probability of $\mathcal{A}$ is at least $\epsilon^{\mathsf{euf\text{-}xrma}} - \Pr[(d+1)\text{-fold}^{\mathsf{real}}]$.

$\mathcal{B}$ can solve the CDH problem as above when $t^* = \tilde{t}$ where $t^* := H(m^*) \mod 2^{j^*}$. Note that the information about $\tilde{t}$ is perfectly hidden from the adversary's view. Hence, the probability that $\mathcal{B}$ can solve the CDH problem is $\frac{1}{\#T_{j^*}}(\epsilon^{\mathsf{euf\text{-}xrma}} - \Pr[(d+1)\text{-fold}^{\mathsf{real}}])$. Since $\frac{1}{\#T_{j^*}} = O(\frac{d}{q})$, we have

$$\epsilon^{\mathsf{euf\text{-}xrma}} = O(\frac{q}{d}) \cdot \epsilon^{\mathsf{cdh}} + \Pr[(d+1)\text{-fold}^{\mathsf{real}}].$$

Finally, we prove that $\Pr[(d+1)\text{-fold}^{\mathsf{real}}]$ is exponentially small.

Claim 3: $\Pr[(d+1)\text{-fold}^{\mathsf{real}}] = \Pr[(d+1)\text{-fold}^{\mathsf{ideal}}] + 2^{-O(\kappa)}$, where $T = T_{j^*}$.

Proof of Claim 3. Let m be a message outputted by MsgGen defined in Sec. 3. By construction, m can be seen as an element in $\mathbb{Z}/p\mathbb{Z}$. Although m is not distributed uniformly over $\mathbb{Z}/p\mathbb{Z}$, we know that $\mathsf{H}_{\infty}(m) = \kappa - 1$, since $p = 2q' - 1$. Therefore, due to the left-over hash lemma, the distribution of $t^{(j^*)} = H(m) \bmod 2^{j^*}$ derived by MsgGen is statistically close to the uniform distribution over T_{j^*}, whose distance is bounded by $\frac{1}{2}2^{\frac{-(\mathsf{H}_{\infty}(m)-\omega(\log \kappa))}{2}} = 2^{-O(\kappa)}$. Considering independent q messages of MsgGen, the distance should be multipled by $q = O(\mathrm{poly}(\kappa))$, but still $2^{-O(\kappa)}$. □

By the claim above, $\Pr[(d+1)\text{-fold}^{\mathsf{real}}] = 2^{-O(\kappa)}$, since $\Pr[(d+1)\text{-fold}^{\mathsf{ideal}}] = 2^{-O(\kappa)}$. We have now concluded the proof. □

4. EUF-CMA Full Security Scheme

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

4.1 Construction

Let SIG_1 be a signature scheme constructed by applying TCOM to SIG_0. We describe it in Fig. 4. The correctness of SIG_1 can be shown in the same way as SIG_0, so it is omitted here (See Appendix B).

Lemma 4: The signature scheme SIG_1 is non-re-randomizable.

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

$$e(\sigma_0, g) = e\left(u(\psi), g^{\alpha}\right) e\left(z(\psi)h, \sigma_1\right). \tag{6}$$

The set of all σ satisfying (6) is therefore identical to the set

$$\begin{aligned}\Sigma(vk, m) &= \{\sigma | \mathsf{Vrfy}(vk, m, \sigma, r) = 1\}\\ &= \left\{\begin{array}{l}\sigma_0 = (u(\psi))^{\alpha}(z(\psi)h)^{s}, \sigma_1 = g^{s};\\ s \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z},\ r \leftarrow \mathsf{COIN}^{\mathsf{com}}\end{array}\right\}.\end{aligned}$$

Consider a PPT algorithm Rerand taking as input vk, σ, and message m. We assume that Rerand samples $s' \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ and returns $\sigma' = (\sigma_0', \sigma_1')$ distributed uniformly over $\Sigma(vk, m)$. However, since Rerand cannot generate $\psi = \mathsf{Com}_{pk}^{\mathsf{tc}}(x; r)$; $r \leftarrow \mathsf{COIN}^{\mathsf{com}}$, there is no Rerand that returns the new signature σ' distributed uniformly over the set of all possible signatures for m. Hence, SIG_1 is non-re-randomizable. □

4.2 Security Analysis

Theorem 5: If $\mathsf{TCOM} = (\mathsf{KGen}^{\mathsf{tc}}, \mathsf{Com}^{\mathsf{tc}}, \mathsf{TCom}^{\mathsf{tc}}, \mathsf{TCol}^{\mathsf{tc}})$ is a trapdoor commitment scheme described in section 3 and SIG_0 be EUF-XRMA secure, with respect to MsgGen then SIG_1 is EUF-CMA secure.

Proof. As we can regard commitments as input in SIG_0 instead of messages, let a PPT $\mathcal{B}_{\mathsf{SIG}_0}^{\mathsf{euf\text{-}xrma}}$ as the adversary against EUF-XRMA security with TCOM of SIG_0, and a PPT $\mathcal{B}^{\mathsf{bind}}$ be a adversary against computational binding for TCOM. Now we show that if a PPT $\mathcal{A}_{\mathsf{SIG}_1}^{\mathsf{euf\text{-}cma}}$ who can break EUF-CMA security of SIG_1 exists, then $\mathcal{B}_{\mathsf{SIG}_0}^{\mathsf{euf\text{-}xrma}}$ or $\mathcal{B}^{\mathsf{bind}}$ exists.

We consider two cases with respect to the outputs of a EUF-XRMA with TCOM game; when commitments $\{\psi_1, \ldots, \psi_q\}$ queried as messages do not contain challenge

```
KGen(1^κ)
    $(\mathbb{G}, \mathbb{G}_T, p, e, g) \leftarrow \mathcal{G}(\kappa).$
    $\alpha \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$
    $a, b \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$ $(H(x) := (ax + b) \bmod p)$
    $(h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}) \xleftarrow{\$} \mathbb{G}$
    $(tk, pk) \leftarrow \mathsf{KGen}^{\mathsf{tc}}(1^\kappa)$
     $vk = (H, g, g^\alpha, h, \{u_i\}_{i=0}^{d}, \{z_j\}_{j=1}^{l}, pk)$
     $sk = (\alpha, vk)$
     return $(vk, sk)$

Sign(sk, m)
    $r \leftarrow \mathsf{COIN}^{\mathsf{com}}, s \xleftarrow{\$} \mathbb{Z}/p\mathbb{Z}$
    $\psi = \mathsf{Com}_{pk}^{\mathsf{tc}}(m; r)$
    $u(\psi) = \prod_{i=0}^{d} u_i^{\psi^i}$
    For $j := 1$ to $l$ do
        $t^{(j)} = H(\psi) \mod 2^j$
    $z(\psi) = \prod_{j=1}^{l} z_j^{t^{(j)}}$
    $\sigma_0 = u(\psi)^\alpha (z(\psi)h)^s$
    $\sigma_1 = g^s$
    return $(\sigma = (\sigma_0, \sigma_1), r)$

Vrfy(vk, m, σ, r)
    $\psi = \mathsf{Com}_{pk}^{\mathsf{tc}}(m; r)$
    For $i := 1$ to $l$ do
        $t^{(j)} = H(\psi) \mod 2^j$
    If $e(\sigma_0, g)$
        $\neq e(u(\psi), g^\alpha) e(z(\psi)h, \sigma_1)$
        return 0
    else
        return 1
```

Fig. 4 SIG_1: EUF-CMA-secure signature scheme with TCOM under the CDH assumption.

commitment ψ^*, $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ which breaks EUF-XRMA security with TCOM exists (**Case 1**) and when $\{\psi_1, \ldots, \psi_q\}$ contains ψ^*, $\mathcal{B}^{\text{bind}}$ which breaks computational binding exists (**Case 2**).

Here, we write the verification key and signing key of SIG_0 as (vk_0, sk_0). From the view of $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$, it is statistically indistinguishable that views of $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ and $\mathcal{B}^{\text{bind}}$.

Setup

We consider $\mathsf{TCom}_{tk}^{\mathsf{tc}}$ as MsgGen of EUF-XRMA, then commitments are generated with auxiliary information such that $(\psi_i, \bar{r}_i) \leftarrow \mathsf{TCom}_{tk}^{\mathsf{tc}}(1^k)$. $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ receives the verification key vk_0, for $1 \leq i \leq q$, commitment ψ_i, signature σ_i of SIG_0, and auxiliary information $w_i = (pk, tk, \bar{r}_i)$, where pk is the public key and tk is the trapdoor key for TCOM. The commitment ψ_i satisfies that $\psi_i = \mathsf{Com}_{pk}^{\mathsf{tc}}(x_i; \bar{r}_i)$ for $x_i \in \mathcal{M}_\kappa$ and σ_i is the signature of SIG_0 for ψ_i. $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ sets $vk = (vk_0, pk)$ and send vk to $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$.

Signing

$\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$ makes q signing queries. For $1 \leq i \leq q$, $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$ gives a message m_i to $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$. Then $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ computes $r_i = \mathsf{TCol}_t^{\mathsf{tc}}k^tc(\psi_i, \bar{r}_i, m_i)$, where r_i satisfies $\psi_i = \mathsf{Com}_p^{\mathsf{tc}}k^tc(m_i; r_i)$. According to the trapdoor property of TCOM, it is statistically indistinguishable whether ψ_i was received from $\mathsf{TCom}_{tk}^{\mathsf{tc}}$ as MsgGen in *Setup* or generated from m_i by $\mathsf{Com}_{pk}^{\mathsf{tc}}$. $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ then returns (σ_i, r_i) for ψ_i corresponding to m_i. Here, the signatures which $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ firstly received as input are regarded as that of SIG_1 since messages can be just replaced by commitments.

Forgery of $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$

$\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ receives a forgery (m^*, σ^*, r^*) of SIG_1 from $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$, where $m^* \notin \{m_1, \ldots, m_q\}$. $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ then computes commitment $\psi^* = \mathsf{Com}_{pk}^{\mathsf{tc}}(m^*; r^*)$.
Case 1: $\psi^* \notin \{\psi_1, \ldots, \psi_q\}$. In this case that $\psi^* \notin \{\psi_1, \ldots, \psi_q\}$, $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ 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 2.
Case 2: $\psi^* \in \{\psi_1, \ldots, \psi_q\}$. In this case that $\psi^* \in \{\psi_1, \ldots, \psi_q\}$, $\mathcal{B}^{\text{bind}}$ 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 $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ succeeds in breaking computational binding for trapdoor commitment as $\mathcal{B}^{\text{bind}}$.

Analysis

Let $\varepsilon^{\text{euf-xrma}}$ be an advantage of $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$, $\varepsilon^{\text{bind}}$ be an advantage of $\mathcal{B}^{\text{bind}}$, and $\varepsilon^{\text{euf-cma}}$ be an advantage of $\mathcal{A}^{\text{euf-cma}}_{\mathsf{SIG}_1}$. $\mathcal{B}^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ breaks EUF-XRMA security when $\psi^* \notin \{\psi_1, \ldots, \psi_q\}$ or $\mathcal{B}^{\text{bind}}$ breaks computational binding for trapdoor commitments when $\psi^* \in \{\psi_1, \ldots, \psi_q\}$. Therefore $\varepsilon^{\text{euf-cma}}_{\mathsf{SIG}_1}$ is bounded by sum of $\varepsilon^{\text{euf-xrma}}_{\mathsf{SIG}_0}$ and $\varepsilon^{\text{bind}}$. Hence,

$$\varepsilon^{\text{euf-cma}} \leq \varepsilon^{\text{bind}} + \varepsilon^{\text{euf-xrma}}.$$

□

5. Discussion

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

$$\varepsilon^{\text{CDH}} \geq \frac{1}{T_{j^*}} \left(\varepsilon^{\text{euf-cma}} - \varepsilon^{\text{PRF}} - Pr[(d+1)\text{-fold}^{\text{real}}] \right),$$

where T_{j^*} is the size of tag sets. In our scheme, $\#T_{j^*} = O(\frac{q}{d})$ since its tag space is $T_{j^*} := \lfloor (d+1)/e \cdot q \rfloor + 1$. The advantage ε^{PRF} regarding PRF is $1/2^{O(\kappa)}$, 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:

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

Since they assumed that the size of d is constant, the evaluation was sufficient. However, we assume $d = O(\kappa)$; thus, we evaluate the probability more strictly. Lemma 1 shows that the probability is exponentially small. Moreover, we can eliminate the reduction loss of PRF thanks to EUF-XRMA security where messages are generated of by a message generator MsgGen instead of the PRF in the experiment.

According to Theorems 2 and 5,

$$\begin{aligned}
&\varepsilon^{\text{CDH}} \\
&\geq \frac{1}{T_{j^*}}\left(\varepsilon^{\text{euf-xrma}} - \Pr[(d+1)\text{-fold}^{\text{real}}] - \frac{1}{2^{\mathcal{O}(\kappa)}}\right) \\
&\geq \mathcal{O}\left(\frac{d}{q}\right)\cdot\varepsilon^{\text{euf-xrma}} \\
&\geq \mathcal{O}\left(\frac{d}{q}\right)\cdot\left(\varepsilon^{\text{euf-cma}} - \varepsilon^{\text{bind}}\right)
\end{aligned}$$

Hence,

$$\varepsilon^{\text{euf-cma}} \leq \mathcal{O}\left(\frac{q}{d}\right)\cdot\varepsilon^{\text{CDH}} + \varepsilon^{\text{bind}}.$$

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 for choosing 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, although the vk size of our scheme 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 any constant-size signature schemes. Particularly, its security reduction, $\mathcal{O}(q/d)$, is the tightest thus far.

References

[1] M. Abe, M. Chase, B. David, M. Kohlweiss, R. Nishimaki, and M. Ohkubo, "Constant-size structure-preserving signatures: Generic constructions and simple assumptions," J. Cryptol., vol.29, no.4, pp.833–878, 2016.

[2] D. Boneh and M. Franklin, "Identity-based encryption from Weil paring," Annual International Cryptology Conference, pp.213–229, 2001.

[3] D. Boneh, and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," International Conference on the Theory and Applications of Cryptographic Techniques, pp.223–238, 2004.

[4] X. Boyen, "Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more," Public Key Cryptography, LNCS, vol.6056, pp.499–517, 2010.

[5] E. Boyle, S. Goldwasser, and I. Ivan, "Functional signatures and pseudorandom functions," International Workshop on Public Key Cryptography, pp.501–519, 2014.

[6] F. Böhl, D. Hofheinz, T. Jager, J. Koch, J.H. Seo, and C. Striecks, "Practical signatures from standard assumptions," Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp.461–485, 2013.

[7] F. Böhl, D. Hofheinz, T. Jager, J. Koch, and C. Striecks, "Confined guessing: New signatures from standard assumptions," J. Cryptol., vol.28, no.1, pp.176–208, 2015.

[8] O. Blazy, S.A. Kakvi, E. Kiltz, and J. Pan, "Tightly-secure signatures from chameleon hash functions," Public Key Cryptography, pp.256–279, 2015.

[9] D. Boneh, I. Mironov, and V. Shoup, "A secure signature scheme from bilinear maps," CT-RSA, LNCS, vol.2612, pp.98–110, 2003.

[10] B. Chevallier-Mames, "An efficient CDH-based signature scheme with a tight security reduction," Annual International Cryptology Conference, pp.511–526, 2005.

[11] B. Chevallier-Mames and M. Joye, "A practical and tightly secure signature scheme without hash function," CT-RSA, LNCS, vol.4377, pp.339–356, 2007.

[12] J. Chen, and H. Wee, "Fully, (almost) tightly secure IBE and dual system groups," Advances in Cryptology CRYPTO 2013, pp.435–460, 2013.

[13] I. Damgård, "Efficient concurrent zero-knowledge in the auxiliary string model," International Conference on the Theory and Applications of Cryptographic Techniques, pp.418–430, 2000.

[14] L. Ducas and D. Micciancio, "Improved short lattice signatures in the standard model," International Cryptology Conference, pp.335–352, 2014.

[15] O. Goldreich, "Foundation of cryptography (in two volumes: Basic tools and basic applications)," Electronic Colloquium on Computational Complexity, 2001.

[16] E.J. Goh, and S. Jarecki, "A signature scheme as secure as the Diffie-Hellman problem," International Conference on the Theory and Applications of Cryptographic Techniques, pp.401–415, 2003.

[17] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," SIAM J. Comput., vol.17, no.2, pp.281–308, 1988.

[18] D. Hofheinz, "Algebraic partitioning: Fully compact and (almost) tightly secure cryptography," Theory of Cryptography Conference, pp.251–281, 2016.

[19] D. Hofheinz and T. Jager, "Tightly secure signatures and public-key encryption," International Cryptology Conference, LNCS, vol.7417 pp.590–607, 2012.

[20] D. Hofheinz, T. Jager, and E. Knapp, "Waters signatures with optimal security reduction," International Workshop on Public Key Cryptography, pp.66–83, 2012.

[21] D. Hofheinz and E. Kiltz, "Programmable hash functions and their applications," J. Cryptol., vol.25, no.3, pp.484–527, 2012.

[22] S. Hohenberger and B. Waters, "Realizing hash-and-sign signatures under standard assumptions," Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp.333–350, 2009.

[23] K. Kajita, K. Ogawa, and E. Fujisaki, "A constant-size signature scheme with tighter reduction from CDH assumption," International Conference on Information Security, pp.137–154, 2017.

[24] J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions," Proc. 10th ACM conference on Computer and communications security, pp.155–164, 2003.

[25] S. Schäge, "Tight proofs for signature schemes without random oracles," International Conference on Theory and Applications of Cryptographic Techniques, LNCS, vol.6632, pp.189–206, 2011.

[26] J.H. Seo, "Short signatures from Diffie-Hellman, revisited: Sublinear public key, CMA security, and tighter reduction," IACR Cryptology ePrint Archive: 138, 2014.

[27] B. Waters, "Efficient identity-based encryption without random oracles," Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp.114–127, 2005.

Appendix A: The Correctness of SIG_0

The correctness of SIG_0 can be proved as follows.

Proof. We show $\mathsf{Vrfy}(vk, m, \sigma) = 1$ for all $m \in \mathcal{M}_\kappa$ and

$\sigma = \mathsf{Sign}(sk, m)$.

In the algorithm $\mathsf{Sign}(sk, m)$, $t = \{t^{(1)}, \ldots, t^{(l)}\}$ is generated, and

$$\begin{aligned}
\sigma &= (\sigma_0, \sigma_1) \\
\sigma_0 &= u(m)^{\alpha}(z(m)h)^{r} \\
\sigma_1 &= g^{r} \\
e(\sigma_0, g) &= e\left(u(m)^{\alpha}(z(m)h)^{r}, g\right) \\
&= e\left(u(m)^{\alpha}, g\right) e\left((z(m)h)^{r}, g\right) \\
&= e\left(u(m), g^{\alpha}\right) e\left((z(m)h), g^{r}\right) \\
&= e\left(u(m), g^{\alpha}\right) e\left((z(m)h), \sigma_1\right).
\end{aligned}$$

Hence, $\mathsf{Vrfy}(vk, m, \sigma)$ always returns 1 for all $m \in \mathcal{M}_{\kappa}$. □

Appendix B: The Correctness of SIG_1

The correctness of SIG_1 can be proved as follows.

Proof. We show $\mathsf{Vrfy}(vk, m, \sigma, r) = 1$ for all $m \in \mathcal{M}_{\kappa}$ and $\sigma = \mathsf{Sign}(sk, m)$.

In both of the algorithms $\mathsf{Sign}(sk, m)$ and $\mathsf{Vrfy}(vk, m, \sigma, r)$, $\psi = \mathsf{Com}^{\mathsf{tc}}_{pk}(m; r)$ and $t = \{t^{(1)}, \ldots, t^{(l)}\}$, where $t^{(j)} = \psi \bmod 2^{j}$, are generated. Then,

$$\begin{aligned}
\sigma &= (\sigma_0, \sigma_1) \\
\sigma_0 &= u(\psi)^{\alpha}(z(\psi)h)^{s} \\
\sigma_1 &= g^{s} \\
e(\sigma_0, g) &= e\left(u(\psi)^{\alpha}(z(\psi)h)^{s}, g\right) \\
&= e\left(u(\psi)^{\alpha}, g\right) e\left((z(\psi)h)^{s}, g\right) \\
&= e\left(u(\psi), g^{\alpha}\right) e\left(z(\psi)h, g^{s}\right) \\
&= e\left(u(\psi), g^{\alpha}\right) e\left(z(\psi)h, \sigma_1\right).
\end{aligned}$$

Hence, $\mathsf{Vrfy}_t(vk, m, \sigma, r)$ always returns 1 for all $m \in \mathcal{M}_{\kappa}$. □

Kaisei Kajita received the B.S. degree from University of Electro Communication in 2015 and M.S. degree from Tokyo Institure of Technology in 2017. He joined NHK (Japan Broadcasting Corporation) in 2017. He is currently a research engineer of NHK Science & Technology Research Laboratories. His research interest include cryptography, information security, Integrated Broadcast-Broadband (IBB) system.

Kazuto Ogawa received the B.E. and Ph.D. degrees from the University of Tokyo in 1987 and 2008, respectively. He joined NHK (Japan Broadcasting Corporation) in 1987. He has mainly engaged in research and development on video image processing systems and digital content rights management systems. He is currently a research engineer of NHK Science & Technology Research Laboratories.

Eiichiro Fujisaki received the B.S. and Ph.D. degrees from Tokyo Institute of Technology in 1991 and 2005, respectively. He joined Nippon Telegraph and Telephone Corporation (NTT) Laboratories in 1991. He mainly engaged in research on cryptography and information security. Since 2017, he has been a Professor in School of Information Science, Japan Advanced Institute of Science and Technology (JAIST). His research interests include cryptography, network security, and computer-aided proofs. He is a member of IEICE, IPSJ, and IACR.