Tight reduction for generic construction of certificateless signature and tightly-secure scheme without pairing

Keitaro Hashimoto*, Wakaha Ogata, and Toi Tomita

Department of Information and Communications Engineering, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550, Japan
*Corresponding author: hashimoto.k.au@m.titech.ac.jp

Abstract. Certificateless signature was proposed by Al-Riyami and Paterson to eliminate the certificate management in the public-key infrastructures and solve the key escrow problem in the identity-based signature. In 2007, Hu et al. proposed a generic construction of certificateless signature. They construct certificateless signature scheme from any standard identity-based signature and signature scheme. However, their security reduction is loose; the security of the constructed scheme depends on the number of users. In this paper, we show that their construction can achieve tight security if the underlying signature scheme is existentially unforgeable under adaptive chosen-message attacks in the multi-user setting with adaptive corruptions. Moreover, we instantiate a tightly-secure certificateless signature scheme without pairing, whose security is independent of the number of users. Best of our knowledge, this scheme is the first tightly-secure certificateless signature scheme.

Keywords: certificateless signatures, key escrow, tight security

1 Introduction

1.1 Background

Signature scheme, IBS, CLS. Digital signatures ensure the validity of a message based on a public key. However, verifiers cannot confirm the owner of the message from the public key alone because verifiers have no information about the issuer of the public key. To confirm the issuer of a public key, we must certify the relationship between the public key and the signer in an external way.

In public-key infrastructure (PKI) setting, a certificate authority issues the certificate that proves the connection between a public key and its owner. However, it is known that certificate management is laborious work.

In 1984, Shamir [Sha84] introduced the concept of identity-based signature (IBS) to eliminate the certificate management. In IBS setting, the user's identity, such as email address, is used as the public key. The corresponding secret key is generated by a trusted key generation center (KGC) and sent to its owner. Although IBS no longer requires certificates, it suffers from the key escrow problem; KGC knows all user's secret keys.

Certificateless signature (CLS) was proposed by Al-Riyami and Paterson [AP03] to solve both certificate management load in PKI and the key escrow problem in IBS. Unlike IBS, KGC only provides a partial private key, which is a part of the full secret key. The other part comes from the user's own choice and is kept secret. Therefore KGC does not have knowledge of the full signing key and key escrow is no longer a problem.

The first CLS scheme and the security definition of CLS were presented in [AP03]. In 2004, Yum and Lee proposed a generic construction of CLS from an IBS and a standard signature [YL04]. Later Hu et al. [HWZ+07] pointed out the security flaw on Yum and Lee construction and fixed it. Since the proposal of [AP03], a lot of CLS scheme using pairings have been proposed [HSM+05; ZWX+06; ZZ08; HHC13; Shi19]. However, these schemes are less efficient because the computational cost of a pairing operation is higher than that of an addition or a scalar multiplication. To improve performance, He et al. proposed the first pairing-free CLS scheme [HCZ12]. Later Tian and Huang revealed that their scheme is insecure [TH13]. In 2014, Gong and Li [GL14] proposed a new CLS scheme. Yeh et al. [YSC+17] proposed a new CLS scheme, but Jia et al. [JHL+18] pointed out the vulnerability of Yeh et al.'s scheme and developed an improved scheme. At present, the secure paring-free CLS schemes are [GL14] and [JHL+18].

Tight security. To prove the security of a cryptographic scheme, we generally construct a reduction algorithm, which turns an efficient attacker on the scheme into an algorithm solving some assumed-to-be-hard computational problem. If the reduction has about the same success probability as the attacker, we say that the reduction is tight and the scheme is tightly-security. If the cryptographic scheme is tightly-secure, we are easy to decide the parameter size because the security of the scheme is independent of other factors such as the number of users or that of hash function evaluations. Besides, we can use the smallest parameters that achieve the desired security level. As a result, data size (e.g. key length or signature length) and computation cost (e.g. signature generation and verification) are reduced. Therefore, tight reductions have been actively studied for many cryptographic primitives.

1.2 Motivation and contribution

Conventional provably secure CLS schemes come with a reduction which loses factors that depends on the number of users or the number of hash function evaluations. For example, the security reductions of [GL14] and [JHL+18] are very loose because they use rewinding technique. The security of CLS schemes from Hu et al. generic construction [HWZ+07] is dependent on the number of users even if underlying IBS and signature are tightly-secure.

Our main goal is to construct a tightly-secure CLS scheme. First, we show Hu et al. generic construction [HWZ+07] achieves tight security by changing the security of the underlying signature scheme. We prove if the underlying signature scheme is existentially unforgeable under adaptive chosen-message attacks in a multi-user setting with adaptive corruptions (MU-EUF-CMA$^{\mathsf{Corr}}$) [BHJ+15], the security of CLS schemes from Hu et al. generic construction is reduced to the security of the underlying signature scheme tightly. This generic construction makes the user easy to construct a new tightly-secure CLS scheme from another assumption without complicated proofs. Second, we instantiate the first tightly-secure CLS scheme without pairing from the tightly-secure IBS scheme [FH18] and the tightly-MU-EUF-CMA$^{\mathsf{Corr}}$-secure signature scheme [GJ18]. Best of our knowledge, the instantiated scheme is the first tightly-secure CLS scheme.

1.3 Paper organization

The rest of the paper is organized as follows. Section 2 introduces notations and definitions of signature, IBS, and CLS. We review the existing generic construction of certificateless signature [HWZ+07] in Section 3. Section 4 presents a tight reduction for the generic construction. In Section 5, we instantiate a tightly-secure certificateless signature scheme without pairing and compare it with other pairing-free CLS schemes. The conclusion of this paper is given in Section 6.

2 Preliminaries

2.1 Notation

If $x_1, \ldots, x_n$ are strings, we denote $x_1 \| \cdots \| x_n$ by the concatenation of $x_1, \ldots, x_n$. If x is a string, then $|x|$ denotes its length. For a PPT algorithm $\mathcal{A}$,

$$\mathcal{A}(x_1, x_2, \ldots; O_1, O_2, \ldots)$$

means $\mathcal{A}$ has inputs $x_1, x_2, \ldots$ and access to oracles $O_1, O_2, \ldots$.

A function f is said to be negligible on λ, if, for any polynomial ν, there exists a natural number λ_0 such that $f(\lambda) < 1/\nu(\lambda)$ for any $\lambda > \lambda_0$.

2.2 Digital signature

A signature scheme Sig consists of three algorithms:

- $\mathsf{Sig.KGen}(1^\lambda)$: On input the security parameter 1^λ, the key generation algorithm outputs a key pair (sk, pk).
- $\mathsf{Sig.Sign}(sk, M)$: On input a private key sk and a message M, the signing algorithm outputs a signature σ.
- $\mathsf{Sig.Vrfy}(pk, M, \sigma)$: On input a public key pk, a message M, and a signature σ, the verification algorithm outputs 0 or 1.

For correctness, we require that for all $\lambda \in \mathbb{N}$ and $M \in \{0,1\}^*$, if $(sk, pk) \leftarrow \mathsf{Sig.KGen}(1^\lambda)$ and $\sigma \leftarrow \mathsf{Sig.Sign}(sk, M)$, then $\Pr[\mathsf{Sig.Vrfy}(pk, M, \sigma) = 1] = 1$ holds.

For security, we define standard existential unforgeability under adaptive chosen-message attacks, called EUF-CMA security in [GMR88].

Experiment $\mathsf{Exp}^{\text{euf-cma}}_{\mathsf{Sig},\mathcal{A}}(\lambda)$

$(pk, sk) \leftarrow \mathsf{Sig.KGen}(1^\lambda)$; $MSG \leftarrow \emptyset$
$(M^*, \sigma^*) \leftarrow \mathcal{A}(pk; \mathbf{SIGN})$
if $M^* \notin MSG \wedge \mathsf{Sig.Vrfy}(pk, M^*, \sigma^*) = 1$
  return 1
else return 0

Oracle $\mathbf{SIGN}(M)$

$\sigma \leftarrow \mathsf{Sig.Sign}(sk, M)$
$MSG \leftarrow MSG \cup \{M\}$
return σ

Fig. 1. Experiment used to define EUF-CMA security for signature scheme.

Definition 1. *Let* Sig *is a signature scheme,* $\mathcal{A}$ *an adversary, and* $\lambda \in \mathbb{N}$ *a security parameter. Define the experiment* $\mathsf{Exp}^{euf\text{-}cma}_{\mathsf{Sig},\mathcal{A}}(\lambda)$ *as shown in Fig. 1. The EUF-CMA advantage of* $\mathcal{A}$ *in attacking* Sig *is*

$$\mathsf{Adv}^{euf\text{-}cma}_{\mathsf{Sig},\mathcal{A}}(\lambda) = \Pr\left[\mathsf{Exp}^{euf\text{-}cma}_{\mathsf{Sig},\mathcal{A}}(\lambda) = 1\right].$$

We say that Sig *is an EUF-CMA-secure signature scheme if* $\mathsf{Adv}^{euf\text{-}cma}_{\mathsf{Sig},\mathcal{A}}(\lambda)$ *is negligible for any* PPT *adversary* $\mathcal{A}$*.*

Next we define multi-user existential unforgeability under adaptive chosen-message attacks with adaptive corruptions, called MU-EUF-CMA$^{\mathsf{Corr}}$ in [BHJ+15].

Definition 2. *Let* Sig *is a signature scheme,* $\mathcal{A}$ *an adversary, and* $\lambda \in \mathbb{N}$ *a security parameter. Define the experiment* $\mathsf{Exp}^{mu\text{-}euf\text{-}cma\text{-}corr}_{\mathsf{Sig},\mathcal{A}}(\lambda)$ *as shown in Fig. 2. The MU-EUF-CMA*$^{\mathsf{Corr}}$ *advantage of* $\mathcal{A}$ *in attacking* Sig *is*

$$\mathsf{Adv}^{mu\text{-}euf\text{-}cma\text{-}corr}_{\mathsf{Sig},\mathcal{A}}(\lambda) = \Pr\left[\mathsf{Exp}^{mu\text{-}euf\text{-}cma\text{-}corr}_{\mathsf{Sig},\mathcal{A}}(\lambda) = 1\right].$$

We say that Sig *is a MU-EUF-CMA*$^{\mathsf{Corr}}$*-secure signature scheme if* $\mathsf{Adv}^{mu\text{-}euf\text{-}cma\text{-}corr}_{\mathsf{Sig},\mathcal{A}}(\lambda)$ *is negligible for any* PPT *adversary* $\mathcal{A}$*.*

Experiment $\mathsf{Exp}^{\text{mu-euf-cma-corr}}_{\mathsf{Sig},\mathcal{A}}(\lambda)$

for 1 **to** μ **do**
  $(pk_i, sk_i) \leftarrow \mathsf{Sig.KGen}(1^\lambda)$
$CU \leftarrow \emptyset$; $MSG[1] \leftarrow \emptyset, ..., MSG[\mu] \leftarrow \emptyset$
$(i^*, M^*, \sigma^*) \leftarrow \mathcal{A}(pk_1, ..., pk_\mu; \mathbf{CORR}, \mathbf{SIGN})$
if $i^* \notin CU \wedge M^* \notin MSG[i^*] \wedge \mathsf{Sig.Vrfy}(pk_{i^*}, M^*, \sigma^*) = 1$
  return 1
else return 0

Oracle $\mathbf{CORR}(i)$

$CU \leftarrow CU \cup \{i\}$
return sk_i

Oracle $\mathbf{SIGN}(M, i)$

$\sigma \leftarrow \mathsf{Sig.Sign}(sk_i, M)$
$MSG[i] \leftarrow MSG[i] \cup \{M\}$
return σ

Fig. 2. Experiment used to define MU-EUF-CMA$^{\mathsf{Corr}}$ security for signature scheme.

2.3 Identity-based signature

An identity-based signature scheme IBS consists of four algorithms:

- $\mathsf{IBS.Setup}(1^\lambda)$: On input 1^λ, the setup algorithm outputs a key pair (msk, mpk).
- $\mathsf{IBS.Extract}(mpk, msk, ID)$: On input a master public key mpk, a master secret key msk, and an identity ID, the key extraction algorithm outputs a key usk.
- $\mathsf{IBS.Sign}(mpk, ID, usk, M)$: On input mpk, ID, usk, and a message M, the signing algorithm outputs a signature σ.
- $\mathsf{IBS.Vrfy}(mpk, ID, M, \sigma)$: On input mpk, ID, a message M, and a signature σ, the verification algorithm outputs 0 or 1.

For correctness, we require that for all $\lambda \in \mathbb{N}$, $ID \in \{0,1\}^*$, and $M \in \{0,1\}^*$, if $(msk, mpk) \leftarrow \mathsf{IBS.Setup}(1^\lambda)$, $usk \leftarrow \mathsf{IBS.Extract}(mpk, msk, ID)$, and $\sigma \leftarrow \mathsf{IBS.Sign}(mpk, ID, usk, M)$, then $\Pr[\mathsf{IBS.Vrfy}(mpk, ID, M, \sigma) = 1] = 1$ holds.

The existential unforgeability under adaptive chosen message attacks (ID-EUF-CMA) of IBS is defined as follows [BNN09]:

Definition 3. *Let IBS is an identity-based signature scheme, $\mathcal{A}$ an adversary, and $\lambda \in \mathbb{N}$ a security parameter. Define the experiment $\mathsf{Exp}^{id\text{-}euf\text{-}cma}_{\mathsf{IBS},\mathcal{A}}(\lambda)$ as shown in Fig. 3. The ID-EUF-CMA advantage of $\mathcal{A}$ in attacking IBS is*

$$\mathsf{Adv}^{id\text{-}euf\text{-}cma}_{\mathsf{IBS},\mathcal{A}}(\lambda) = \Pr\left[\mathsf{Exp}^{id\text{-}euf\text{-}cma}_{\mathsf{IBS},\mathcal{A}}(\lambda) = 1\right].$$

We say that IBS is an ID-EUF-CMA-secure IBS scheme if $\mathsf{Adv}^{id\text{-}euf\text{-}cma}_{\mathsf{IBS},\mathcal{A}}(\lambda)$ is negligible for any PPT adversary $\mathcal{A}$.

Oracle **INIT**(ID)

if $ID \in CU \cup HU$ **then return** $\perp$
$usk[ID] \leftarrow \mathsf{IBS.Extract}(mpk, msk, ID)$
$MSG[ID] \leftarrow \emptyset; HU \leftarrow HU \cup \{ID\}$
return 1

Oracle **EXT**(ID)

$HU \leftarrow HU \setminus \{ID\}$
$CU \leftarrow CU \cup \{ID\}$
return $usk[ID]$

Oracle **SIGN**(ID, M)

if $ID \notin HU$ **then return** $\perp$
$\sigma \leftarrow \mathsf{IBS.Sign}(mpk, ID, usk[ID], M)$
$MSG[ID] \leftarrow MSG[ID] \cup \{M\}$
return σ

Experiment $\mathsf{Exp}^{\text{id-euf-cma}}_{\mathsf{IBS},\mathcal{A}}(\lambda)$

$(msk, mpk) \leftarrow \mathsf{IBS.Setup}(1^\lambda)$
$HU \leftarrow \emptyset; CU \leftarrow \emptyset$
$(ID^*, M^*, \sigma^*) \leftarrow \mathcal{A}(mpk; \mathbf{INIT}, \mathbf{EXT}, \mathbf{SIGN})$
if $ID^* \in HU \land M^* \notin MSG[ID^*] \land \mathsf{IBS.Vrfy}(mpk, ID^*, M^*, \sigma^*) = 1$
  return 1
else return 0

Fig. 3. Experiment used to define ID-EUF-CMA security for identity-based signature scheme.

2.4 Certificateless signature

A certificateless signature scheme CLS consists of five algorithms:

- $\mathsf{CLS.Setup}(1^\lambda)$: On input 1^λ, the setup algorithm outputs a key pair (msk, mpk).
- $\mathsf{CLS.PPKExtract}(mpk, msk, ID)$: On input a master public key mpk, a master secret key msk, and an identity ID, the partial private key extraction algorithm outputs a partial-private-key psk.
- $\mathsf{CLS.UserKeyGen}(mpk, ID)$: On input mpk and ID, the user key generation algorithm outputs a key pair (sk, pk).
- $\mathsf{CLS.Sign}(mpk, ID, psk, sk, pk, M)$: On input mpk, ID, psk, sk, pk, and a message M, the signing algorithm outputs a signature σ.
- $\mathsf{CLS.Vrfy}(mpk, ID, pk, M, \sigma)$: On input mpk, ID, pk, M, and σ, the verification algorithm outputs 0 or 1.

For correctness, we require that for all $\lambda \in \mathbb{N}$, $ID \in \{0,1\}^*, M \in \{0,1\}^*$, if $(msk, mpk) \leftarrow \mathsf{CLS.Setup}(1^\lambda)$, $psk \leftarrow \mathsf{CLS.PPKExtract}(mpk, msk, ID)$, $(sk, pk) \leftarrow \mathsf{CLS.UserKeyGen}(mpk, ID)$, and $\sigma \leftarrow \mathsf{CLS.Sign}(mpk, ID, usk, sk, pk, M)$, then $\Pr[\mathsf{CLS.Vrfy}(mpk, ID, pk, M, \sigma) = 1] = 1$ holds.

In CLS setting, there exist two types of adversaries, $\mathcal{A}_1$ and $\mathcal{A}_2$. Adversary $\mathcal{A}_1$ represents malicious users. $\mathcal{A}_1$ can compromise the target user's secret key or replace the public key but cannot obtain the master secret key nor the partial private keys. $\mathcal{A}_2$ represents a malicious KGC. $\mathcal{A}_2$ knows the master secret key and partial private keys but is not able to obtain the user secret key nor replace the public keys.

As in [HWZ+07], we define existential unforgeability under adaptive chosen-message attacks for both adversaries.

Definition 4. *Let* CLS *is a certificateless signature scheme,* $\mathcal{A}_1$ *an adversary, and* $\lambda \in \mathbb{N}$ *a security parameter. Define the experiment* $\mathsf{Exp}^{\textit{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda)$ *as shown in Fig. 4. The CL-EUF-CMA-1 advantage of* $\mathcal{A}_1$ *in attacking* CLS *is*

$$\mathsf{Adv}^{\textit{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda) = \Pr\left[\mathsf{Exp}^{\textit{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda) = 1\right].$$

We say that CLS *is a CL-EUF-CMA-1-secure CLS scheme if* $\mathsf{Adv}^{\textit{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda)$ *is negligible for any* PPT *adversary* $\mathcal{A}_1$*.*

Definition 5. *Let* CLS *is a certificateless signature scheme,* $\mathcal{A}_2$ *an adversary, and* $\lambda \in \mathbb{N}$ *a security parameter. Define the experiment* $\mathsf{Exp}^{\textit{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda)$ *as shown in Fig. 4. The CL-EUF-CMA-2 advantage of* $\mathcal{A}_2$ *in attacking* CLS *is*

$$\mathsf{Adv}^{\textit{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda) = \Pr\left[\mathsf{Exp}^{\textit{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda) = 1\right].$$

We say that CLS *is a CL-EUF-CMA-2-secure CLS scheme if* $\mathsf{Adv}^{\textit{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda)$ *is negligible for any* PPT *adversary* $\mathcal{A}_2$*.*

Oracle $\mathbf{CU}(ID)$

$\textbf{if } ID \in CU \cup HU \textbf{ then return } \bot$
$usk[ID] \leftarrow \mathsf{CLS.PPKExtract}(mpk, msk, ID)$
$(sk[ID], pk[ID]) \leftarrow \mathsf{CLS.UserKeyGen}(mpk, ID)$
$MSG[ID] \leftarrow \emptyset; HU \leftarrow HU \cup \{ID\}$
$\textbf{return } pk[ID]$

Oracle $\mathbf{PPK}(ID)$

$\textbf{if } ID \notin HU \textbf{ then return } \bot$
$HU \leftarrow HU \setminus \{ID\}$
$CU \leftarrow CU \cup \{ID\}$
$\textbf{return } usk[ID]$

Oracle $\mathbf{SK}1(ID)$

$\textbf{if } ID \notin HU \textbf{ then return } \bot$
$\textbf{return } sk[ID]$

Oracle $\mathbf{SK}2(ID)$

$\textbf{if } ID \notin HU \textbf{ then return } \bot$
$HU \leftarrow HU \setminus \{ID\}$
$CU \leftarrow CU \cup \{ID\}$
$\textbf{return } sk[ID]$

Oracle $\mathbf{PKR}(ID, pk')$

$\textbf{if } ID \notin HU \cup CU \textbf{ then return } \bot$
$pk[ID] \leftarrow pk', sk[ID] \leftarrow \bot$
$\textbf{return } 1$

Oracle $\mathbf{SIGN}(ID, M)$

$\textbf{if } ID \notin HU \vee sk[ID] = \bot \textbf{ then return } \bot$
$\sigma \leftarrow \mathsf{CLS.Sign}(mpk, ID, usk[ID], sk[ID], pk[ID], M)$
$MSG[ID] \leftarrow MSG[ID] \cup \{M\}$
$\textbf{return } \sigma$

Experiment $\mathsf{Exp}^{\text{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda)$

$(msk, mpk) \leftarrow \mathsf{CLS.Setup}(1^\lambda)$
$HU \leftarrow \emptyset; CU \leftarrow \emptyset$
$(ID^*, M^*, \sigma^*) \leftarrow \mathcal{A}_1(mpk; \mathbf{CU}, \mathbf{PPK}, \mathbf{SK}1, \mathbf{PKR}, \mathbf{SIGN})$
$\textbf{if } ID^* \in HU \wedge M^* \notin MSG[ID^*] \wedge \mathsf{CLS.Vrfy}(mpk, ID^*, pk[ID^*], M^*, \sigma^*) = 1$
$\quad \textbf{return } 1$
$\textbf{else return } 0$

Experiment $\mathsf{Exp}^{\text{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda)$

$(msk, mpk) \leftarrow \mathsf{CLS.Setup}(1^\lambda)$
$HU \leftarrow \emptyset; CU \leftarrow \emptyset$
$(ID^*, M^*, \sigma^*) \leftarrow \mathcal{A}_2(msk, mpk; \mathbf{CU}, \mathbf{PKR}, \mathbf{SK}2, \mathbf{SIGN})$
$\textbf{if } ID^* \in HU \wedge sk[ID^*] \neq \bot \wedge M^* \notin MSG[ID^*] \wedge \mathsf{CLS.Vrfy}(mpk, ID^*, pk[ID^*], M^*, \sigma^*) = 1$
$\quad \textbf{return } 1$
$\textbf{else return } 0$

Fig. 4. Experiment used to define CL-EUF-CMA security of the scheme.

$\underline{\mathsf{CLS.Setup}(1^\lambda)}$

$(msk, mpk) \leftarrow \mathsf{IBS.Setup}(1^\lambda)$
return (msk, mpk)

$\underline{\mathsf{CLS.PPKExtract}(msk, ID)}$

$psk_{ID} \leftarrow \mathsf{IBS.Extract}(msk, ID)$
return psk_{ID}

$\underline{\mathsf{CLS.UserKeyGen}(mpk, ID)}$

$(sk_{ID}, pk_{ID}) \leftarrow \mathsf{Sig.KGen}(1^\lambda)$
return (sk_{ID}, pk_{ID})

$\underline{\mathsf{CLS.Sign}(mpk, ID, psk_{ID}, sk_{ID}, pk_{ID}, M)}$

$\sigma_1 \leftarrow \mathsf{Sig.Sign}(sk_{ID}, M \| mpk \| ID \| pk_{ID})$
$\sigma_2 \leftarrow \mathsf{IBS.Sign}(mpk, ID, psk_{ID}, M \| mpk \| ID \| pk_{ID} \| \sigma_1)$
return (σ_1, σ_2)

$\underline{\mathsf{CLS.Vrfy}(mpk, ID, pk_{ID}, M, \sigma)}$

Parse $(\sigma_1, \sigma_2) \leftarrow \sigma$
if $\mathsf{IBS.Vrfy}(mpk, ID, M \| mpk \| ID \| pk_{ID}, \sigma_1) = 0$
  return 0
if $\mathsf{Sig.Vrfy}(pk_{ID}, M \| mpk \| ID \| pk_{ID} \| \sigma_1, \sigma_2) = 0$
  return 0
else return 1

Fig. 5. Generic construction of CLS.

3 Generic construction of certificateless signature

In this section, we review Hu et al. construction in [HWZ+07]. Let $\mathsf{IBS} = (\mathsf{IBS.Setup}, \mathsf{IBS.Extract}, \mathsf{IBS.Sign}, \mathsf{IBS.Vrfy})$ be an ID-EUF-CMA-secure identity-based scheme and $\mathsf{Sig} = (\mathsf{Sig.KGen}, \mathsf{Sig.Sign}, \mathsf{Sig.Vrfy})$ be an EUF-CMA-secure signature scheme. CLS scheme from Hu et al. construction $\mathsf{CLS} = (\mathsf{CLS.Setup}, \mathsf{CLS.PPKExtract}, \mathsf{CLS.UserKeyGen}, \mathsf{CLS.Sign}, \mathsf{CLS.Vrfy})$ is described in Fig. 5.

The following propositions hold for the construction.

Proposition 1 ([HWZ+07, Theorem 1]). *For any Type-I adversary $\mathcal{A}_1$ that breaks the CL-EUF-CMA-1 security of CLS, there exists an algorithm $\mathcal{B}_1$ that breaks the ID-EUF-CMA security of IBS, where*

$$\mathsf{Adv}^{\textit{cl-euf-cma-1}}_{\mathsf{CLS},\mathcal{A}_1}(\lambda) = \mathsf{Adv}^{\textit{id-euf-cma}}_{\mathsf{IBS},\mathcal{B}_1}(\lambda).$$

Proposition 2 ([HWZ+07, Theorem 2]). *Let Q_{cu} be the number of queries for $\boldsymbol{CU}$ oracle, i.e. the number of users. For any Type-II adversary $\mathcal{A}_2$ that breaks the CL-EUF-CMA-2 security of CLS, there exists an algorithm $\mathcal{B}_2$ that breaks the EUF-CMA security of Sig, where*

$$\mathsf{Adv}^{\textit{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda) \leq Q_{cu} \mathsf{Adv}^{\textit{euf-cma}}_{\mathsf{Sig},\mathcal{B}_2}(\lambda).$$

As shown in Proposition 2, the reduction to EUF-CMA-secure signature scheme is not tight. Thus we cannot obtain tightly-secure schemes from the above reduction. In the next section, we show the new security reduction to construct tightly-secure CLS schemes.

Oracle $\mathbf{CU}(ID)$

---

if $ID \in HU \cup CU$ **then return** $\bot$
$pk[ID] \leftarrow pk_{ctr}; ctr[ID] \leftarrow ctr$
$psk[ID] \leftarrow \mathsf{IBS.Extract}(msk, ID)$
$MSG[ID] \leftarrow \emptyset$
$HU \leftarrow HU \cup \{ID\}; ctr \leftarrow ctr + 1$
return $pk[ID]$

Oracle $\mathbf{SK}2(ID)$

---

if $ID \notin HU$ **then return** $\bot$
$CU \leftarrow CU \cup \{ID\}; HU \leftarrow HU \setminus \{ID\}$
$sk[ID] \leftarrow \mathbf{CORR}(ctr[ID])$
return $sk[ID]$

Oracle $\mathbf{PKR}(ID, pk')$

---

if $ID \notin HU \cup CU$ **then return** $\bot$
$pk[ID] \leftarrow pk', sk[ID] \leftarrow \bot$
return 1

Oracle $\mathbf{SIGN}(ID, M)$

---

if $ID \notin HU \vee sk[ID] = \bot$ **then return** $\bot$
$\sigma_1 \leftarrow \mathbf{SIGN}(M \| mpk \| ID \| pk_{ID}, ctr[ID])$
$\sigma_2 \leftarrow \mathsf{IBS.Sign}(ID, psk[ID], M \| mpk \| ID \| pk[ID] \| \sigma_1)$
$MSG[ID] \leftarrow MSG[ID] \cup \{M\}$
return (σ_1, σ_2)

Fig. 6. Oracle simulation performed by $\mathcal{B}_2$.

4 Tight reduction for the generic construction

We show that Hu et al. construction is tightly secure if the underlying signature scheme is MU-EUF-CMA$^{\mathsf{Corr}}$. Note that the security against Type-I adversary is the same as Proposition 1.

Theorem 1. *For any Type-II adversary $\mathcal{A}_2$ that breaks the CL-EUF-CMA-2 security of CLS, there exists an algorithm $\mathcal{B}_2$ that breaks the MU-EUF-CMA$^{\mathsf{Corr}}$ security of Sig, where*

$$\mathsf{Adv}^{cl\text{-}euf\text{-}cma\text{-}2}_{\mathsf{CLS},\mathcal{A}_2}(\lambda) = \mathsf{Adv}^{mu\text{-}euf\text{-}cma\text{-}corr}_{\mathsf{Sig},\mathcal{B}_2}(\lambda).$$

Proof. Let $\mathcal{A}_2$ be a PPT adversary against CLS. We construct a PPT adversary $\mathcal{B}_2$ which breaks the MU-EUF-CMA$^{\mathsf{Corr}}$ security of Sig by running $\mathcal{A}_2$.

$\mathcal{B}_2$ takes input the security parameter 1^λ and Q_{CU} public keys $pk_1, \ldots, pk_{Q_{\mathrm{CU}}}$ of Sig, where Q_{CU} is the number of $\mathbf{CU}$ queries. It has access to the corruption oracle $\mathbf{CORR}$ and signing oracle $\mathbf{SIGN}$. $\mathcal{B}_2$ generates $(msk, mpk) \leftarrow \mathsf{CLS.Setup}(1^\lambda)$ and sets $HU \leftarrow \emptyset, CU \leftarrow \emptyset, ctr \leftarrow 1$. It runs $\mathcal{A}_2$ as subroutine and answers their oracle queries as shown in Fig. 6.

$\mathcal{A}_2$ outputs $ID^*, M^*, \sigma^* = (\sigma_1^*, \sigma_2^*)$. Let ctr^* be the counter and pk_{ID^*} be the public key corresponding to ID^*. If $\mathcal{A}_2$ wins the game, $pk_{ID^*} = pk_{ctr^*}$ holds because $\mathbf{PKR}(ID^*, \cdot)$ has never been queried. Moreover, $(M^* \| mpk \| ID^* \| pk_{ID^*}, \sigma_1^*)$ is a valid signature with respect to the signature scheme Sig. In addition, $\mathbf{SK}2(ID^*)$ and $\mathbf{SIGN}(ID^*, M^*)$ has never been queried from $\mathcal{A}_2$, i.e. $ID^* \notin CU$ and $M^* \notin MSG[ID^*]$. In other words, $\mathcal{B}_2$ has never queried $\mathbf{EXT}(ctr^*)$ and $\mathbf{SIGN}(M^* \| mpk \| ID^* \| pk_{ID^*}, ctr^*)$. Therefore $(ctr^*, M^* \| mpk \| ID^* \| pk_{ID^*}, \sigma_1^*)$ is a valid forgery for Sig.

If $\mathcal{A}_2$ is successful, $\mathcal{B}_2$ is also successful. Thus we get

$$\mathsf{Adv}^{\text{cl-euf-cma-2}}_{\mathsf{CLS},\mathcal{A}_2}(\lambda) = \mathsf{Adv}^{\text{mu-euf-cma-corr}}_{\mathsf{Sig},\mathcal{B}_2}(\lambda).$$

Theorem 1 indicates that the generic construction in Fig. 5 achieves tight security if the underlying signature scheme is tightly MU-EUF-CMA$^{\mathsf{Corr}}$-security. Thus we are ready to construct a tightly-secure CLS scheme.

5 Instantiation

5.1 Tightly-secure certificateless signature scheme without pairing

We can instantiate real tightly-secure CLS schemes using the generic construction. We choose the IBS scheme of Fukumitsu and Hasegawa [FH18] as the underlying IBS scheme, which is the most efficient and tightly-secure scheme in the DDH assumption. For the underlying MU-EUF-CMA$^{\mathsf{Corr}}$-secure signature scheme, we choose the efficient scheme of Gjøsteen and Jager [GJ18] whose security is tightly reduced to the DDH assumption. Therefore, the instantiated CLS scheme also provides tight security in the DDH assumptions. As both [FH18] and [GJ18] are pairing-free, the constructed CLS scheme is also pairing-free.

5.2 Comparison

We compare the tightly-secure instantiation (Tight) with the two conventional pairing-free CLS scheme [GL14; JHL+18] and a non-tight instantiation (Non-Tight) from EUF-CMA-secure signature. To instantiate a CLS scheme from EUF-CMA-secure signature, we choose [GJK+07] as the underlying EUF-CMA-secure signature scheme, which is an efficient pairing-free and tightly-secure signature schemes in the DDH assumption.

We denote by $(\mathbb{G}, q)$ a group $\mathbb{G}$ of a prime order q. Table 1 shows the estimation of the bit length of the group element. We choose parameters that provide 128 bits security. Table 2 shows the number of elements in the secret key, public key, and signature and the actual signature size. Because both security reduction

Table 1. Evaluation of security level for each scheme and the bit length of group elements. ϵ denotes a success probability of an adversary against each scheme and we set the parameters so that $\epsilon = 2^{-256}$ for all schemes. ϵ' denotes a success probability of an algorithm that solves the underlying problem. The column "Tightness" shows the gap between ϵ and ϵ'. We assume the number of users is $\mu = 2^{50}$ and that of hash function evaluations is $h = 2^{80}$.

Scheme	Assumption	Tightness	ϵ'	$\lvert\mathbb{Z}_q\rvert$ and $\lvert\mathbb{G}\rvert$ [bits]
Gong and Li [GL14]	DL	$\epsilon \leq h\sqrt[4]{h^6\epsilon'}$	2^{-1584}	1584
Jia et al. [JHL+18]	DL	$\epsilon \leq \mu\sqrt[4]{h^6\epsilon'}$	2^{-1554}	1554
Non-Tight (IBS: [FH18] + Sig: [GJK+07])	DDH	$\epsilon \leq \mu\epsilon'$	2^{-306}	306
Tight (IBS: [FH18] + Sig:[GJ18])	DDH	$\epsilon \leq 4\epsilon'$	2^{-258}	258

Table 2. Comparison on the number of group elements and the actual signature size.

Scheme	$\|psk\| + \|sk\|$	$\|pk\|$	$\|\sigma\|$
Gong and Li [GL14]	$\|\mathbb{G} + 2\mathbb{Z}_q\|$	$\|\mathbb{G}\|$	$2\|\mathbb{G}\| + \|\mathbb{Z}_q\|$
Jia et al. [JHL+18]	$2\|\mathbb{Z}_q\|$	$2\|\mathbb{G}\|$	$\|\mathbb{G}\| + \|\mathbb{Z}_q\|$
Non-Tight (IBS: [FH18] + Sig: [GJK+07])	$2\|\mathbb{G}\| + 2\|\mathbb{Z}_q\|$	$3\|\mathbb{G}\|$	$2\|\mathbb{G}\| + 4\|\mathbb{Z}_q\|$
Tight (IBS: [FH18] + Sig:[GJ18])	$2\|\mathbb{G}\| + 2\|\mathbb{Z}_q\| + 1$	$2\|\mathbb{G}\|$	$4\|\mathbb{G}\| + 6\|\mathbb{Z}_q\| + \lambda$

Scheme	$\|psk\| + \|sk\|$ [bits]	$\|pk\|$ [bits]	$\|\sigma\|$ [bits]
Gong and Li [GL14]	4752	1584	4752
Jia et al. [JHL+18]	3108	3108	3108
Non-Tight (IBS: [FH18] + Sig: [GJK+07])	1224	918	1836
Tight (IBS: [FH18] + Sig:[GJ18])	1033	516	2708

in [GL14] and [JHL+18] is very loose, we need larger group order q. As a result, the actual signature size is very large in spite of the small number of group elements in signature. Both Non-Tight and Tight instantiation has a small order. In general, the smaller the group order, the better the computation efficiency. Comparing Tight instantiation with Non-Tight instantiation, Tight instantiation is better in key size and Non-Tight instantiation is better in signature size.

6 Conclusion

In this paper, we have improved the reduction cost for generic construction of certificateless signature proposed by Hu et al. [HWZ+07]. Using the construction, we have instantiated the first tightly-secure certificateless signature scheme without pairing.

References

[AP03] Sattam S. Al-Riyami and Kenneth G. Paterson. "Certificateless Public Key Cryptography". In: *Advances in Cryptology – ASIACRYPT 2003*. Vol. 2894. Lecture Notes in Computer Science. 2003, pp. 452–473. DOI: 10.1007/978-3-540-40061-5_29.

[BHJ+15] Christoph Bader, Dennis Hofheinz, Tibor Jager, et al. "Tightly-Secure Authenticated Key Exchange". In: *TCC 2015*. Vol. 9014. Lecture Notes in Computer Science. 2015, pp. 629–658. DOI: 10.1007/978-3-662-46494-6_26.

[BNN09] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. "Security proofs for identity-based identification and signature schemes". In: *Journal of Cryptology* 22.1 (2009), pp. 1–61. DOI: 10.1007/s00145-008-9028-8.

[FH18] M. Fukumitsu and S. Hasegawa. "A Galindo-Garcia-Like Identity-Based Signature with Tight Security Reduction, Revisited". In: *2018 Sixth International Symposium on Computing and Networking (CANDAR)*. 2018, pp. 92–98. DOI: 10.1109/CANDAR.2018.00019.

[GJ18] Kristian Gjøsteen and Tibor Jager. "Practical and Tightly-Secure Digital Signatures and Authenticated Key Exchange". In: *Advances in Cryptology – CRYPTO 2018*. Vol. 10992. Lecture Notes in Computer Science. 2018, pp. 95–125. DOI: 10.1007/978-3-319-96881-0_4.

[GJK+07] Eu-Jin Goh, Stanislaw Jarecki, Jonathan Katz, et al. "Efficient Signature Schemes with Tight Reductions to the Diffie-Hellman Problems". In: *Journal of Cryptology* 20.4 (2007), pp. 493–514. DOI: 10.1007/s00145-007-0549-3.

[GL14] Peng Gong and Ping Li. "Further improvement of a certificateless signature scheme without pairing". In: *International Journal of Communication Systems* 27.10 (2014), pp. 2083–2091. DOI: 10.1002/dac.2457.

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. "A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks". In: *SIAM Journal on Computing* 17.2 (1988), pp. 281–308. DOI: 10.1137/0217017.

[HCZ12] D. He, J. Chen, and R. Zhang. "An efficient and provably-secure certificateless signature scheme without bilinear pairings". In: *International Journal of Communication Systems* 25.11 (2012), pp. 1432–1442. DOI: 10.1002/dac.1330.

[HHC13] D. He, B. Huang, and J. Chen. "New certificateless short signature scheme". In: *IET Information Security* 7.2 (2013), pp. 113–117. DOI: 10.1049/iet-ifs.2012.0176.

[HSM+05] Xinyi Huang, Willy Susilo, Yi Mu, et al. "On the Security of Certificateless Signature Schemes from Asiacrypt 2003". In: *Proceedings of the 4th International Conference on Cryptology and Network Security*. CANS'05. 2005, pp. 13–25. DOI: 10.1007/11599371_2.

[HWZ+07] Bessie C Hu, Duncan S Wong, Zhenfeng Zhang, et al. "Certificateless signature: a new security model and an improved generic construction". In: *Designs, Codes and Cryptography* 42.2 (2007), pp. 109–126. DOI: 10.1007/s10623-006-9022-9.

[JHL+18] Xiaoying Jia, Debiao He, Qin Liu, et al. "An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment". In: *Ad Hoc Networks* 71 (2018), pp. 78–87. DOI: 10.1016/j.adhoc.2018.01.001.

[Sha84] Adi Shamir. "Identity-Based Cryptosystems and Signature Schemes". In: *Advances in Cryptology – CRYPTO 1984*. Vol. 196. Lecture Notes in Computer Science. 1984, pp. 47–53. DOI: 10.1007/3-540-39568-7_5.

[Shi19] Kyung-Ah Shim. "A New Certificateless Signature Scheme Provably Secure in the Standard Model". In: *IEEE Systems Journal* 13.2 (2019), pp. 1421–1430. DOI: 10.1109/JSYST.2018.2844809.

[TH13] Miaomiao Tian and Liusheng Huang. "Cryptanalysis of a certificateless signature scheme without pairings". In: *International Jour-*

nal of Communication Systems 26.11 (2013), pp. 1375–1381. DOI: 10.1002/dac.2310.

[YL04] Dae Hyun Yum and Pil Joong Lee. "Generic Construction of Certificateless Signature". In: *ACISP 2004*. Vol. 3108. Lecture Notes in Computer Science. 2004, pp. 200–211. DOI: 10.1007/978-3-540-27800-9_18.

[YSC+17] Kuo-Hui Yeh, Chunhua Su, Kim-Kwang Raymond Choo, et al. "A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things". In: *Sensors* 17.5 (2017). DOI: 10.3390/s17051001.

[ZWX+06] Zhenfeng Zhang, Duncan S. Wong, Jing Xu, et al. "Certificateless Public-Key Signature: Security Model and Efficient Construction". In: *ACNS 2006*. Vol. 3989. Lecture Notes in Computer Science. 2006, pp. 293–308. DOI: 10.1007/11767480_20.

[ZZ08] L. Zhang and F. Zhang. "A New Provably Secure Certificateless Signature Scheme". In: *2008 IEEE International Conference on Communications*. 2008, pp. 1685–1689. DOI: 10.1109/ICC.2008.325.