

Signature Scheme from Trapdoor Functions

Yuanhao Wang, Meiyan Xiao, Ying Miao, Wenbo Liu, and Qiong Huang*
South China Agricultural University, Guangzhou 510642, China
yuanhao.wang@stu.scau.edu.cn, maymayxiao@scau.edu.cn,
{scauym, wenboliu}@stu.scau.edu.cn, qhuang@scau.edu.cn

Abstract

Digital Signature is a basic cryptographic primitive. Security of signature scheme has been studied for decades. How to build an efficient signature scheme based on simple and standard assumptions without relying on random oracle heuristic has been an interesting problem. In this paper we provide a solution to this problem from another angle. We present a generic construction of digital signature schemes existentially unforgeable under chosen message attacks from adaptive trapdoor function, which has shown its power in building other important cryptographic primitives. Furthermore, we extend the generic construction and present a construction of secure digital signature schemes from tag-based adaptive trapdoor function. Since there are many instantiations of (tag-based) adaptive trapdoor function, our constructions could be instantiated based on simple assumptions like CDH and RSA in the standard model.

Keywords: digital signature, standard model, trapdoor function

1 Introduction

As the analogy of handwriting signatures in the digital world, digital signatures are a basic public-key cryptographic primitive which ensure the integrity of an electronic document. The party who generates signatures, usually named the signer, could not deny the source of a signature if it passes the prescribed verification algorithm. This is called *non-repudiation*, and is usually achieved by requiring that no one is able to forge a signature w.r.t. the signer's public key if it is not given the corresponding secret key.

How to build a secure signature scheme has been a hot research topic in the community. There are two ingredients to consider. The first is to define the security of signature schemes. Goldwasser et al [6] clarified the security of signature schemes into several levels. The *de facto* security definition is *existentially unforgeable under adaptive chosen message attacks* (EUF-CMA), in which the adversary is required to forge signatures on a new message after seeing many signatures on messages of its choice adaptively. The other ingredient is how to construct a scheme with EUF-CMA security. The community has put great efforts on the construction of secure signature schemes. To name a few, a well-known and efficient signature scheme is modified from Schnorr's identification scheme [15], which was proved by Pointcheval et al. [12] to be secure based on the discrete logarithm (DL) assumption in the random oracle model [1]. Boneh et al. [2] proposed another signature scheme with short signature representation, which is based on bilinear pairing and is EUF-CMA secure based on Computational Diffie-Hellman (CDH) assumption in the random oracle model. Although powerful and admitting many efficient constructions, random oracle model does not necessarily guarantee security when the random oracles are replaced with real-life hash functions [4]. Researchers have been devoted to the construction of signature schemes secure without random oracles. Remarkably, Cramer and Shoup proposed a practically efficient signature scheme based on Strong RSA assumption with EUF-CMA security in the standard model [5]. Waters

Journal of Internet Services and Information Security (JISIS), volume: 9, number: 2 (May 2019), pp. 31-41

*Corresponding author: Room 208, College of Mathematics and Informatics, South China Agricultural University, 483 Wushan Road, Guangzhou 510642, P.R. China, Tel: +86-20-85285389

proposed the first signature scheme secure based on CDH assumption without random oracles [16], which works in groups equipped with a bilinear pairing. The scheme has been widely studied and used to build other primitives, for example verifiably encrypted signature [10], multi-signature [10], aggregate signature [10] and etc. Hohenberger and Waters proposed to associate each signature with an index representing the number of signatures that the signer has issued [7], and gave two new signature schemes based on RSA assumption and CDH assumption in bilinear groups. However, the signer is stateful so that it has to remember the signature index. Soon after that, the same authors enhanced their results [8], and proposed a new method of constructing stateless signature schemes with security based on RSA and CDH assumptions in the standard model. Brakerski and Kalai described in [3] an approach to building EUF-CMA secure signature scheme from AMU-SCMA secure (cf. Def. 2.4) one, which abstracts the construction of Hohenberger and Waters [8].

(*Trapdoor Functions*). Trapdoor functions (TDF) are a special class of one-way functions, which allow the inversion of images with the knowledge of a *trapdoor*. A trapdoor function consists of three probabilistic polynomial-time algorithms. The key generation algorithm outputs a key pair of the function, an evaluation key ek and a trapdoor td . Given ek , the evaluation algorithm outputs the image y of an input x . Without td , it is infeasible to find the correct pre-image of a given y ; however, it is easy to do so if given the knowledge of td . The first trapdoor in the literature was due to Rivest et al. [13]. Trapdoor functions are an important cryptographic tool, and have played a central role in the construction of cryptographic primitives, especially for secure public key cryptosystems. For example, Peikert and Waters introduced a variant of trapdoor functions, called *lossy* trapdoor functions (lossy TDF) [11], and showed its power in the construction of chosen-ciphertext secure (CCA secure) public key encryption schemes. Their construction, different from the non-interactive zero-knowledge (NIZK) proof approach, is very efficient and its security is solely based on that of the underlying lossy TDF and *all-but-one* TDF (ABO-TDF, a variant of lossy TDF) [11]. It has been shown that lossy TDF can be constructed based on various number-theoretic assumptions, for example, Decisional Diffie-Hellman assumption (DDH), Decisional Composite Residuosity assumption (DCR), Learning With Error assumption (LWE) and etc. Rosen and Segev weakened the requirement on trapdoor functions, and proposed a black-box construction of public key encryption from a new notion called *correlated product* TDF (CP-TDF). They also showed that CP-TDF is a potentially weaker primitive than lossy TDF.

1.1 Our Work

In this paper we provide a new construction of digital signature schemes. We show how to build a EUF-CMA secure signature scheme from adaptive trapdoor function by presenting generic transforms step by step. First we give a construction of AMU-CMA secure (Def. 2.4) signature from adaptive one-way TDF (Def. 2.5). Then we show how to transform AMU-CMA security to SMU-CMA security. We complete the construction of EUF-CMA secure signature by giving a transform from SMU-CMA security to EUF-CMA security, which makes use of a one-time signature. As an extension of our transform, we show how to build a EUF-CMA secure signature scheme from tag-based trapdoor functions.

Since adaptive trapdoor functions could be instantiated based on various number-theoretic assumptions, as well as the underlying one-time signature, in turn we can obtain EUF-CMA secure signatures based on these assumptions as well by applying our transform.

1.2 Paper Organization

In Sec. 2 we review some basic notions of digital signature and trapdoor functions. We provide the generic constructions of EUF-CMA secure signature schemes from adaptive trapdoor functions and tag-based adaptive trapdoor functions in Sec. 3 and Sec. 4, respectively. Finally we conclude the paper in

Sec. 6.

2 Backgrounds

2.1 Digital Signature

Definition 2.1 (Signature). *A digital signature scheme consists of the following (probabilistic) polynomial-time algorithms.*

- **Kg**: On input 1^k , output a public/private key pair (Pk, Sk) .
- **Sig**: On input Sk and a message $m \in \mathcal{M}$ to be signed, output a signature σ .
- **Ver**: On input Pk , $m \in \mathcal{M}$ and σ , output 1 if σ is a valid signature on m under Pk , and 0 otherwise.

Security of Signature Scheme: The *de facto* security requirement of a signature scheme is *existential unforgeability under chosen-message attacks* (EUF-CMA for short). For any probabilistic polynomial-time algorithm \mathcal{A} , consider its advantage defined as below:

$$\text{Adv}_{\mathcal{A}}^{\text{euf-cma}}(k) \stackrel{\text{def}}{=} \Pr[\text{Ver}(\text{Pk}, m^*, \sigma^*) = 1 \wedge m^* \notin \mathcal{Q} \mid (\text{Pk}, \text{Sk}) \leftarrow \text{Kg}(1^k); (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathcal{O}(\text{Sk})}(\text{Pk})],$$

where $\mathcal{O}(\text{Sk})$ is the signing oracle which takes as input a message m and outputs $\sigma \leftarrow \text{Sig}(\text{Sk}, m)$, and \mathcal{Q} is the set of messages that \mathcal{A} issued to $\mathcal{O}(\text{Sk})$.

Definition 2.2 (EUF-CMA Security). *A signature scheme is EUF-CMA secure if for any probabilistic polynomial-time adversary \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{\text{euf-cma}}(k)$ is negligible.*

A weak variant of EUF-CMA security is called *selective-message unforgeability under chosen-message attacks* (SMU-CMA for short). For any probabilistic polynomial-time algorithm $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, consider its advantage defined as below:

$$\text{Adv}_{\mathcal{A}}^{\text{smu-cma}}(k) \stackrel{\text{def}}{=} \Pr[\text{Ver}(\text{Pk}, m^*, \sigma^*) = 1 \wedge m^* \notin \mathcal{Q} \mid (m^*, st) \leftarrow \mathcal{A}_1(1^k); (\text{Pk}, \text{Sk}) \leftarrow \text{Kg}(1^k); \sigma^* \leftarrow \mathcal{A}_2^{\mathcal{O}(\text{Sk})}(\text{Pk}, st)],$$

where st is the state of \mathcal{A} .

Definition 2.3 (SMU-CMA Security). *A signature scheme is SMU-CMA secure if for any probabilistic polynomial-time adversary \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{\text{smu-cma}}(k)$ is negligible.*

Another even weaker but still useful security definition is *a-priori-message unforgeability under chosen-message attacks* (AMU-CMA for short). For any probabilistic polynomial-time algorithm \mathcal{A} , consider its advantage defined as below:

$$\text{Adv}_{\mathcal{A}}^{\text{amu-cma}}(k) \stackrel{\text{def}}{=} \Pr[\text{Ver}(\text{Pk}, m^*, \sigma^*) = 1 \wedge m^* \notin \mathcal{Q} \mid m^* \leftarrow \mathcal{M}; (\text{Pk}, \text{Sk}) \leftarrow \text{Kg}(1^k); \sigma^* \leftarrow \mathcal{A}^{\mathcal{O}(\text{Sk})}(\text{Pk}, m^*)].$$

Definition 2.4 (AMU-CMA Security). *A signature scheme is AMU-CMA secure if for any probabilistic polynomial-time adversary \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{\text{amu-cma}}(k)$ is negligible.*

2.2 Adaptive Trapdoor Functions

Recall that a *trapdoor function* (TDF) is a triple of (probabilistic) polynomial-time algorithms, where Tdg takes as input 1^k and generates an evaluation/trapdoor key pair $(ek, td) \leftarrow \text{Tdg}(1^k)$, $F(ek, \cdot)$ implements a function $f_{ek}(\cdot)$ over $\{0, 1\}^k$ and $F^{-1}(td, \cdot)$ implements its inverse $f_{ek}^{-1}(\cdot)$. We require TDFs to be injective. Briefly, a TDF is *adaptive* if it remains one-way after revealing the pre-images of points chosen by the adversary adaptively. Let \mathcal{A} be any probabilistic polynomial-time inverter. Consider its advantage defined as below:

$$\text{Adv}_{\mathcal{A}}^{\text{aow}}(k) \stackrel{\text{def}}{=} \Pr[x' = x \mid (ek, td) \leftarrow \text{Tdg}(1^k); x \leftarrow \{0, 1\}^k; y \leftarrow F(ek, x); x' \leftarrow \mathcal{A}^{F^{-1}(td, \cdot)}(ek, y)],$$

where \mathcal{A} is prohibited from querying y to $F^{-1}(td, \cdot)$.

Definition 2.5 (Adaptive One-wayness [9]). *A TDF is adaptive one-way if for any probabilistic polynomial-time adversary \mathcal{A} , $\text{Adv}_{\mathcal{A}}^{\text{aow}}(k)$ is negligible.*

A TDF with adaptive one-wayness is called *Adaptive Trapdoor Function* (ATDF).

We also consider *tag-based* trapdoor function. Let $\text{TDF}_{\text{tag}} = (\text{Tdg}_{\text{tag}}, F_{\text{tag}}, F_{\text{tag}}^{-1})$ be a tag-based TDF with associated tag space $\text{TagSp}(k)$, where Tdg_{tag} is probabilistic and on input 1^k generates an evaluation/trapdoor key pair $(ek, td) \leftarrow \text{Tdg}_{\text{tag}}(1^k)$. Besides, for every $t \in \text{TagSp}(k)$, $F_{\text{tag}}(ek, t, \cdot)$ implements a function $f_{ek,t}(\cdot)$ over $\{0, 1\}^k$ and $F_{\text{tag}}^{-1}(td, t, \cdot)$ implements its inverse $f_{td,t}^{-1}(\cdot)$.

Definition 2.6 (Tag-based Adaptive One-wayness [9]). *A tag-based TDF is tag-based adaptively one-way if for any probabilistic polynomial-time adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, its advantage defined as below is negligible:*

$$\text{Adv}_{\mathcal{A}}^{\text{tb-aow}}(k) \stackrel{\text{def}}{=} \Pr \left[x' = x \mid \begin{array}{l} t \leftarrow \mathcal{A}_1(1^k); (ek, td) \leftarrow \text{Tdg}_{\text{tag}}(1^k); x \leftarrow \{0, 1\}^k \\ y \leftarrow F_{\text{tag}}(ek, t, x); x' \leftarrow \mathcal{A}_2^{F_{\text{tag}}^{-1}(td, \cdot, \cdot)}(ek, t, y) \end{array} \right],$$

where \mathcal{A} is prohibited from querying y to $F_{\text{tag}}^{-1}(td, \cdot, \cdot)$.

3 Signature Scheme from Adaptive Trapdoor Functions

3.1 A Warmup

As a warmup, let us consider the following construction. Let $\{0, 1\}^k$ be the message space to be signed and $\text{TDF} = (\text{Tdg}, F, F^{-1})$ be an adaptive trapdoor function over $\{0, 1\}^k$. The signature scheme works as below.

Key Generation: On input 1^k , run $(ek, td) \leftarrow \text{Tdg}(1^k)$. Set $\text{Pk} := ek$ and $\text{Sk} := td$. Return (Pk, Sk) .

Signing: On input $\text{Sk} = td$ and $m \in \{0, 1\}^k$, return $\sigma \leftarrow F^{-1}(td, m)$.

Verification: On input $\text{Pk} = ek$, $m \in \{0, 1\}^k$ and $\sigma \in \{0, 1\}^k$, check if

$$F(ek, \sigma) = m. \tag{1}$$

Output 1 if the equation holds, and 0 otherwise.

Observe that the definition of adaptive one-wayness of TDF (w.r.t. Definition 2.5) shares a close similarity with that of AMU-CMA security (w.r.t. Definition 2.4) of signature schemes. Therefore, we have the following theorem directly.

Theorem 3.1. *If TDF is adaptive one-way, the signature scheme above is AMU-CMA secure.*

The signature scheme supports to sign messages of fixed-length. To extend the message space to include arbitrarily long strings, one may consider to make use of a collision-resistant hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^k$, and modify the scheme by replacing every occurrence of message m with its hash $H(m)$. Indeed, this is the common practice in the design of signature schemes. However, in contrary to signature schemes with standard EUF-CMA security, the well-known ‘hash-then-sign’ paradigm does *not* work for signature schemes with AMU-CMA security, i.e. we could not prove the resulting scheme to be AMU-CMA secure. The difficulty is in that after receiving the target image y (as well as the evaluation key ek), we do not know how to connect it with some ‘known’ message m^* (that will be given to the forger) so that $H(m^*) = y$, except by modeling H as a random oracle, by which we cannot achieve the desired objective of this work.

Hence, in the following, we overcome the difficulty and propose a new signature scheme based on TDF, which supports to sign arbitrarily long messages. We show its SMU-CMA (instead of AMU-CMA) security if the given TDF is adaptive one-way.

3.2 The Basic Scheme: an Efficient Method to Achieve SMU-CMA Security from TDF

To overcome the difficulty aforementioned, we choose to separate the image y (to be inverted under F) into two parts. One is the hash of message m and the other is another image α which is set as part of the public key. Every signature is set to be the inversion of the combination of the message’s hash and α . After receiving the target image y^* , we can connect it with the challenge message m^* by setting $\alpha := y^* \oplus H(m^*)$ and adding α to the public key. Formally, our signature scheme works as follows.

Let $TDF = (Tdg, F, F^{-1})$ be an adaptive trapdoor function over $\{0, 1\}^k$, and $H : \{0, 1\}^* \rightarrow \{0, 1\}^k$ be a collision-resistant hash function. We construct a signature scheme $SIG = (Kg, Sig, Ver)$ from TDF as follows.

Key Generation: On input 1^k , run $(ek, td) \leftarrow Tdg(1^k)$ and select at random $\alpha \leftarrow \{0, 1\}^k$. Set $Pk := (ek, \alpha)$ and $Sk := td$. Return (Pk, Sk) .

Signing: On input $Sk = td$ and $m \in \{0, 1\}^*$, compute $\sigma \leftarrow F^{-1}(td, H(m) \oplus \alpha)$.

Verification: On input $Pk = (ek, \alpha)$, $m \in \{0, 1\}^*$ and $\sigma \in \{0, 1\}^k$, check if

$$F(ek, \sigma) = H(m) \oplus \alpha. \quad (2)$$

Output 1 if the equation holds, and 0 otherwise.

Immediately, we have the following theorem.

Theorem 3.2. *If TDF is adaptive one-way and H is collision-resistant, the signature scheme SIG constructed above is SMU-CMA secure.*

Proof. Let G_0 be the original SMU-CMA security game as defined in Def. 2.4. We first modify G_0 so that if there exists any two message m, m' during the game satisfying that $H(m) = H(m')$, the game aborts. Denote by G_1 the new game, and by $\text{Adv}_{\mathcal{A}, i}^{\text{smu-cma}}(k)$ the advantage of an adversary \mathcal{A} in game G_i . Obviously, we have the following claim:

Claim 3.3. *If H is collision-resistant, $\text{Adv}_{\mathcal{A}, 0}^{\text{smu-cma}}(k) - \text{Adv}_{\mathcal{A}, 1}^{\text{smu-cma}}(k)$ is negligible in k .*

Next we consider the adversary's advantage in game G_1 . Let \mathcal{F} be an SMU-CMA adversary against SIG under game G_1 , in which we omit the case where the game aborts. We build another algorithm \mathcal{A} to break the adaptive one-wayness of TDF.

Given (ek, y) from its challenger, \mathcal{A} invokes \mathcal{F} on input 1^k and obtains a message m^* on which \mathcal{F} intends to forge a signature. It then sets $\alpha \leftarrow \mathbb{H}(m^*) \oplus y$, and invokes \mathcal{F} on input $\text{Pk} := (ek, \alpha)$. Note that α looks uniform to \mathcal{F} due to the randomness of y .

After receiving a signing query m_i from \mathcal{F} , \mathcal{A} computes $m'_i \leftarrow \mathbb{H}(m_i) \oplus \alpha$, sends m'_i to its inversion oracle and obtains the inversion x_i so that

$$F(ek, x_i) = m'_i.$$

\mathcal{A} then returns $\sigma_i := x_i$ as the signature on m_i to \mathcal{F} .

Finally, \mathcal{F} outputs its forgery σ^* on m^* w.r.t. Pk . We have that

$$F(ek, \sigma^*) = \mathbb{H}(m^*) \oplus \alpha = \mathbb{H}(m^*) \oplus (\mathbb{H}(m^*) \oplus y) = y.$$

\mathcal{A} simply outputs σ^* , which is a correct inversion of y as long as the forgery of \mathcal{F} is valid. \square

Remark. One may observe that the definition of adaptive one-way security of TDF shares a close similarity with that of SMU-CMA security of signature schemes, and would consider a simpler variant of our proposal above, in which a signature on m is simply the inversion of $\mathbb{H}(m)$ under F . It seems that if the TDF is adaptive one-way, the resulting signature scheme would be AMU-CMA (not SMU-CMA) secure. However, we could not make a formal proof. The difficulty is in that after receiving the target image y (and the evaluation key ek), we do not have a way to connect it with some 'known' message m^* so that $\mathbb{H}(m^*) = y$, except by modeling \mathbb{H} as a random oracle.

3.3 From SMU-CMA Security to EUF-CMA Security

In this part we give a transform that given a signature scheme $S = (\text{Kg}, \text{Sig}, \text{Ver})$ that is SMU-CMA secure and has message space $\{0, 1\}^{\leq \ell}$, produces a scheme $S' = (\text{Kg}', \text{Sig}', \text{Ver}')$ that is EUF-CMA secure. Let $\text{OTS} = (\text{Kg}, \text{Sig}, \text{Ver})$ be a one-time signature scheme with space of verification key being $\{0, 1\}^\ell$. The transform works as follows.

- $\text{Kg}'(1^k)$. Run $(\text{Pk}, \text{Sk}) \leftarrow S.\text{Kg}(1^k)$. Return $(\text{Pk}', \text{Sk}') := (\text{Pk}, \text{Sk})$.
- $\text{Sig}'(\text{Sk}', m)$. Recall that $\text{Sk}' = \text{Sk}$. Generate a one-time key pair $(\text{otvk}, \text{otsk}) \leftarrow \text{OTS}.\text{Kg}(1^k)$. Then for $1 \leq i \leq \ell$, compute $\sigma_i \leftarrow S.\text{Sig}(\text{Sk}, \text{otvk}_{\leq i})$. Finally compute $\delta \leftarrow \text{OTS}.\text{Sig}(\text{otsk}, m)$. Return $\sigma' = (\{\sigma_i\}_{i=1}^\ell, \delta, \text{otvk})$.
- $\text{Ver}'(\text{Pk}', m, \sigma')$. Recall that $\text{Pk}' = \text{Pk}$ and $\sigma' = (\{\sigma_i\}_{i=1}^\ell, \delta, \text{otvk})$. Output 1 if for all $1 \leq i \leq \ell$, $S.\text{Ver}(\text{Pk}, \text{otvk}_{\leq i}, \sigma_i)$ outputs 1 and $\text{OTS}.\text{Ver}(\text{otvk}, m, \delta)$ outputs 1 as well. Otherwise, output 0.

Theorem 3.4. *If the underlying signature scheme S is SMU-CMA secure and OTS is one-time secure, the resulting scheme S' is EUF-CMA secure.*

Proof. Let G_0 be the original EUF-CMA security game as defined in Def. 2.4. Let $\sigma^* = (\{\sigma_i^*\}_{i=1}^\ell, \delta^*, \text{otvk}^*)$ be the signature output by the adversary, and $\sigma'^{(j)} = (\{\sigma_i^{(j)}\}_{i=1}^\ell, \delta^{(j)}, \text{otvk}^{(j)})$ be the answer to the adversary's j -th signing query $m^{(j)}$.

We first modify G_0 so that if there exists some $1 \leq i \leq q$ (where q is the number of signing queries issued by the adversary), $\text{otvk}^* = \text{otvk}^{(j)}$, the game aborts. Denote by G_1 the new game, and by $\text{Adv}_{\mathcal{A}, i}^{\text{euf-cma}}(k)$ the advantage of an adversary \mathcal{A} in game G_i . Via a standard argument we have that

Claim 3.5. *If OTS is one-time secure, $\text{Adv}_{\mathcal{A},0}^{\text{euf-cma}}(k) - \text{Adv}_{\mathcal{A},1}^{\text{euf-cma}}(k)$ is negligible in k .*

Next we consider the adversary's advantage in game G_1 , in which we omit for simplicity the case where G_1 aborts. Let \mathcal{F}' be an EUF-CMA adversary against S' under G_1 . We construct another algorithm \mathcal{F} to break the SMU-CMA security of S . It works as below.

First of all, \mathcal{F} generates q key pairs for the one-time signature scheme, denoted by $(\text{otvk}^{(j)}, \text{otsk}^{(j)})$ for $1 \leq i \leq q$, which will be used to answer the q signing queries submitted by \mathcal{F}' . It then samples at random $(i^*, j^*) \leftarrow [\ell] \times [q]$ and sets $\hat{m}^* \leftarrow \text{otvk}_{\leq i^*}^{(j^*)} \oplus e_{i^*}$, where $e_{i^*} = 0^{i^*-1}1$. \mathcal{F} sends \hat{m}^* to its challenger as the selective message to be forged in the SMU-CMA game.

After receiving the j -th signing query $m^{(j)}$, \mathcal{F} sends $\text{otvk}_{\leq 1}^{(j)}, \dots, \text{otvk}_{\leq \ell}^{(j)}$ to its signing oracle for signatures, and is returned $\sigma_1^{(j)}, \dots, \sigma_\ell^{(j)}$. It then computes $\delta^{(j)} \leftarrow \text{OTS.Sig}(\text{otsk}^{(j)}, m^{(j)})$, and returns $\sigma'^{(j)} := (\{\sigma_i^{(j)}\}_{i=1}^\ell, \delta^{(j)}, \text{otvk}^{(j)})$ to \mathcal{F}' . It is readily seen that the returned signature is identically distributed as in a real attack.

Finally, \mathcal{F}' outputs its forgery $(m^*, \sigma^*) = (m^*, (\{\sigma_i^*\}_{i=1}^\ell, \delta^*, \text{otvk}^*))$. \mathcal{F} returns $\hat{\sigma}^* := \sigma_{i^*}^*$ as its forgery on the selective message \hat{m}^* . Suppose that \mathcal{F}' is successful in forging. We have that

$$\forall 1 \leq i \leq \ell, \quad S.\text{Ver}(\text{Pk}, \text{otvk}_{\leq i}^*, \sigma_i^*) = 1, \text{ and } \text{OTS.Ver}(\text{otvk}^*, m^*, \delta^*) = 1.$$

Since $\text{otvk}^* \notin \{\text{otvk}_{\leq j}^{(j)}\}_{j \in [q]}$, there must exist an $i' \in [\ell]$ such that

$$\text{otvk}_{\leq i'-1}^* \in \{\text{otvk}_{\leq i'-1}^{(j)}\}_{j \in [q]} \text{ but } \text{otvk}_{\leq i'}^* \notin \{\text{otvk}_{\leq i'}^{(j)}\}_{j \in [q]}.$$

As the pair (i^*, j^*) was selected at random and the view of \mathcal{F}' is independent of the pair, it holds that

$$\Pr \left[(i^* = i') \wedge (\text{otvk}_{\leq i'-1}^* = \text{otvk}_{\leq i'-1}^{(j^*)}) \right] \geq \frac{1}{\ell q}.$$

Suppose it is indeed the case where $i^* = i'$ and $\text{otvk}_{\leq i'-1}^* = \text{otvk}_{\leq i'-1}^{(j^*)}$. Since $\text{otvk}_{\leq i^*}^* \neq \text{otvk}_{\leq i^*}^{(j^*)}$, we have

$$\text{otvk}_{\leq i^*}^* = \text{otvk}_{\leq i^*}^{(j^*)} \oplus e_{i^*} = \hat{m}^*.$$

That is, $\text{otvk}_{\leq i^*}^*$ is the selective message that \mathcal{F} was committed to at the onset of the game. As shown above, the signature $\hat{\sigma}^*$ output by \mathcal{F} could pass the verification of \mathcal{S} . Namely, it holds that

$$S.\text{Ver}(\text{Pk}, \hat{m}^*, \hat{\sigma}^*) = 1.$$

Furthermore, the fact that $\text{otvk}_{\leq i^*}^* \notin \{\text{otvk}_{\leq i}^{(j)}\}_{j \in [q]}$ means that $\hat{m}^* \notin \{\text{otvk}_{\leq i}^{(j)}\}_{(i,j) \in [\ell] \times [q]}$. That is, \mathcal{F} did not ask its signing oracle for a signature on \hat{m}^* . Therefore, \mathcal{F} wins the SMU-CMA game. \square

Remark. Brakerski et al.'s construction [3] goes in three steps. First, they obtain SMU-SCMA security from AMU-SCMA security, then obtain EUF-SCMA security from SMU-SCMA security, and finally obtain EUF-CMA security from EUF-SCMA security. While in this work we first show how to build a SMU-CMA secure signature scheme from adaptive trapdoor functions, in which the adversary could issue signing queries adaptively instead of statically, and then show how to transform SMU-CMA security to EUF-CMA security.

4 Signature from Tag-based Adaptive Trapdoor Functions

Let $\text{TDF}_{\text{tag}} = (\text{Tdg}_{\text{tag}}, F_{\text{tag}}, F_{\text{tag}}^{-1})$ be a tag-based TDF with associated tag space $\text{TagSp}(k)$ and range $\text{Range}(F_{\text{tag}})$. We construct a signature scheme $\text{SIG} = (\text{Kg}, \text{Sig}, \text{Ver})$ from TDF_{tag} as follows.

Key Generation: On input 1^k , run $(ek, td) \leftarrow \text{Tdg}_{\text{tag}}(1^k)$ and select a collision-resistant hash function $H : \{0, 1\}^* \rightarrow \text{TagSp}(k)$. Select at random $y \leftarrow \text{Range}(F_{\text{tag}})$ and set $\text{Pk} := (ek, y, H)$ and $\text{Sk} := td$. Return (Pk, Sk) .

Signing: On input $\text{Sk} = td$ and $m \in \{0, 1\}^*$, compute $t \leftarrow H(m)$ and $x \leftarrow F_{\text{tag}}^{-1}(td, t, y)$. Return $\sigma = x$.

Verification: On input $\text{Pk} = (ek, y, H)$, $m \in \{0, 1\}^*$ and $\sigma = x$, compute $t \leftarrow H(m)$ and check if

$$F_{\text{tag}}(ek, t, x) = y. \quad (3)$$

Output 1 if the equation holds, and 0 otherwise.

Theorem 4.1. *If TDF_{tag} is tag-based adaptive one-way and H is collision-resistant, the resulting signature scheme above is SMU-CMA secure.*

Proof. Let G_0 be the original SMU-CMA security game as defined in Def. 2.4. We first modify G_0 so that if there exists any two message m, m' during the game satisfying that $H(m) = H(m')$, the game aborts. Denote by G_1 the new game, and by $\text{Adv}_{\mathcal{A}, i}^{\text{smu-cma}}(k)$ the advantage of an adversary \mathcal{A} in game G_i . Obviously, we have the following claim:

Claim 4.2. *If H is collision-resistant, $\text{Adv}_{\mathcal{A}, 0}^{\text{smu-cma}}(k) - \text{Adv}_{\mathcal{A}, 1}^{\text{smu-cma}}(k)$ is negligible in k .*

Next we consider the adversary's advantage in game G_1 . Let \mathcal{F} be an SMU-CMA adversary against SIG under game G_1 , in which we omit the case where the game aborts. We build another algorithm \mathcal{A} to break the tag-based adaptive one-wayness of TDF_{tag} .

Given the input 1^k , \mathcal{A} invokes \mathcal{F} on input 1^k and obtains m^* from \mathcal{F} . It then sets $t^* \leftarrow H(m^*)$ and submits t^* to its own challenger. After receiving (ek, y) from the challenger, \mathcal{A} sets $\text{Pk} := (ek, y)$, and gives it to the adversary.

After receiving the j -th signing query m_j , \mathcal{A} computes $t_j \leftarrow H(m_j)$, sends (t_j, y) to its inversion oracle, and obtains the pre-image x_j so that

$$F_{\text{tag}}(ek, t_j, x_j) = y.$$

\mathcal{A} returns $\sigma_j := x_j$ to the adversary.

Finally, \mathcal{F} outputs its forgery σ^* on message m^* . \mathcal{A} simply outputs $x^* := \sigma^*$ as the inversion of y under the selective tag t^* . Suppose that \mathcal{F} succeeds in the SMU-CMA game. We have that

$$F_{\text{tag}}(ek, t^*, x^*) = y^*,$$

which means that x^* is the correct inversion. Furthermore, \mathcal{F} did not ask for a signature on m^* , nor did \mathcal{A} ask the inversion of y under the tag t^* . Therefore, \mathcal{A} wins in the tag-based adaptive one-wayness game. \square

Full Security. The signature scheme above is SMU-CMA secure. To obtain the standard EUF-CMA security, we could apply the transform presented in Sec. 3.3.

5 Discussions

Kiltz et al. [9] showed that adaptive trapdoor functions can be constructed from correlated-product trapdoor functions [14], which in turn can be constructed from lossy trapdoor functions [11]. There are many concrete and efficient constructions of lossy trapdoor functions, based on DDH, DCR and SIS assumptions, respectively. Furthermore, as demonstrated in [9], tag-based trapdoor functions could be constructed from *instance-independent RSA assumption*. Therefore, we could obtain signature schemes based on a bunch of simple assumptions without random oracles, which enriches the research of secure digital signatures from another angle.

On the other hand, Kiltz et al. showed the power of adaptive trapdoor function in the construction of CCA-secure public key encryption schemes [9], while we showed its usage in constructing existentially unforgeable digital signature schemes, further demonstrating the power of adaptive trapdoor functions.

6 Conclusion

In this paper we provided another solution to the construction of EUF-CMA secure digital signature schemes in the standard model. We present a generic transform from SMU-CMA secure signature scheme to EUF-CMA secure one without resorting to the random oracle model, which makes use of one-time signature and the ‘prefix’ method. As an extension of the transform, we also showed how to build a EUF-CMA secure signature scheme from tag-based adaptive trapdoor functions. Our construction is generic so that it can be instantiated based on various number-theoretic assumptions, for example, RSA assumption, CDH assumption and etc.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61872152, 61472146).

References

- [1] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. of the 1st ACM Conference on Computer and Communications Security (CCS'93)*, Fairfax, Virginia, USA, pages 62–73. ACM, November 1993.
- [2] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *Journal of Cryptology*, 17(4):297–319, September 2004.
- [3] Z. Brakerski and Y. T. Kalai. A framework for efficient signatures, ring signatures and identity based encryption in the standard model. *IACR Cryptology ePrint Archive*, 2010:86, 2010.
- [4] R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *Proc. of the 30th Annual ACM Symposium on the Theory of Computing (STOC'98)*, Dallas, Texas, USA, pages 209–218. ACM, May 1998.
- [5] R. Cramer and V. Shoup. Signature schemes based on the strong rsa assumption. In *Proc. of the 6th ACM Conference on Computer and Communications Security (CCS'99)*, Singapore, pages 46–51. ACM, November 1999.
- [6] S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attack. *SIAM Journal on Computing*, 17(2):281–308, 1988.
- [7] S. Hohenberger and B. Waters. Realizing hash-and-sign signatures under standard assumptions. In *Proc. of the 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'09)*, Cologne, Germany, volume 5479 of *Lecture Notes in Computer Science*, pages 333–350. Springer, April 2009.

- [8] S. Hohenberger and B. Waters. Short and stateless signatures from the RSA assumption. In *Proc. of the 29th Annual International Cryptology Conference (CRYPTO'09), Santa Barbara, California, USA*, volume 5677 of *Lecture Notes in Computer Science*, pages 654–670. Springer, August 2009.
 - [9] E. Kiltz, P. Mohassel, and A. O’Neill. Adaptive trapdoor functions and chosen-ciphertext security. In *Proc. of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'10), Monaco / French Riviera*, volume 6110 of *Lecture Notes in Computer Science*, pages 673–692. Springer, May-June 2010.
 - [10] S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In *Proc. of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'06), St. Petersburg, Russia*, volume 4004 of *Lecture Notes in Computer Science*, pages 465–485. Springer, May-June 2006.
 - [11] C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *Proc. of the 40th Annual ACM Symposium on Theory of Computing (STOC'08), Victoria, British Columbia, Canada*, pages 187–196. ACM, May 2008.
 - [12] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptology*, 13(3):361–396, 2000.
 - [13] R. Rivest, A. Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of ACM*, 21(2):120–126, 1978.
 - [14] A. Rosen and G. Segev. Chosen-ciphertext security via correlated products. In *Proc. of the 6th Theory of Cryptography Conference (TCC'09), San Francisco, CA, USA*, volume 5444 of *Lecture Notes in Computer Science*, pages 419–436. Springer, March 2009.
 - [15] C. Schnorr. Efficient signature generation by smart cards. *J. Cryptology*, 4(3):161–174, 1991.
 - [16] B. Waters. Efficient identity-based encryption without random oracles. In *Proc. of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'05), Aarhus, Denmark*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, May 2005.
-

Author Biography



Yuanhao Wang received the B.S. degree in Network Engineering from South China Agricultural University in 2017. He is currently pursuing the M.S. degree at College of Mathematics and Informatics, South China Agricultural University. His research interests include information security, digital signature and searchable encryption.



Meiyan Xiao received her master’s degree from South China Agricultural University, Guangzhou, China, in 2009. Currently, she is a teacher and also a PhD student at College of Mathematics and Informatics, South China Agricultural University. Her research interests include cyberspace security, public key cryptography and blockchain security.



Ying Miao received her B.S. degree in Network Engineering from South China Agricultural University in 2018. Currently, she is a master student at College of Mathematics and Informatics, South China Agricultural University. Her research interests include cryptography and blockchain.



Wenbo Liu received the B.S. degree from College of Computer Science and Engineering, Cangzhou Normal University in 2018. Currently, he is a M.S. degree student at College of Mathematics and Informatics, South China Agricultural University. His research interests include public key encryption and functional encryption.



Qiong Huang got his PhD degree from City University of Hong Kong in 2010. Now he is a professor at South China Agricultural University. His research interests include cryptography and information security, in particular, cryptographic protocols design and analysis.