Tight Proofs of Identity-based Signatures without Random Oracle

Huiyan Chen[1], Yanshuo Zhang[1], Zongjie Wan[1], Chenchen Zhang[1,2]
(Corresponding author: Huiyan Chen)

Beijing Electronic Science and Technology Institute[1]
No. 7, Fufeng road, Fengtai district, Beijing 100070, China
Xidian University, Xi'an 710126, China[2]
(Email: chenhy03@126.com)

(Received Nov. 10, 2017; revised and accepted May 5, 2018)

Abstract

It is a very desirable property of an identity-based signature to have a tight security reduction. According to our known knowledge, there are few results on designing identity-based signature schemes with tight security reduction. Inspired by the work of David Galindo *et al.* [13] and based on the signatures proposed by Sven Schäge [36, 37], we construct identity-based signatures which are existentially unforgeable under adaptively chosen message and identity attacks and whose security is also tightly related to Strong Diffie-Hellman assumption in the standard model.

Keywords: Existential Unforgeability; Identity-based Signature; q-Strong Diffie-Hellman Problem; Standard Model

1 Introduction

One focus of modern cryptography has been the construction of identity-based signature scheme that can be rigorously proven secure based on specific computational assumptions.

A number of identity-based signature (IBS) schemes [7–9, 16, 17, 21, 26, 28, 30, 32, 34, 40–43] have been devised since the concept of identity-based cryptography was proposed by Shamir [39] in 1984. At present, there are two known generic constructions of IBS. The first is due to Bellare *et al.* [29]. They show that a large number of previously proposed schemes are instances of their generic construction. The other generic construction is due to Kurosawa and Heng [15]. The construction of Kurosawa and Heng requires an efficient zero-knowledge protocol for proof of knowledge of a signature, which makes their construction applicable to only a few schemes such as RSA-FDH and BLS [22].

1.1 Our Contribution

In this work, we ask the following question: how does one construct identity-based signature with tight security proof in the standard model? The security of an IBS scheme is generally confirmed by a security proof which typically describes a reduction from some hard computational problem to breaking a defined security property of the IBS scheme. The reduction for the IBS scheme is considered as tight when this success probability of an adversary breaking the IBS is roughly equal to the probability of solving the underlying hard problem in roughly the same amount of time. Tightness of security reduction gives explicit bound on the probability that adversary successfully forges a signature for an IBS scheme as a function of its expended resources, and affects the efficiency of the IBS scheme when instantiated in practice: A tighter reduction allows to securely use smaller parameters, *e.g.*, shorter moduli, a smaller group size. Therefore it is a very desirable property of an IBS to have a tight security reduction. According to our known knowledge, there are few results on designing IBS schemes with tight security reductions. In this paper, we study the problem above and our work stems from the results of Sven Schäge [36, 37] and Galindo *et al.* [13]. In [36, 37], Schäge presented combing function based signature and chameleon hash function based signature which are strongly existential unforgeability under adaptively chosen message attack in standard model and which have tight security proof. In [13], Galindo *et al.* gave a Schnorr-like identity-based signature which is existentially unforgeable under adaptively chosen message and identity attack in random oracle model. Galindo *et al.*'s work is different from that of Bellare *et al.* [29], is also different from that of Kurosawa and Heng [15]. Inspired by the work of Galindo *et al.*, we construct four identity-based schemes with tight security reduction from combing function based signature and chameleon hash function based signature [36,37]. According to the type of parings used in our four schemes, we have divided them into two types and denoted them as

TYPE I and TYPE II, respectively. TYPE I is based the fact that there is efficiently computable homomorphism on the bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$, and TYPE II is just the opposite. According to the efficiency and the security, we compare our IBS scheme with the known IBS schemes in Table 1.

1.2 Related Works

It is a very desirable property of an IBS scheme to have a tight security reduction. Therefore, providing new security proofs for cryptosystems that were already well known to be secure in the random oracle model or for some of their variants (*e.g.*, [2, 3, 10, 11, 27, 36, 37]) and constructing new schemes (*e.g.*, [5, 6, 14, 18, 19, 23–25]) that provide tight security reductions have been a new research focus in in the area of provable security. In addition, to verify whether there is a tight security proof for the Schnorr signature scheme, cryptographers have given considerable research efforts, *e.g.*, [4, 31, 38].

However, the research on tight security reduction for IBS schemes has made little progress. In fact, Hess and Barreto *et al.* gave proofs under the Diffie-Hellman assumption for their respective scheme through Pointcheval and Stern's forking lemma [35] which does not yield tight security reductions. Chen *et al.* [7,8,21] gave proofs under the Diffie-Hellman assumption for their schemes by "ID reduction technique" from [1] which does not yield tight security reductions. Bellare *et al.* [29] defined a framework to provide security proofs for a large family of IBS schemes. Unfortunately, their framework does not provide tight security bounds for the resulting family of IBS. Kurosawa and Heng [15] showed a transformation from any digital signature scheme satisfying certain condition to an IBS scheme and gave security proof for the resulting IBS scheme. Although their security proof avoids the use of the forking technique, their reduction is still quite loose. Until today, there have few results on IBS schemes with tight security reductions except that the scheme was constructed by Libert *et al.* [20].

2 Preliminaries

2.1 Security Notion of Signature Scheme

A signature scheme is made up of three algorithms, KeyGen, Sign, and Verify, for generating keys, signing, and verifying signatures, respectively.

The standard notion of security for a signature scheme is called existential unforgeability under a chosen message attack, which is defined using the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

Setup. $\mathcal{C}$ runs the algorithm `KeyGen` of the signature scheme and obtains both the public key PK and the private key SK. The adversary $\mathcal{A}$ is given PK but the private key SK is kept by the challenger.

Queries. Proceeding adaptively, $\mathcal{A}$ requests signatures on at most q_S messages of his choice $m_1, \ldots, m_{q_S} \in \{0,1\}^*$ under PK. $\mathcal{C}$ responds to each query with a signature $\sigma_i = \texttt{Sign}(SK, m_i)$.

Forgery. The adversary outputs a pair (m^*, σ^*). The adversary succeeds if the following hold true:

1) $\texttt{Verify}(PK, m^*, \sigma^*) = \texttt{accept}$.
2) m^* is not any of $m_1, , \ldots, m_{q_S}$.

We define $\texttt{AdvSig}_{\mathcal{A}}$ to be the probability that $\mathcal{A}$ wins in the above game, taken over the coin tosses made by $\mathcal{A}$ and the challenger.

Definition 1. *An adversary $\mathcal{A}$ (t, q_S, ε)-breaks a signature scheme if $\mathcal{A}$ runs in time at most t and makes at most q_S signature queries in the above game, and $\texttt{AdvSig}_{\mathcal{A}}$ is at least ε. A signature scheme is (t, q_S, ε)- existentially unforgeable under adaptively chosen message attacks if no adversary (t, q_S, ε)-breaks it.*

We also consider a slightly stronger notion of security, called strong existential unforgeability. The above game can easily be extended to cover strongly existential unforgeability by changing the second requirement in the forgery stage as follows.

Forgery. The adversary outputs a pair (m^*, σ^*). The adversary succeeds if the following hold true:

1) $\texttt{Verify}(PK, m^*, \sigma^*) = \texttt{accept}$.
2) (m^*, σ^*) is not any of $(m_1, \sigma_1), \ldots (m_{q_S}, \sigma_{q_S})$.

Definition 2. *An adversary $\mathcal{A}$ (t, q_S, ε)-breaks a signature scheme if $\mathcal{A}$ runs in time at most t and makes at most q_S signature queries in the modified game above, and $\texttt{AdvSig}_{\mathcal{A}}$ is at least ε. A signature scheme is (t, q_S, ε)-strongly existentially unforgeable under adaptively chosen message attacks if no adversary (t, q_S, ε)-breaks it.*

2.2 Security Notion of Identity-Based Signature Scheme

An identity-based signature scheme can be described as a collection of the following four algorithms:

Setup. This algorithm is run by the "Private Key Generator" (PKG) on input a security parameter, and generates the public parameters *params* of the scheme and a master secret. PKG publishes *params* and keeps the master secret to itself.

Extract. Given an identity *ID*, the master secret and *params*, this algorithm generates the private key d_{ID} of *ID*. PGK will use this algorithm to generate private keys for all entities participating in the scheme and distribute the private keys to their respective owners through a secure channel.

Table 1: Scheme comparison

Scheme	Reduction	Type of Pairing	Pairing Operation	Security Assumption	Random Oracles
KJ [32]	Loose	Type 1	3	CDH	NO
BJ [20]	Tight	Type 1	2	one more CDH	YES
RG [41]	Tight	Type 1	2	SDH	NO
TYPE I	Tight	Type 1,2	2	SDH	NO
TYPE II	Tight	Type 3	4	SDH	NO

Sign. Given a message m, an identity ID, a private key d_{ID} and *params*, this algorithm generates the signature σ of ID on m. The entity with identity ID will use this algorithm for signing.

Verify. Given a signature σ, a message m, an identity ID and *params*, this algorithm outputs `accept` if σ is a valid signature on m for identity ID, and outputs `reject` otherwise.

We recall here the security notion [20] for identity-based signatures which is an extension of the usual notion of existential unforgeability under chosen-message attacks for signature and which is defined security for identity-based signature schemes by the following game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$:

Setup. $\mathcal{C}$ runs the algorithm `Setup` of the signature scheme and obtains both the public parameters *params* and the master secret SK. $\mathcal{A}$ is given *params* but the master secret SK is kept by the challenger.

Queries. The adversary $\mathcal{A}$ adaptively makes a number of different queries to the challenger.

1) **Extraction query**.Proceeding adaptively, $\mathcal{A}$ requests extractions on at most q_E identities of his choice $ID_1, \ldots, ID_{q_E} \in \{0,1\}^*$. $\mathcal{C}$ responds to each query with $d_{ID_i} = \texttt{Extract}(param, SK, ID_i)$.
2) **Signature query**.Proceeding adaptively, $\mathcal{A}$ requests signatures on at most q_S messages of his choice $(ID_{i_1}, m_1), \ldots, (ID_{i_{q_S}}, m_{q_S}) \in \{0,1\}^* \times \{0,1\}^*$. $\mathcal{C}$ responds to each query by running $\texttt{Extract}(params,\ SK, ID_{i_j})$ to obtain the private key $d_{ID_{i_j}}$ of ID_{i_j}, then running σ_j=$\texttt{Sign}(params,\ d_{ID_{i_j}},\ ID_{i_j}, m_j)$, last forwarding σ_j to the adversary $\mathcal{A}$.

Forgery. The adversary outputs a tuple $(ID^*,\ m^*,\sigma^*)$. The adversary succeeds if the following hold true:

1) $\texttt{Verify}(params, ID^*, m^*, \sigma^*)$=`accept`.
2) ID^* was not any of $ID_1, \ldots, ID_{q_E}$.
3) (ID^*, m^*) was not any of $(ID_{i_1},\ m_1), \ldots, (ID_{i_{q_S}},\ m_{q_S})$.

We define $\texttt{AdvSig}_{\mathcal{A}}$ to be the probability that $\mathcal{A}$ wins in the above game, taken over the coin tosses made by $\mathcal{A}$ and the challenger.

Definition 3. *An adversary $\mathcal{A}$ $(t, q_E, q_S, \varepsilon)$-breaks an IBS signature scheme if $\mathcal{A}$ runs in time at most t and makes at most q_S signature queries, q_E extraction queries in the above game, and* $\textbf{\texttt{AdvSig}}_{\mathcal{A}}$ *is at least ε. A signature scheme is $(t, q_E, q_S, \varepsilon)$- existentially unforgeable under adaptively chosen message and identity attacks if no adversary $(t, q_E, q_S, \varepsilon)$-breaks it.*

2.3 Bilinear Parings and Complexity Assumptions

We consider the mathematical preliminaries for constructing and proving our signature schemes.

Let us consider three cyclic multiplicative group $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ of the same prime order p. Let g_1 be a generator of $\mathbb{G}_1$, g_2 be a generator of $\mathbb{G}_2$. Let $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ be a bilinear pairing with the following properties:

Bilinearity: $\widehat{e}(u^a, v^b) = \widehat{e}(u, v)^{ab}$ for all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$, $a, b \in Z_p$.

Non-degeneracy: There exists $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$ such that $\widehat{e}(u, v) \neq 1$.

Computability: There is an efficient algorithm to compute $\widehat{e}(u, v)$ for all $u \in \mathbb{G}_1$, $v \in \mathbb{G}_2$.

Definition 4. ***Bilinear Groups.*** *We say that $(\mathbb{G}_1, \mathbb{G}_2)$ are bilinear groups if there exists a group $\mathbb{G}_T$ and a non-degenerate bilinear pairing $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, such that the group order of $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ is a prime p, and the bilinear map $\widehat{e}$ and the group operations in $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are all efficiently computable.*

Galbraith, Paterson, and Smart [33] defined three types of pairings:

- In Type 1, $\mathbb{G}_1 = \mathbb{G}_2$.
- In Type 2, $\mathbb{G}_1 \neq \mathbb{G}_2$ but there exists an efficient homomorphism ψ: $\mathbb{G}_2 \to \mathbb{G}_1$, while no efficient one exists in the other direction.
- In Type 3, $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable homomorphism exist between $\mathbb{G}_1$ and $\mathbb{G}_2$, in either direction.

Although Type 1 pairings were mostly used in the early-age of pairing-based cryptography, they have been gradually discarded in favor of Type 3 pairings.

Definition 5. ***q-Strong Diffie-Hellman Problem (q-SDH).*** *Over bilinear groups* $(\mathbb{G}_1, \mathbb{G}_2)$*, given as input a* $q+3$ *tuple of elements* $(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x)$ *output a pair* $(c, g_1^{1/(x+c)})$ *for some value* $c \in \mathbb{Z}_p \setminus \{-x\}$*, where* g_1 *is a generator of* $\mathbb{G}_1$ *and* g_2 *is a generator of* $\mathbb{G}_2$*.*

An algorithm $\mathcal{A}$ solves the q-SDH problem over bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ with advantage ε if

$$\mathtt{SDHAdv}_{q,\mathcal{A}} = Pr[\mathcal{A}(g_1, g_1^x, g_1^{x^2}, \ldots, g_1^{x^q}, g_2, g_2^x) = (c, g_1^{1/(x+c)})] \geq \varepsilon$$

where the probability is over the random choice of generators $g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, the random choice of $x \in \mathbb{Z}_p^*$, and the random bits consumed by $\mathcal{A}$.

Definition 6. ***Strong Diffie-Hellman Assumption (SDH).*** *We say that the* (q, t, ε)*-SDH assumption holds over bilinear groups* $(\mathbb{G}_1, \mathbb{G}_2)$ *if no t-time algorithm has advantage at least* ε *in solving the q-SDH problem over the bilinear groups* $(\mathbb{G}_1, \mathbb{G}_2)$*.*

2.4 Chameleon Hash Function and Combining Function

In this section, we review the notions of chameleon hash function and combining function from [36, 37].

A chameleon hash function CH = (CHGen, CHEval, CHColl) consists of three algorithms. The probabilistic polynomial-time algorithm CHGen takes as input the security parameter k and outputs a secret key $\mathtt{SK_{CH}}$ and a public key $\mathtt{PK_{CH}}$. Given $\mathtt{PK_{CH}}$, a random r from a randomization space $\mathcal{R}$ and a message m from a message space $\mathcal{M}$, the algorithm CHEval outputs a chameleon hash value c in the hash space $\mathcal{C}$. Analogously, CHColl deterministically outputs, on input $\mathtt{SK_{CH}}$ and $(r, m, m') \in \mathcal{R} \times \mathcal{M} \times \mathcal{M}$, $r' \in \mathcal{R}$ such that $\mathtt{CHEval}(\mathtt{PK_{CH}}, m, r) = \mathtt{CHEval}(\mathtt{PK_{CH}}, m', r')$.

Definition 7. ***Collision-resistant chameleon hash function.*** *We say that CH is* (ε, t)*-collision-resistant if no* t*-time algorithm, only given* PK_{CH}*, outputs* (r, r', m, m') *such that* $m \neq m'$ *and* $\mathtt{CHEval}(PK_{CH}, m, r) = \mathtt{CHEval}(PK_{CH}, m', r')$ *with probability at least* ε*, where the probability is over the random choices of* PK_{CH} *and the coin tosses of algorithm.*

For the convenience of writing, we write $\mathtt{CH}(r, m)$ to denote $\mathtt{CHEval}(\mathtt{PK_{CH}}, r, m)$ and $\mathtt{CH}^{-1}(r, m, m')$ for $\mathtt{CHColl}(\mathtt{SK_{CH}}, r, m, m')$ if the keys are obvious from the context.

Definition 8. ***Combining Functions.*** *Let* $\mathcal{V}_k$ *for* $k \in N$ *be a collection of functions of the form* $z : \mathcal{R} \times \mathcal{M} \rightarrow \mathcal{Z}$ *with* $|\mathcal{Z}| \leq 2^k$*. Let* $\mathcal{V} = \{\mathcal{V}_k\}_{k \in N}$*. We say that* $\mathcal{V}$ *is* (t, ε, δ)*-combining if for all attackers* $\mathcal{A}$ *there exist negligible functions* ε *and* δ *and the following properties hold for randomly picked* z *from* $\mathcal{V}_k$*.*

1) *for all* $m \in \mathcal{M}$ *it holds that* $|\mathcal{R}| = |\mathcal{Z}_m|$ *where* $\mathcal{Z}_m$ *is defined as* $\mathcal{Z}_m = z(\mathcal{R}, m)$*. For all* $m \in \mathcal{M}$ *and all* $t \in \mathcal{Z}$ *there exists an efficient algorithm* $z^{-1}(t, m)$ *that, if* $t \in \mathcal{Z}_m$*, outputs the unique value* $r \in \mathcal{R}$ *such that* $z(r, m) = t$*, and* $\perp$ *otherwise.*

2) *for randomly picked* $t \in \mathcal{Z}$ *and* $r' \in \mathcal{R}$*, we have for the maximal (over all* $m \in \mathcal{M}$*) statistical distance between* r' *and* $z^{-1}(t, m)$ *that*

$$\underset{m \in \mathcal{M}}{\mathrm{MAX}}\{\frac{1}{2}\sum_{r \in \mathcal{R}} |Pr[r' = r] - Pr[z^{-1}(t, m) = r]|\} \leq \delta$$

3) *for all* $r \in \mathcal{R}$*, it holds for all t-time attackers* $\mathcal{A}$ *that output* (m, m') *such* $m \neq m'$ *and* $z(r, m) = z(r, m')$ *with probability at most* ε*.*

2.5 The SDH Signatures

The Boneh-Boyen (BB) signature [5, 6] is proven tightly secure under a new flexible assumption, the q-Strong Diffie Hellman (SDH) assumption and without random oracle. Based on this work, Sven Schäge [36, 37] gives combing function based signature (denoted as $\mathrm{S}_{\mathtt{CMB,\ SDH}}$, where CMB is the abbreviation of combing function) and chameleon hash function based signature (denoted as $\mathrm{S}_{\mathtt{CH,\ SDH}}$), respectively.

For the combining signature $\mathrm{S}_{\mathtt{CMB,\ SDH}}$ and the chameleon signature $\mathrm{S}_{\mathtt{CH,\ SDH}}$, if the combing function is $(t_{comb}, \varepsilon_{comb}, \delta_{comb})$-combining, where functions ε_{comb} and δ_{comb} are negligible, and chameleon hash function is collision-resistant, Sven Schäge [36, 37] gave the following result.

Proposition 1. *The combining signature* $S_{\mathtt{CMB,\ SDH}}$*, and the chameleon signature* $S_{\mathtt{CH,\ SDH}}$ *are tightly secure against strong existential forgeries under adaptively chosen message attacks.*

3 $\mathrm{S}_{\mathtt{CMB,\ SDH}}$ Based IBS

3.1 $\mathrm{S}_{\mathtt{CMB,\ SDH}}$ Based IBS over Bilinear Groups with Efficiently Computable Isomorphism

Let $(\mathbb{G}_1, \mathbb{G}_2)$ be bilinear groups with group order $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p,ψ be an efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, if $\mathbb{G}_1 = \mathbb{G}_2$, one could take ψ to be the identity map. For the moment we assume that the messages m to be signed are elements in $\mathbb{Z}_p$, but the domain can be extended to all of $\{0, 1\}^*$ using (target) collision resistant hashing.

Setup: Select five random generators a,b,c,$g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, and random integers x,y,$z \in \mathbb{Z}_p^*$. Then, the bilinear map over bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ is taken as $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$. Compute $u = g_2^x \in \mathbb{G}_2$, $h_1 = g_1^{xy} \in \mathbb{G}_1$, $h_2 = g_1^y \in \mathbb{G}_1$, $f_1 = g_1^{xz} \in \mathbb{G}_1$,

$f_2 = g_1^z \in \mathbb{G}_1$. $\pi : \mathcal{R} \times \mathcal{ID} \to \mathcal{Z}$ is a combining function, where we assume that $\mathcal{Z} \subseteq \mathbb{Z}_p$, $\mathcal{R} \subseteq \mathbb{Z}_p$, $\mathcal{ID}$ is an identity space. Also compute $\gamma_a = \widehat{e}(a, g_2) \in \mathbb{G}_T, \gamma_b = \widehat{e}(b, g_2) \in \mathbb{G}_T, \gamma_c = \widehat{e}(c, g_2) \in \mathbb{G}_T$. The public system parameters are the tuple $(a, b, c, g_1, g_2, h_1, h_2, f_1, f_2, u, \gamma_a, \gamma_b, \gamma_c, \pi, \widehat{e})$. The master secret key is the triple (x, y, z).

Extraction: Given the secret key (x, y, z) and an identity $ID \in \mathcal{ID}$, pick chooses a random value $r \in \mathcal{R}$, a random value $r_0 \in \mathbb{Z}_p \backslash \{-x\}$ and compute $\tau = (ab^r c^{\pi(r,ID)})^{1/(x+r_0)} \in \mathbb{G}_1$. Here, the inverse $1/(x + r_0)$ is computed modulo p. The private key corresponding ID is the pair (τ, r, r_0).

Signature: Given a private key (τ, r, r_0) corresponding identity $ID \in \mathcal{ID}$ and a message $m \in \mathbb{Z}_p$. Pick a random value $k \in \mathbb{Z}_p$ and compute $\sigma_1 = \tau((h_1 h_2^{r_0})^m (f_1 f_2^{r_0}))^k$, $\sigma_2 = (ug_2^{r_0})^k$. The signature is $\sigma = (\sigma_1, \sigma_2, r, r_0)$.

Verification: Given the public system parameters $(a, b, c, g_1, g_2, h_1, h_2, f_1, f_2, u, \gamma_a, \gamma_b, \gamma_c, \pi, \widehat{e})$, an identity $ID \in \mathcal{ID}$, a message $m \in \mathbb{Z}_p$, and a signature $\sigma = (\sigma_1, \sigma_2, r, r_0)$, verify that

$$\widehat{e}(\sigma_1, ug_2^{r_0}) = \gamma_a \gamma_b^r \gamma_c^{\pi(r,ID)} \widehat{e}((h_1 h_2^{r_0})^m (f_1 f_2^{r_0}), \sigma_2)$$

If the equality holds the result is valid; otherwise the result is invalid.

On the IBS scheme above, we have the following result.

Theorem 1. *Suppose the $S_{\texttt{CMB, SDH}}$ signature is $(t', q_E + q_S, \varepsilon')$-secure against strongly existential forgery under an adaptively chosen message attack. Then the identity-based signature scheme above is $(t, q_E, q_S, \varepsilon)$-secure against existential forgery under an adaptively chosen massage and identity attack provided that $q_S + q_E \leq q$, $\varepsilon' \geq \varepsilon - 2q_S/p$, and $t' = t + O((6q_S + 4)T)$, where T is the maximum time for an exponentiation in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{Z}p$.*

Due to limited space, we omit the proof of Theorem 1.

According to Theorem 1 and Proposition 1, for the $S_{\texttt{CMB, SDH}}$ based identity-based signature, we get the following result.

Corollary 1. *Suppose SDH assumption holds in bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$. Then the identity-based signature above is tightly secure against existential forgeries under adaptively chosen massage and identity attacks in standard model.*

3.2 $S_{\texttt{CMB, SDH}}$ Based IBS over Bilinear Groups without Efficiently Computable Isomorphism

Let $(\mathbb{G}_1, \mathbb{G}_2)$ be bilinear groups where $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p, and there are no efficiently computable homomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$. For the moment we assume that the messages m to be signed are elements in $\mathbb{Z}_p$, but the domain can be extended to all of $\{0, 1\}^*$ using (target) collision resistant hashing.

1) **Setup:** Select five random generators $a, b, c, g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, and random integers $x, y, z \in \mathbb{Z}_p^*$. Then, the bilinear map over bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ is taken as $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Compute $u = g_2^x \in \mathbb{G}_2$, $h_1 = g_1^y \in \mathbb{G}_1$, $f_1 = g_1^z \in \mathbb{G}_1$. $\pi : \mathcal{R} \times \mathcal{ID} \to \mathcal{Z}$ is a combining function, where we assume that $\mathcal{Z} \subseteq \mathbb{Z}_p$, $\mathcal{R} \subseteq \mathbb{Z}_p$, $\mathcal{ID}$ is an identity space. Also compute $\gamma_a = \widehat{e}(a, g_2) \in \mathbb{G}_T, \gamma_b = \widehat{e}(b, g_2) \in \mathbb{G}_T, \gamma_c = \widehat{e}(c, g_2) \in \mathbb{G}_T$. The public system parameters are the tuple $(a, b, c, g_1, g_2, h_1, f_1, u, \gamma_a, \gamma_b, \gamma_c, \pi, \widehat{e})$. The master secret key is the triple (x, y, z).

2) **Extraction:** Given the secret key (x, y, z) and an identity $ID \in \mathcal{ID}$, pick chooses a random value $r \in \mathcal{R}$, a random value $r_0 \in \mathbb{Z}_p \backslash \{-x\}$ and compute $\tau = (ab^r c^{\pi(r,ID)})^{1/(x+r_0)} \in \mathbb{G}_1$. Here, the inverse $1/(x + r_0)$ is computed modulo p. The private key corresponding ID is the pair (τ, r, r_0).

3) **Signature:** Given a private key (τ, r, r_0) corresponding identity $ID \in \mathcal{ID}$ and a message $m \in \mathbb{Z}_p$, pick a random value $k \in \mathbb{Z}_p$ and compute $\sigma_1 = \tau(h_1^m f_1)^k$, $\sigma_2 = (ug_2^{r_0})^k$, $\sigma_3 = g_1^k$. The signature is $\sigma = (\sigma_1, \sigma_2, \sigma_3, r, r_0)$.

4) **Verification:** Given the public system parameters $(a, b, c, g_1, g_2, h_1, f_1, u, \gamma_a, \gamma_b, \gamma_c, \pi, \widehat{e})$, an identity $ID \in \mathcal{ID}$, a message $m \in \mathbb{Z}_p$, and a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, r, r_0)$, verify that

$$\widehat{e}(\sigma_1, ug_2^{r_0}) = \gamma_a \gamma_b^r \gamma_c^{\pi(r,ID)} \widehat{e}(h_1^m f_1, \sigma_2)$$
$$\widehat{e}(\sigma_3, ug_2^{r_0}) = \widehat{e}(g_1, \sigma_2).$$

If the equality holds the result is valid; otherwise the result is invalid.

On the IBS scheme above, we have the following result.

Theorem 2. *Suppose the $S_{\texttt{CMB, SDH}}$ signature is $(t', q_E + q_S, \varepsilon')$-secure against strongly existential forgery under an adaptively chosen message attack. Then the identity-based signature scheme above is $(t, q_E, q_S, \varepsilon)$-secure against existential forgery under an adaptively chosen massage and identity attack provided that*

$$q_S + q_E \leq q,\ \varepsilon' \geq \varepsilon - 2q_S/p, \text{ and } t' = t + O((5q_S + 4)T),$$

where T is the maximum time for an exponentiation in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{Z}p$.

Due to limited space, we omit the proof of Theorem 2.

According to Theorem 2 and Proposition 1, for the $S_{\texttt{CMB, SDH}}$ based identity-based signature, we get the following result.

Corollary 2. *Suppose SDH assumption holds in bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$. Then the identity-based signature above is tightly secure against existential forgeries under adaptively chosen massage and identity attacks in standard model.*

4 $S_{\texttt{CH},\ \texttt{SDH}}$ Based IBS

4.1 Construction over Bilinear Groups with Efficiently Computable Isomorphism

Let $(\mathbb{G}_1, \mathbb{G}_2)$ be bilinear groups where $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p, ψ be an efficiently computable isomorphism from $\mathbb{G}_2$ to $\mathbb{G}_1$, if $\mathbb{G}_1 = \mathbb{G}_2$, one could take ψ to be the identity map. For the moment we assume that the messages m to be signed are elements in $\mathbb{Z}_p$, but the domain can be extended to all of $\{0,1\}^*$ using (target) collision resistant hashing.

1) **Setup:** Select random generators $a, b, g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, and random integers $x, y, z \in \mathbb{Z}_p^*$. Then, the bilinear map over bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ is taken as $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Compute $u = g_2^x \in \mathbb{G}_2$, $h_1 = g_1^{xy} \in \mathbb{G}_1$, $h_2 = g_1^y \in \mathbb{G}_1$, $f_1 = g_1^{xz} \in \mathbb{G}_1$, $f_2 = g_1^z \in \mathbb{G}_1$. $\texttt{CH}$ is a chameleon hash function and its public key is $\texttt{PK}_{\texttt{CH}}$. Also compute $\gamma_a = \widehat{e}(a, g_2) \in \mathbb{G}_T$,$\gamma_b = \widehat{e}(b, g_2) \in \mathbb{G}_T$. The public system parameters are the tuple $(a, b, g_2, h_1, h_2, f_1, f_2, u, \gamma_a, \gamma_b, \texttt{CH}, \texttt{PK}_{\texttt{CH}}, \widehat{e})$. The master secret key is the triple (x, y, z).

2) **Extraction:** Given the master secret key (x, y, z) and an identity $ID \in \mathcal{ID}$, pick chooses a random $r \in \mathcal{R}$, a random $t \in \mathbb{Z}_p \backslash \{-x\}$ and compute $\tau = (ab^{\texttt{CH}(r,ID)})^{1/(x+t)} \in \mathbb{G}_1$. Here, the inverse $1/(x+t)$ is computed modulo p. The private key corresponding ID is the pair (τ, r, t).

3) **Signature:** Given a private key (τ, r, t) corresponding identity ID and a message $m \in \mathbb{Z}_p$, pick a random $k \in \mathbb{Z}_p$ and compute $\sigma_1 = \tau((h_1 h_2^t)^m (f_1 f_2^t))^k$, $\sigma_2 = (u g_2^t)^k$. The signature is $\sigma = (\sigma_1, \sigma_2, r, t)$.

4) **Verification:** Given the public system parameters $(a, b, c, g_1, g_2, h_1, h_2, f_1, f_2, u, \gamma_a, \gamma_b, \gamma_c, \pi, \widehat{e})$, an identity ID, a message $m \in \mathbb{Z}_p$, and a signature $\sigma = (\sigma_1, \sigma_2, r, t)$, verify that

$$\widehat{e}(\sigma_1, u g_2^t) = \gamma_a \gamma_b^{\texttt{CH}(r,ID)} \widehat{e}((h_1 h_2^t)^m (f_1 f_2^t), \sigma_2) \quad (1)$$

If the equality holds the result is valid; otherwise the result is invalid.

On the IBS scheme above, we have the following result.

Theorem 3. *Suppose the $S_{\texttt{CH},\ \texttt{SDH}}$ signature is $(t', q_E + q_S, \varepsilon')$-secure against strongly existential forgery under an adaptively chosen message attack. Then the identity-based signature scheme above is $(t, q_E, q_S, \varepsilon)$-secure against existential forgery under an adaptively chosen massage and identity attack provided that $q_S + q_E \leq q$, $\varepsilon' \geq \varepsilon - 2q_S/(p-1)$, and $t' = t + O((6q_S + 6)T)$, where T is the maximum time for an exponentiation in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{Z}p$.*

Due to limited space, we omit the proof of Theorem 3.

According to Theorem 3 and Proposition 1, for the $S_{\texttt{CH},\ \texttt{SDH}}$ based identity-based signature, we get the following result.

Corollary 3. *Suppose SDH assumption holds in bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$. Then the identity-based signature above is tightly secure against existential forgeries under adaptively chosen massage and identity attacks in standard model.*

4.2 Construction over Bilinear Groups without Efficiently Computable Isomorphism

Let $(\mathbb{G}_1, \mathbb{G}_2)$ be bilinear groups where $|\mathbb{G}_1| = |\mathbb{G}_2| = p$ for some prime p, and there are no efficiently computable homomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$. For the moment we assume that the messages m to be signed are elements in $\mathbb{Z}_p$, but the domain can be extended to all of $\{0,1\}^*$ using (target) collision resistant hashing.

1) **Setup:** Select random generators $a, b, g_1 \in \mathbb{G}_1$ and $g_2 \in \mathbb{G}_2$, and random integers $x, y, z \in \mathbb{Z}_p^*$. Then, the bilinear map over bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ is taken as $\widehat{e} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. Compute $u = g_2^x \in \mathbb{G}_2$, $h_1 = g_1^y \in \mathbb{G}_1$, $f_1 = g_1^z \in \mathbb{G}_1$. $\texttt{CH}$ is a chameleon hash function and its public key is $\texttt{PK}_{\texttt{CH}}$. Also compute $\gamma_a = \widehat{e}(a, g_2) \in \mathbb{G}_T$,$\gamma_b = \widehat{e}(b, g_2) \in \mathbb{G}_T$. The public system parameters are the tuple $(a, b, g_2, h_1, f_1, u, \gamma_a, \gamma_b, \texttt{CH}, \texttt{PK}_{\texttt{CH}}, \widehat{e})$. The master secret key is the triple (x, y, z).

2) **Extraction:** Given the master secret key (x, y, z) and an identity $ID \in \mathcal{ID}$, pick chooses a random $r \in \mathcal{R}$, a random $t \in \mathbb{Z}_p \backslash \{-x\}$ and compute $\tau = (ab^{\texttt{CH}(r,ID)})^{1/(x+t)} \in \mathbb{G}_1$. Here, the inverse $1/(x+t)$ is computed modulo p. The private key corresponding ID is the pair (τ, r, t).

3) **Signature:** Given a private key (τ, r, t) corresponding identity ID and a message $m \in \mathbb{Z}_p$, pick a random $k \in \mathbb{Z}_p$ and compute $\sigma_1 = \tau(h_1^m f_1)^k$, $\sigma_2 = (u g_2^t)^k$,$\sigma_3 = g_1^k$. The signature is $\sigma = (\sigma_1, \sigma_2, \sigma_3, r, t)$.

4) **Verification:** Given the public system parameters $(a, b, c, g_1, g_2, h_1, f_1, u,\ \gamma_a,\gamma_b,\gamma_c, \pi, \widehat{e})$, an identity ID, a message $m \in \mathbb{Z}_p$, and a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, r, t)$, verify that

$$\widehat{e}(\sigma_1, u g_2^t) = \gamma_a \gamma_b^{\texttt{CH}(r,ID)} \widehat{e}(h_1^m f_1, \sigma_2)$$
$$\widehat{e}(\sigma_3, u g_2^t) = \widehat{e}(g_1, \sigma_2)$$

If the equality holds the result is valid; otherwise the result is invalid.

On the IBS scheme above, we have the following result.

Theorem 4. *Suppose the $S_{\texttt{CH},\ \texttt{SDH}}$ signature is $(t', q_E + q_S, \varepsilon')$-secure against strongly existential forgery under an adaptively chosen message attack. Then the identity-based signature scheme above is $(t, q_E, q_S, \varepsilon)$-secure against existential forgery under an adaptively chosen massage and identity attack provided that $q_S + q_E \leq q$, $\varepsilon' \geq \varepsilon - 2q_S/(p-1)$, and $t' = t + O((5q_S + 4)T)$, where T is the maximum time for an exponentiation in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{Z}p$.*

Due to limited space, we omit the proof of Theorem 4.

According to Theorem 4 and Proposition 1, for the $S_{\texttt{CH, SDH}}$ based identity-based signature, we get the following result.

Corollary 4. *Suppose SDH assumption holds in bilinear groups* $(\mathbb{G}_1, \mathbb{G}_2)$*. Then the identity-based signature above is tightly secure against existential forgeries under adaptively chosen massage and identity attacks in standard model.*

5 Conclusion

In this paper, according to the fact whether bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ have an efficiently computable homomorphism, we give two IBS schemes, which are existentially unforgeable under adaptively chosen message and identity attacks and whose security is tightly related to q-SDH in the standard model, based on $S_{\texttt{CMB, SDH}}$ proposed by Sven Schäge [36,37]. And then, we apply the idea constructing IBS schemes above to the $S_{\texttt{CH, SDH}}$ by Sven Schäge [36,37], we also get IBS schemes which are existentially unforgeable under adaptively chosen message and identity attacks and whose security is also tightly related to q-SDH in the standard model.

Acknowledgments

The authors gratefully acknowledge the anonymous reviewers for their valuable comments. This study is supported by the Fundamental Research Funds for the Central Universities.

References

[1] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," in *Advances in Cryptology (ASIACRYPT'99)*, pp. 378–389, 1999.

[2] M. Bellare and P. Rogaway, "The exact security of digital signatures: How to sign with rsa and rabin," in *Advances in Cryptology (EUROCRYPT'96)*, pp. 399–416, 1996.

[3] D. J. Bernstein, "Proving tight security for rabin-williams signatures," in *Advances in Cryptology (EUROCRYPT'08)*, pp. 70–87, 2008.

[4] R. Bhaskar, S. Garg and S. V. Lokam, "Improved bounds on security reductions for discrete log based signatures," in *Advances in Cryptology (CRYPTO'08)*, pp. 93–107, 2008.

[5] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," in *Advances in Cryptology (EUROCRYPT'04)*, pp. 56–73, 2004.

[6] D. Boneh and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[7] H. Chen, Y. Li, "Efficient identity-based signature scheme with partial message recovery," in *Proceedings of the Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing (SNPD'07)*, pp. 883–888, 2007.

[8] H. Chen, Z. Wang, "A practical identity-based signature scheme from bilinear map," in *Emerging Directions in Embedded and Ubiquitous Computing (EUC'07)*, pp. 704–715, 2007.

[9] J. H. Cheon J. C. Cha, "An identity-based signature from gap diffie-hellman groups," in *Public Key Cryptography (PKC'03)*, pp. 18–30, 2003.

[10] J. S. Coron, "Optimal security proofs for PSS and other signature schemes," in *Advances in Cryptology (EUROCRYPT'02)*, pp. 272–287, 2002.

[11] Y. Dodis and L. Reyzin, "On the power of claw-free permutations," in *Third International Conference on Security in Communication Networks*, pp. 55–73, 2002.

[12] N. Fleischhacker, T. Jager, D. Schröder, "On tight security proofs for schnorr signatures," in *Advances in Cryptology (ASIACRYPT'14)*, pp. 512–531, 2014.

[13] F. D. Garcia, D. Galindo, "A schnorr-like lightweight identity-based signature scheme," in *International Conference on Cryptology in Africa*, pp. 135–148, 2009.

[14] E. J. Goh and S. Jarecki, "A signature scheme as secure as the diffie-hellman problem," in *Advances in Cryptology (EUROCRYPT'03)*, pp. 401–415, 2003.

[15] S. H. Heng, K. Kurosawa, "From digital signature to id-based identification/signature," in *Public Key Cryptography (PKC'04)*, pp. 248–261, 2004.

[16] F. Hess, "Efficient identity based signature schemes based on pairings," in *9th Annual International Workshop on Selected Areas in Cryptography*, pp. 310–324, 2002.

[17] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", *Computer Standards & Interfaces*, vol. 26, no. 6, pp. 565–569, 2004.

[18] J. Katz and N. Wang, "Efficiency improvements for signature schemes with tight security reductions," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS'03)*, pp. 155–164, 2003.

[19] J. Katz, N. Wang, E. J. Goh, S. Jarecki, "Efficient signature schemes with tight reductions to the diffie-hellman problems," *Journal of Cryptology*, vol. 20, no. 4, pp. 493–514, 2007.

[20] B. Libert and J. J. Quisquater, "The exact security of an identity based signature and its applications," in *Iacr Cryptology Eprint Archive*, 2004. (`http://eprint.iacr.org/2004/102`)

[21] Z. H. Liu, H. Y. Chen, S. W. Lu, "Identity-based signature scheme with partial message recovery," *Chinese Journal of Computers*, vol. 29, no. 9, pp. 1622–1627, 2006.

[22] B. Lynn, D. Boneh and H. Shacham, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[23] V. Lyubashevsky, M. Abdalla, P. A. Fouque and M. Tibouchi, "Tightly-secure signatures from lossy identification schemes," in *Advances in Cryptology (EUROCRYPT'12)*, pp. 572–590, 2012.

[24] B. C. Mames, "An efficient CDH-based signature scheme with a tight security reduction," in *Advances in Cryptology (CRYPTO'05)*, pp. 511–526, 2005.

[25] B. C. Mames and M. Joye, "A practical and tightly secure signature scheme without hash function," in *Cryptographers' Track at the RSA Conference (CT-RSA'07)*, pp. 339–356, 2007.

[26] J. Mao, J. Zhang, "A novel id-based designated verifier signature scheme," *Information Sciences*, vol. 178, no. 3, pp. 766–773, 2008.

[27] S. Micali and L. Reyzin, "Improving the exact security of digital signature schemes," *Journal of Cryptology*, vol. 15, no. 1, pp. 1–18, 2002.

[28] Y. Mu, F. Zhang, W. Susilo, "Identity-based partial message recovery signatures (or how to shorten id-based signatures)," in *The 9th International Conference on Financial Cryptography and Data Security (FC'05)*, pp. 45–56, 2005.

[29] C. Namprempre, M. Bellare and G. Neven, "Security proofs for identity-based identification and signature schemes," in *Advances in Cryptology (EUROCRYPT'04)*, pp. 268–286, 2004.

[30] T. Okamoto, R. Tso, C. Gu and E. Okamoto, "Efficient id-based digital signatures with message recovery," in *Cryptology and Network Security (CANS'07)*, pp. 47–59, 2007.

[31] P. Paillier and D. Vergnaud, "Discrete-log-based signatures may not be equivalent to discrete log," in *Advances in Cryptology (ASIACRYPT'05)*, pp. 1–20, 2005.

[32] K. G. Paterson and J. C. N. Schuldt, "Efficient identity-based signatures secure in the standard model," in *Australasian Conference on Information Security and Privacy*, pp. 207–222, 2006.

[33] K. G. Paterson, N. P. Smart, S. D. Galbraith, "Pairings for cryptographers," *Discrete Applied Mathematics*, vol. 156, pp. 3113–3121, 2008.

[34] N. M. Paulo, S. L. M. Barreto, B. Libert and J. J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 515–532, 2005.

[35] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361–396, 2000.

[36] S. Schäge, "Tight proofs for signature schemes without random oracles," in *Advances in Cryptology (EUROCRYPT'11)*, pp. 189–206, 2011.

[37] S. Schäge, "Tight security for signature schemes without random oracles," *Journal of Cryptology*, vol. 28, no. 3, pp. 641–670, 2015.

[38] Y. Seurin, "On the exact security of schnorr-type signatures in the random oracle model," in *Advances in Cryptology (EUROCRYPT'12)*, pp. 554–571, 2013.

[39] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Cryptology (CRYPTO'84)*, pp. 176–180, June 2008.

[40] W. Susilo, F. Zhang, R. S. Naini, "An efficient signature scheme from bilinear pairings and its applications," in *Public Key Cryptography (PKC'04)*, pp. 277–290, 2004.

[41] R. Yanli and G. Dawu, "Efficient identity based signature/signcryption scheme in the standard model," in *The First International Symposium on Data, Privacy and E-Commerce (ISDPE'07)*, pp. 133–137, 2007.

[42] X. Yi, "An identity-based signature scheme from the weil pairing," *IEEE Communications Letters*, vol. 7, no. 2, pp. 76–78, 2003.

[43] S. Zheng, Y. Yang, Z. Wang, L. Wang and Z. Hu, "Provably secure and efficient identity-based signature scheme based on cubic residues," *International Journal of Network Security*, vol. 14, no. 1, pp. 33–38, 2012.

Biography

Chen Huiyan received his PhD degree from Graduate University of Chinese Academy of Sciences in 2007. His research interests include cryptography, information security, and cloud computing.

Zhang Yanshuo received his PhD degree from Academy of Mathematics and Systems Science of the Chinese Academy of Sciences in 2009. His research interests include cryptography, information security.

Wan Zongjie received his M.S. degree from Beijing University of Post and Telecommunications in 2008. His research interests include cryptography, network security, and cloud computing.

Zhang Chenchen is currently a master degree candidate in the School of information and Communication Engineering,Xidian University. His research interests are information security and cryptography.