INFORMATICA, 2014, Vol. 25, No. 3, 505–521

DOI: http://dx.doi.org/10.15388/Informatica.2014.26

Efficient Strongly Unforgeable ID-Based Signature Without Random Oracles

Tung-Tso TSAI, Yuh-Min TSENG*, Sen-Shan HUANG,
Department of Mathematics, National Changhua University of Education
Jin-De Campus, Chang-Hua City 500, Taiwan
e-mail: ymtseng@cc.ncue.edu.tw

Received: May 2013; accepted: October 2013

Abstract. Up to date, a large number of ID-based signature (IBS) schemes based on bilinear pairings have been proposed. Most of these IBS schemes possess existential unforgeability under adaptive chosen-message attacks, among which some offer strong unforgeability. An IBS scheme is said to be strongly unforgeable if it possesses existential unforgeability and an adversary who is given signatures of the IBS scheme on some message m is unable to generate a new signature on m. Strong unforgeable IBS schemes can be used to construct many important ID-based cryptographic schemes. However, the existing strongly unforgeable IBS schemes lack efficiency for the signature size and the computation cost of verification phase. In this paper, we propose an efficient strongly unforgeable IBS scheme without random oracles. Under the computational Diffie–Hellman and collision resistant hash assumptions, we demonstrate that the proposed IBS scheme possesses strong unforgeability against adaptive chosen-message attacks. When compared with previously proposed strongly unforgeable IBS schemes, our scheme has better performance in terms of signature size and computation cost.

Key words: ID-based signature, strong unforgeability, standard model, bilinear pairing.

1. Introduction

Shamir (1984) presented a brilliant idea for public key cryptosystems, in which a user's public key is derived from the user's known identity information such as social security number, e-mail address, telephone number, name, etc. Based on Shamir's idea, Boneh and Franklin (2001) constructed the first practical identity (ID)-based encryption (IBE) scheme. Their scheme was built on the progress in elliptic curves with bilinear pairings such as Weil, Tate and Ate pairings. Subsequently, the study of ID-based cryptography using bilinear pairings has received significant attention from cryptographic research community. A large number of ID-based cryptographic schemes were presented in the literature such as ID-based key agreement protocols (Boyd and Choo, 2005; Chow and Choo, 2007; Chen *et al*., 2007; Wu and Tseng, 2010), ID-based encryption schemes (Boneh and Hamburg, 2008; Tseng and Tsai, 2012; Wang *et al*., 2012; Tsai *et al*., 2012), ID-based authentication protocols (Bellare *et al*., 2004; Tseng *et al*.,

*Corresponding author.

2008) and ID-based group key agreement schemes (Choi *et al*., 2008; Wu *et al*., 2011; Wu and Tseng, 2012).

Paterson (2002) proposed an ID-based signature (IBS) scheme using bilinear pairings, in which the computation efficiency and signature size need improvement. Later, Cha and Cheon (2003) proposed an IBS scheme more efficient than Paterson's. However, their IBS scheme is unable to provide batch verifications. Yoon *et al*. (2004) proposed an improved IBS scheme that supports batch verifications, but increases the computation cost in the signing phase. Tseng *et al*. (2009) and Shim (2010), respectively, proposed IBS schemes that support variant kinds of batch verifications and retain efficiency as Cha and Cheon's scheme. The IBS schemes above were proven to be secure in the random oracle model (Bellare and Rogaway, 1993). However, the ID-based cryptographic schemes in the random oracle model could be insecure when random oracles are instantiated with concrete hash functions. Afterwards, several IBS without random oracles were proposed such as (Waters, 2005; Paterson and Schuldt, 2006; Narayan and Parampalli, 2008; Sato *et al*., 2009).

Most of these IBS schemes possess (weakly) existential unforgeability under adaptive chosen-message attacks, among which some offer strong unforgeability. An IBS scheme is said to be strongly unforgeable if it possesses existential unforgeability and an adversary who is given signatures of the IBS scheme on some message m is unable to generate a new signature on m. Strongly unforgeable IBS schemes can be used to construct many important ID-based cryptographic schemes, such as chosen-ciphertext secure ID-based cryptosystems and ID-based group signatures, etc. In particular, in a chosen-ciphertext secure ID-based cryptosystem, a ciphertext often incorporates a signature generated by an encryptor. In this situation, if a signature did not possess strong unforgeability, an adversary would be able to modify the signature on the challenge ciphertext so that she/he could issue a decryption query for the modified ciphertext and break the cryptosystem.

In the past, several strongly unforgeable non-ID-based signature schemes without random oracles have been proposed such as (Boneh and Boyen, 2004; Zhang *et al*., 2006; Camenisch and Lysyanskaya, 2004; Boneh *et al*., 2006). Some work (Bellare *et al*., 2004; Dodis *et al*., 2003; Galindo *et al*., 2006) provided transformation methods to construct strongly unforgeable IBS schemes from strongly unforgeable non-ID-based signature schemes. Huang *et al*. (2007) proposed a generic transformation method which converts existentially unforgeable IBS schemes without random oracles into strongly unforgeable ones by attaching a strong one-time signature (Zhang *et al*., 2006; Boneh *et al*., 2006). However, the strongly unforgeable IBS schemes constructed by the methods above need at least six signature parameters. Sato *et al.* (2009, 2010) proposed a strongly unforgeable IBS scheme without random oracles based on Paterson and Schuldt's IBS scheme (Paterson and Schuldt, 2006). Their scheme is directly constructed without applying any transformation, and the signature size is reduced to five signature parameters. Nevertheless, all the schemes without random oracles above still lacked efficiency for signature size and computation cost.

In the article, our goal is to construct an efficient strongly unforgeable IBS scheme without random oracles. In general, a directly constructed strongly unforgeable IBS

schemes has a better performance than those transformed from known schemes. Therefore, we adopt a direct construction to propose our scheme. Based on Paterson and Schuldt's existentially unforgeable IBS scheme, we propose a strongly unforgeable IBS scheme by making use of collision-resistant hash functions. Our scheme retains the same computation performance as Paterson and Schuldt's scheme in terms of signature size and computation cost. We emphasize that the employed collision-resistant hash functions are not viewed as random oracles in our security proofs. Collision-resistant hash functions based on the computational Diffie–Hellman assumption (Boneh *et al*., 2006) can be easily constructed and do not strengthen the complexity assumption of our scheme. Under the computational Diffie–Hellman and collision resistant hash assumptions, we demonstrate that the proposed IBS scheme possesses strong unforgeability against adaptive chosen-message attacks (ID-SUF-ACMA). When compared with previously proposed strongly unforgeable IBS schemes without random oracles, our scheme has better performance in terms of signature size and computation cost.

The remainder of the paper is organized as follows. Preliminaries are given in Section 2. The framework and security notions for strongly unforgeable IBS schemes are formally defined in Section 3. In Section 4, we presents a concrete strongly unforgeable IBS scheme without random oracles. In Section 5, we analyze the security of our scheme. In Section 6, we demonstrates performance analysis and comparisons. Conclusions are given in Section 7.

2. Preliminaries

In this section, we briefly introduce the concept of bilinear pairings and the related mathematical assumptions.

2.1. *Bilinear Pairings*

We assume that $\mathbb{G}_1$ and $\mathbb{G}_2$ are two multiplicative cyclic groups of large prime order p, and let g be a generator of $\mathbb{G}_1$. We say that the map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is an admissible bilinear map if the map $\hat{e}$ satisfies the following properties.

(1) Bilinearity: $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$ for all $g \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p^*$.
(2) Non-degeneracy: $\hat{e}(g, g) \neq 1$.
(3) Computability: there exists an efficient algorithm to compute $\hat{e}(g_1, g_2)$ for all $g_1, g_2 \in \mathbb{G}_1$.

Full descriptions of groups, maps and other parameters are discussed in Boneh and Franklin (2001), Bellare *et al*. (2004), Waters (2005), Paterson and Schuldt (2006).

2.2. *Related Assumption*

Here, we define the computational Diffie–Hellman (CDH) problem in a group $\mathbb{G}_1$ of large prime order p with generator g. Given elements $g, g^a, g^b \in \mathbb{G}_1$ for unknown $a, b \in \mathbb{Z}_p^*$, the CDH problem in $\mathbb{G}_1$ is to compute g^{ab}.

DEFINITION 1. The CDH assumption is defined as follows. Given $g, g^a, g^b \in \mathbb{G}_1$ for unknown $a, b \in \mathbb{Z}_p^*$, there exists no probabilistic polynomial-time adversary $\mathcal{A}$ with non-negligible probability who can compute g^{ab}. The successful probability (advantage) of the adversary $\mathcal{A}$ is presented as

$$Adv_{\mathcal{A}} = \Pr\left[\mathcal{A}\left(g, g^a, g^b\right) = g^{ab} : g \in \mathbb{G}_1,\ a, b \in \mathbb{Z}_p^*\right],$$

where the probability is over the random choices consumed by the adversary $\mathcal{A}$.

2.3. *Collision Resistant Hash Assumption*

Here, we present the definition of a collision-resistant hash family of functions (Damgard, 1987; Boneh *et al*., 2006) on which our scheme is based, called the CRH assumption.

DEFINITION 2. The CRH assumption is defined as follows. We assume that there is a collision-resistant hash family of functions $H_k : \{0,1\}^* \to \{0,1\}^n$, where n is a fixed length and k is an index. Concretely, there exists no probabilistic polynomial-time adversary $\mathcal{A}$ with non-negligible probability who can break the collision resistance of H_k. The successful probability (advantage) of the adversary $\mathcal{A}$ is presented as

$$Adv_{\mathcal{A}}^{CRH} = \Pr\left[\mathcal{A}(k) = (m_0, m_1) : m_0 \neq m_1,\ H_k(m_0) = H_k(m_1)\right],$$

where the probability is over the random choice consumed by the adversary $\mathcal{A}$.

REMARK 1. Based on the CDH assumption, we can easily construct collision-resistant hash functions (Damgard, 1987; Boneh *et al*., 2006). In such a case, the requirement of collision resistant hash functions does not strengthen the complexity assumption of our IBS scheme. In practice, we would use a standard hash function such as SHA-256 in our IBS scheme. Since the employed hash functions are not viewed as random oracles in our security proofs, we assume that they are collision-resistant (Boneh *et al*., 2006).

3. Framework and Security Notions for Strongly Unforgeable IBS Schemes

In this section, we present the framework for strongly unforgeable IBS schemes and its security notions. The framework of strongly unforgeable IBS schemes is identical to that given in Cha and Cheon (2003) or Paterson and Schuldt (2006).

DEFINITION 3. A strongly unforgeable IBS is a 4-tuple $(\mathcal{G}, \mathcal{E}, \mathcal{S}, \mathcal{V})$ of polynomial-time algorithms:

- *Setup algorithm* $\mathcal{G}$: Taking a security parameter l as input, the algorithm returns a system secret key s and public parameters *Parms*. The public parameters *Parms* are made public.

- *Extract algorithm* $\mathcal{E}$: The system secret key s and a user's identity ID are taken as input and the algorithm returns the user's private key D_{ID}.
- *Signing algorithm* $\mathcal{S}$: Taking as input a user's private key D_{ID} and a message M, the algorithm generates a signature σ on message M.
- *Verification algorithm* $\mathcal{V}$: Taking as input a signature σ, a message M and a user's identity ID, the algorithm outputs "accept" if σ is a valid signature on the message M, and "reject" otherwise.

The security notion for strongly unforgeable IBS schemes, termed strong unforgeability, is identical to that given by Sato *et al*. (2009).

Definition 4. We say that a strongly unforgeable IBS scheme possesses strong unforgeability against adaptive chosen-message attacks (ID-SUF-ACMA) if no probabilistic polynomial-time adversary $\mathcal{A}$ has a non-negligible advantage in the following game (ID-SUF-ACMA game) played with a challenger $\mathcal{B}$.

- *Setup*. The challenger $\mathcal{B}$ takes a security parameter l and runs the *Setup algorithm* $\mathcal{G}$ to produce a system secret key s and public parameters *Parms*. The challenger $\mathcal{B}$ then gives *Parms* to $\mathcal{A}$ and keeps the system secret key s to itself.
- *Queries*. The adversary $\mathcal{A}$ adaptively makes queries of two kinds to the challenger $\mathcal{B}$ as follows.
  - *Extract query* (ID). Upon receiving this query along with identity ID, the challenger $\mathcal{B}$ runs the *Extract algorithm* $\mathcal{E}$ to return the user's private key D_{ID} to $\mathcal{A}$.
  - *Signing queries* (ID, M). Upon receiving the query along with (ID, M), the challenger $\mathcal{B}$ first runs the *Extract algorithm* $\mathcal{E}$ to obtain the user's private key D_{ID}, and then runs the *Signing algorithm* $\mathcal{S}$ to generate a signature σ on the message M by using D_{ID}. The challenger $\mathcal{B}$ returns σ to $\mathcal{A}$.
- *Forgery*. We say that the adversary $\mathcal{A}$ wins the ID-SUF-ACMA game if $\mathcal{A}$ generates a tuple (ID^*, M^*, σ^*) which satisfies the following conditions:

  (1) The response of the *Verification algorithm* $\mathcal{V}$ on (ID^*, M^*, σ^*) is "accept".
  (2) (ID^*, M^*, σ^*) did not appear in the *Signing query*.
  (3) ID^* did not appear in the *Extract query*.

The adversary $\mathcal{A}$'s advantage is defined as the probability that $\mathcal{A}$ wins.

Remark 2. We say that an IBS scheme possesses existential unforgeability against adaptive chosen-message attacks (ID-UF-ACMA) if no probabilistic polynomial-time adversary $\mathcal{A}$ has a non-negligible advantage in the ID-UF-ACMA game played with a challenger $\mathcal{B}$. The ID-UF-ACMA game is identical to ID-SUF-ACMA game except that the condition (2) in *Forgery* of the former game is modified as "(ID^*, M^*) did not appear in the *Signing query*". Evidently, a strongly unforgeable IBS scheme provides stronger unforgeability than an existentially unforgeable IBS scheme.

4. Strongly Unforgeable IBS Scheme Without Random Oracles

Here, we present an efficient strongly unforgeable IBS scheme without random oracles that consists of four algorithms: *Setup*, *Extract*, *Signing* and *Verification*.

- *Setup*. A trusted PKG takes a security parameter l as input. The PKG chooses two groups $\mathbb{G}_1, \mathbb{G}_2$ of sufficiently large prime order $p > 2^l$, a generator g of $\mathbb{G}_1$ and an admissible bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. The PKG sets three collision resistant hash functions, namely, $H_1 : \{0,1\}^* \to \{0,1\}^m$ and $H_2, H_3 : \{0,1\}^* \to \{0,1\}^n$, where m and n are fixed lengths. We assume $p > 2^m$ and $p > 2^n$ so that the hash outputs can be viewed as the elements of $\mathbb{Z}_p$. The PKG randomly chooses two values $u', w' \in \mathbb{G}_1$ as well as two vectors $U = (u_i)$ of length m and $W = (w_j)$ of length n, where $u_i, w_j \in \mathbb{G}_1$ for $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$. The PKG then chooses a secret random value $\alpha \in \mathbb{Z}_p^*$ and computes $g_1 = g^\alpha \in \mathbb{G}_1$. Finally, the PKG randomly chooses $g_2 \in \mathbb{G}_1$ and sets the system secret key $s = g_2^\alpha$ and the public parameters $Parms = \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, u', U, w', W \rangle$.
- *Extract*. Given a user's identity $ID \in \{0,1\}^*$, the PKG sets $v = H_1(ID)$. Here, $v = (v_1, \ldots, v_m)$ is a bit string of length m. Let $\mathcal{U} \subset \{1, 2, \ldots, m\}$ be the set of index i such that $v_i = 1$, for $i = 1, 2, \ldots, m$. The PKG chooses a random value $r_v \in \mathbb{Z}_p^*$ and computes the user's private key $D_{ID} = (D_1, D_2) = (g_2^\alpha (u' \prod_{i \in \mathcal{U}} u_i)^{r_v}, g^{r_v})$. The PKG transmits D_{ID} to the user via a secure channel.
- *Signing*. Given a message $M \in \{0,1\}^*$, let $vm = H_2(M)$ be a bit string of length n and let vm_j denote the jth bit of vm. Let $\mathcal{W} \subset \{1, 2, \ldots, n\}$ be the set of index j such that $vm_j = 1$, for $j = 1, 2, \ldots, n$. The signer with identity ID chooses a random number $r_m \in \mathbb{Z}_p^*$ and then computes $h = H_3(M || g^{r_m})$. The signer uses her/his private key $D_{ID} = (D_1, D_2)$ to create a signature on the message M by

$$\begin{aligned}\sigma &= (\sigma_1, \sigma_2, \sigma_3) \\ &= \left(D_1^h \left(w' \prod_{j \in \mathcal{W}} w_j \right)^{r_m}, D_2^h, g^{r_m} \right) \\ &= \left(\left(g_2^\alpha \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v} \right)^h \left(w' \prod_{j \in \mathcal{W}} w_j \right)^{r_m}, g^{r_v h}, g^{r_m} \right).\end{aligned}$$

- *Verification*. Given a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ of a signer ID on a message M, a verifier can compute $h = H_3(M || \sigma_3)$ to validate the signature tuple by the equation

$$\hat{e}(\sigma_1, g) = \hat{e}(g_2, g_1)^h \cdot \hat{e}\left(u' \prod_{i \in \mathcal{U}} u_i, \sigma_2 \right) \cdot \hat{e}\left(w' \prod_{j \in \mathcal{W}} w_j, \sigma_3 \right).$$

The algorithm outputs "accept" if the last equation holds, and "reject" otherwise.

In the following, we present the correctness of the equation in the *Verification algorithm* as follows.

$$\begin{aligned}
\hat{e}(\sigma_1, g) &= \hat{e}\left(\left(g_2^{\alpha}\left(u'\prod_{i\in\mathcal{U}} u_i\right)^{r_v}\right)^{h}\left(w'\prod_{j\in\mathcal{W}} w_j\right)^{r_m}, g\right) \\
&= \hat{e}\left(g_2^{\alpha h}, g\right)\cdot\hat{e}\left(\left(u'\prod_{i\in\mathcal{U}} u_i\right)^{r_v h}, g\right)\cdot\hat{e}\left(w'\prod_{j\in\mathcal{W}} w_j, g^{r_m}\right) \\
&= \hat{e}\left(g_2, g^{\alpha}\right)^{h}\cdot\hat{e}\left(u'\prod_{i\in\mathcal{U}} u_i, g^{r_v h}\right)\cdot\hat{e}\left(w'\prod_{j\in\mathcal{W}} w_j, g^{r_m}\right) \\
&= \hat{e}(g_2, g_1)^{h}\cdot\hat{e}\left(u'\prod_{i\in\mathcal{U}} u_i, \sigma_2\right)\cdot\hat{e}\left(w'\prod_{j\in\mathcal{W}} w_j, \sigma_3\right).
\end{aligned}$$

5. Security Analysis

Here, we give the security analysis for the proposed IBS scheme without random oracles. The security of our scheme is based on the CDH and CRH assumptions under which we show that the proposed strongly unforgeable IBS scheme possesses strong unforgeability against ID-SUF-ACMA attacks.

Theorem 1. *In the standard model* (*without random oracles*)*, the proposed IBS scheme possesses strong unforgeability against adaptive chosen-message attacks* (*ID-SUF-ACMA*) *under the CDH and CRH assumptions. Concretely, if there exists an adversary* $\mathcal{A}$ *who has an advantage* ϵ *against the proposed IBS scheme within a running time* τ*, where* $\mathcal{A}$ *can make at most* $q_E > 0$ *extract queries and* $q_S > 0$ *signing queries, then there is an algorithm* $\mathcal{B}$ *which has an advantage*

$$\epsilon' > \frac{\epsilon}{16q_S(q_E+q_S)(m+1)(n+1)}$$

to solve the CDH problem or

$$\epsilon'' > \frac{\epsilon}{4}$$

to violate the CRH assumption within a running time

$$\tau' = \tau + O\big((m\cdot q_E + (m+n)q_S)\tau_1 + (q_E+q_S)\tau_2\big),$$

in which τ_1 *and* τ_2*, respectively, denote the executing time of a multiplication in* $\mathbb{G}_1$ *and an exponentiation in* $\mathbb{G}_1$.

Proof. Assume that an adversary $\mathcal{A}$ can break the proposed strongly unforgeable IBS scheme. In the following, we will construct a challenger $\mathcal{B}$ in the ID-SUF-ACMA game to solve the CDH problem or violate the CRH assumption. We assume that the challenger $\mathcal{B}$ is given $\langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, g, g^a, g^b \rangle$ as an instance of the CDH problem, where $a, b \in \mathbb{Z}_p^*$. The challenger $\mathcal{B}$ would like to compute g^{ab} or find a collision pair for the CRH assumption. $\mathcal{B}$ simulates the challenger in the ID-SUF-ACMA game as follows.

- *Setup*. The challenger $\mathcal{B}$ sets three collision-resistant hash functions, namely, $H_1 : \{0,1\}^* \to \{0,1\}^m$ and $H_2, H_3 : \{0,1\}^* \to \{0,1\}^n$, where m and n are fixed lengths. Note that the employed collision resistant hash functions are not viewed as random oracles in our security proofs. The challenger $\mathcal{B}$ sets $l_v = 2(q_E + q_S)$ and $l_m = 2q_S$, and randomly chooses two integers k_v and k_m, with $0 \leqslant k_v \leqslant m$ and $0 \leqslant k_m \leqslant n$. We assume that $l_v(m+1) < p$ and $l_m(n+1) < p$ for the given values of q_E, q_S, m and n. Let $v = H_1(ID) = (v_1, \ldots, v_m)$ be a bit string of length m representing ID. Let $\mathcal{U} \subset \{1, 2, \ldots, m\}$ be the set of index i such that $v_i = 1$, for $i = 1, 2, \ldots, m$. The challenger $\mathcal{B}$ performs the following steps to define two functions $F(v)$ and $J(v)$.

  (1) Randomly choose an integer $x' \in \mathbb{Z}_{l_v}$ and a vector $X = (x_i)$ of length m, where $x_i \in \mathbb{Z}_{l_v}$ for $i = 1, 2, \ldots, m$.
  (2) Randomly choose an integer $y' \in \mathbb{Z}_p$ and a vector $Y = (y_i)$ of length m, where $y_i \in \mathbb{Z}_p$ for $i = 1, 2, \ldots, m$.
  (3) Define $F(v) = -l_v k_v + x' + \sum_{i \in \mathcal{U}} x_i$ and $J(v) = y' + \sum_{i \in \mathcal{U}} y_i$.

  Let $vm = H_2(M) = (vm_1, \ldots, vm_n)$ be a bit string of length n representing M. Let $\mathcal{W} \subset \{1, 2, \ldots, n\}$ be the set of index j such that $vm_j = 1$, for $j = 1, 2, \ldots, n$. The challenger $\mathcal{B}$ performs the following steps to define two functions $K(vm)$ and $L(vm)$.

  (1) Randomly choose an integer c' and a vector $C = (c_j)$ of length n, where $c', c_j \in \mathbb{Z}_{l_m}$ for $j = 1, 2, \ldots, n$.
  (2) Randomly choose an integer $d' \in \mathbb{Z}_p$ and a vector $D = (d_j)$ of length n, where $d_j \in \mathbb{Z}_p$ for $j = 1, 2, \ldots, n$.
  (3) Define $K(vm) = -l_m k_m + c' + \sum_{j \in \mathcal{W}} c_j$ and $L(vm) = d' + \sum_{j \in \mathcal{W}} d_j$.

  Then, the challenger $\mathcal{B}$ sets $g_1 = g^a$, $g_2 = g^b$, $u' = g_2^{-l_v k_v + x'} g^{y'}$, $u_i = g_2^{x_i} g^{y_i}$, $w' = g_2^{-l_m k_m + c'} g^{d'}$ and $w_j = g_2^{c_j} g^{d_j}$, for $1 \leqslant i \leqslant m$ and $1 \leqslant j \leqslant n$.

  Finally, we list two useful relations to which will be referred in the sequel, namely,

$$u' \prod_{i \in \mathcal{U}} u_i = g_2^{F(v)} g^{J(v)} \quad \text{and} \quad w' \prod_{j \in \mathcal{W}} w_j = g_2^{K(vm)} g^{L(vm)}. \tag{5.1}$$

- *Queries*. $\mathcal{B}$ responds the *extract query*, and the *signing query*, respectively, as follows.
  – *Extract query* (ID). Upon receiving the query along with identity ID, the challenger $\mathcal{B}$ sets $v = H_1(ID)$, and then computes $F(v)$ and $J(v)$. If $F(v) = 0 \bmod p$,

the challenger $\mathcal{B}$ reports failure and terminates. If $F(v) \neq 0 \bmod p$, the challenger $\mathcal{B}$ chooses a random $r_v \in \mathbb{Z}_p^*$ and computes the initial secret key D_{ID} as follows:

$$D_{ID} = (D_1, D_2) = \left(g_1^{\frac{-J(v)}{F(v)}} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v}, g_1^{\frac{-1}{F(v)}} g^{r_v} \right).$$

Here, $D_{ID} = (D_1, D_2)$ is indeed a valid private key since, by the first equality in (5.1),

$$\begin{aligned} D_1 &= \left(g^a\right)^{\frac{-J(v)}{F(v)}} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{\frac{a}{F(v)}} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v - \frac{a}{F(v)}} \\ &= \left(g^a\right)^{\frac{-J(v)}{F(v)}} \left(g_2^{F(v)} g^{J(v)}\right)^{\frac{a}{F(v)}} \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v - \frac{a}{F(v)}} \\ &= g_2^a \left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v'}, \\ D_2 &= \left(g^a\right)^{\frac{-1}{F(v)}} g^{r_v} = g^{r_v - \frac{a}{F(v)}} = g^{r_v'}, \end{aligned}$$

where $r_v' = r_v - \frac{a}{F(v)}$.

– *Signing query* (ID, M). Upon receiving the query along with (ID, M), the challenger $\mathcal{B}$ sets $v = H_1(ID)$ and then computes $F(v)$ and $J(v)$. Here, we consider two cases.

Case 1: If $F(v) \neq 0 \bmod l_v$, the challenger $\mathcal{B}$ can construct the private key for $v = H_1(ID)$ as in the *extract query*, and then use the *Signing algorithm* to respond a signature σ on M.

Case 2: If $F(v) = 0 \bmod l_v$, the challenger $\mathcal{B}$ sets $vm = H_2(M)$ and then computes $K(vm)$.

Case 2.1: If $K(vm) = 0 \bmod l_m$, the challenger $\mathcal{B}$ reports failure and terminates.

Case 2.2: If $K(vm) \neq 0 \bmod p$, the challenger $\mathcal{B}$ chooses two random values $r_v, r_m \in \mathbb{Z}_p^*$ and then computes $h = H_3(M || g^{r_m})$. Finally, the challenger $\mathcal{B}$ responds with a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ on M, where

$$\begin{aligned} \sigma_1 &= \left(\left(u' \prod_{i \in \mathcal{U}} u_i \right)^{r_v} \right)^h \cdot g_1^{\frac{-L(vm) \cdot h}{K(vm)}} \cdot \left(w' \prod_{j \in \mathcal{W}} w_j \right)^{r_m}, \\ \sigma_2 &= \left(g^{r_v}\right)^h, \\ \sigma_3 &= g_1^{\frac{-h}{K(vm)}} \cdot g^{r_m}. \end{aligned}$$

Here, $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is indeed a valid signature since, by the second equality in (5.1),

$$\begin{aligned}
\sigma_1 &= \left(\left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_v}\right)^h \cdot \left(g^a\right)^{\frac{-L(vm)\cdot h}{K(vm)}} \cdot \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{r_m} \\
&= \left(g_2^a \left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_v}\right)^h \cdot \left(g_2^{K(vm)} g^{L(vm)}\right)^{\frac{-ah}{K(vm)}} \cdot \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{r_m} \\
&= \left(g_2^a \left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_v}\right)^h \cdot \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{\frac{-ah}{K(vm)}} \cdot \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{r_m} \\
&= \left(g_2^a \left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_v}\right)^h \cdot \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{r'_m}, \\
\sigma_2 &= \left(g^{r_v}\right)^h, \\
\sigma_3 &= \left(g^a\right)^{\frac{-h}{K(vm)}} \cdot g^{r_m} = g^{r'_m},
\end{aligned}$$

where $r'_m = r_m - \frac{ah}{K(vm)}$.

- *Forgery*. Assume that the adversary $\mathcal{A}$ generates a valid signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ for ID^* on M^*, where ID^* and M^* are the target identity and message, respectively. We discuss two cases.

  Case 1: If (ID^*, M^*) did not appear in the *signing query*, the challenger $\mathcal{B}$ generates $v^* = H_1(ID^*)$ and $vm^* = H_2(M^*)$. If $F(v^*) \neq 0 \bmod p$ or $K(vm^*) \neq 0 \bmod p$, the challenger $\mathcal{B}$ reports failure and terminates. If $F(v^*) = 0 \bmod p$ and $K(vm^*) = 0 \bmod p$, the challenger $\mathcal{B}$ computes $h = H_3(M \| \sigma_3^*)$, and outputs g^{ab} as follows.

$$\begin{aligned}
\left(\frac{\sigma_1^*}{(\sigma_2^*)^{J(v^*)}(\sigma_3^*)^{L(vm^*)}}\right)^{\frac{1}{h}} &= \frac{g_2^a \left(u' \prod_{i \in \mathcal{U}} u_i\right)^{r_v} \left(w' \prod_{j \in \mathcal{W}} w_j\right)^{r_m \cdot \frac{1}{h}}}{g^{r_v J(v^*)} \cdot g^{r_m L(vm^*) \cdot \frac{1}{h}}} \\
&= \frac{g_2^a (g_2^{F(v^*)} g^{J(v^*)})^{r_v} (g_2^{K(vm^*)} g^{L(vm^*)})^{r_m \cdot \frac{1}{h}}}{g^{r_v \cdot J(v^*)} \cdot g^{r_m \cdot L(vm^*) \cdot \frac{1}{h}}} \\
&= g_2^a \quad \left(\text{since } F\left(v^*\right) = K\left(vm^*\right) = 0 \bmod p\right) \\
&= g^{ab}.
\end{aligned}$$

  This resolves the CDH problem.

  Case 2: If (ID^*, M^*) has appeared in the *signing query*, the adversary $\mathcal{A}$ owned a previously queried signature $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ of ID^* on M^*. If $\sigma_2 \neq \sigma_2^*$, the challenger $\mathcal{B}$ is able to output g^{ab} as in Case 1. Otherwise, if $\sigma_2 = \sigma_2^*$, then, since $\sigma_2^* = g^{r_v h^*}$ and $\sigma_2 = g^{r_v h}$, we have $h^* = h$, namely,

$$H_3\left(M \| g^{r_m^*}\right) = H_3\left(M \| g^{r_m}\right),$$

where $\sigma_3^* = g^{r_m^*}$ and $\sigma_3 = g^{r_m}$. This causes a collision of H_3 which violates the CRH assumption.

Next, we proceed to the probability analysis for the simulation above. For convenience, we list the events that challenger $\mathcal{B}$ does not abort during the simulation process.

(1) In the phase of *extract query*: if $F(v) \neq 0 \bmod p$, the challenger $\mathcal{B}$ can correctly answer queries without aborting.
(2) In the phase of *signing query*: if $K(vm) \neq 0 \bmod p$, the challenger $\mathcal{B}$ can correctly respond queries without aborting.
(3) In the phase of *forgery*: if $F(v^*) = K(vm^*) = 0 \bmod p$, the challenger $\mathcal{B}$ can perform the simulation without aborting.

By the previous assumptions $l_v(m+1) < p$ and $l_m(n+1) < p$, we have $0 \leqslant l_v k_v \leqslant p$, $0 \leqslant x' + \sum_{i \in \mathcal{U}} x_i \leqslant p$, $0 \leqslant l_m k_m \leqslant p$ and $0 \leqslant c' + \sum_{j \in \mathcal{W}} c_j \leqslant p$. Hence, $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$ and $K(vm) = 0 \bmod p$ implies $K(vm) = 0 \bmod l_m$.

Let q_I be the number of identities appearing in *extract queries* or *signing queries* not involving the challenge identity. Let q_M be the number of messages in the *signing queries* involving the challenge identity. Clearly, we will have $q_I < q_E + q_S$ and $q_M < q_S$. To simplify the analysis, we define the events A_i: $F(v) \neq 0 \bmod l_v$ for the ith query $(1 \leqslant i \leqslant q_I)$; A^*: $F(v^*) = 0 \bmod p$; B_j: $K(vm) \neq 0 \bmod l_m$ for the jth query $(1 \leqslant j \leqslant q_M)$; B^*: $K(vm^*) = 0 \bmod p$. Hence, the probability of the challenger $\mathcal{B}$ not aborting in Cases 1 and 2, respectively, of *Forgery* phase are

$$\begin{aligned}
\Pr[\neg\text{abortCase1}] &\geqslant \Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{j=1}^{q_M} B_j \wedge B^*\right] \\
&= \Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] \cdot \Pr\left[\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right], \\
\Pr[\neg\text{abortCase2}] &\geqslant \Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge \bigwedge_{j=1}^{q_M} B_j\right] \\
&= \Pr\left[\bigwedge_{i=1}^{q_I} A_i\right] \cdot \Pr\left[\bigwedge_{j=1}^{q_M} B_j\right].
\end{aligned}$$

To compute $\Pr[A^*]$, note that $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$. On the other hand, if $F(v) = 0 \bmod l_v$, there exists a unique choice of k_v with $0 \leqslant k_v \leqslant m$ such that $F(v) = 0 \bmod p$. Since k_v, x' and X are chosen randomly, we have the probability of the event A^* as follows.

$$\begin{aligned}
\Pr\left[A^*\right] &= \Pr\left[F\left(v^*\right) = 0 \bmod p\right] \\
&\geqslant \Pr\left[F(v^*) = 0 \bmod p \wedge F\left(v^*\right) = 0 \bmod l_v\right]
\end{aligned}$$

$$= \Pr\left[F\left(v^*\right) = 0 \bmod l_v\right] \cdot \Pr\left[F\left(v^*\right) = 0 \bmod p \middle| F\left(v^*\right) = 0 \bmod l_v\right]$$
$$= \frac{1}{l_v}\frac{1}{m+1}.$$

By similar arguments, we have

$$\begin{aligned}\Pr\left[B^*\right] &= \Pr\left[K\left(vm^*\right) = 0 \bmod p\right] \\ &\geqslant \Pr\left[K\left(vm^*\right) = 0 \bmod p \wedge K\left(vm^*\right) = 0 \bmod l_m\right] \\ &= \Pr\left[K\left(vm^*\right) = 0 \bmod l_m\right] \cdot \Pr\left[K\left(vm^*\right) = 0 \bmod p \middle| K\left(vm^*\right) = 0 \bmod l_m\right] \\ &= \frac{1}{l_m}\frac{1}{n+1}.\end{aligned}$$

We then have that

$$\begin{aligned}\Pr\left[\bigwedge_{i=1}^{q_I} A_i \middle| A^*\right] &= 1 - \Pr\left[\bigvee_{i=1}^{q_I} \neg A_i \middle| A^*\right] \geqslant 1 - \sum_{i=1}^{q_I} \Pr\left[\neg A_i \middle| A^*\right] \\ &= 1 - \frac{q_I}{l_v} \geqslant 1 - \frac{q_E + q_S}{l_v}, \\ \Pr\left[\bigwedge_{j=1}^{q_M} B_j \middle| B^*\right] &= 1 - \Pr\left[\bigvee_{j=1}^{q_M} \neg B_j \middle| B^*\right] \geqslant 1 - \sum_{j=1}^{q_M} \Pr\left[\neg B_j \middle| B^*\right] \\ &= 1 - \frac{q_M}{l_m} \geqslant 1 - \frac{q_S}{l_m}.\end{aligned}$$

Hence, we obtain

$$\Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] = \Pr\left[A^*\right] \cdot \Pr\left[\bigwedge_{i=1}^{q_I} A_i \middle| A^*\right] \geqslant \left(\frac{1}{l_v}\frac{1}{m+1}\right) \cdot \left(1 - \frac{q_E + q_S}{l_v}\right),$$
$$\Pr\left[\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right] = \Pr\left[B^*\right] \cdot \Pr\left[\bigwedge_{j=1}^{q_M} B_j \middle| B^*\right] \geqslant \left(\frac{1}{l_m}\frac{1}{n+1}\right) \cdot \left(1 - \frac{q_S}{l_m}\right),$$
$$\Pr\left[\bigwedge_{i=1}^{q_I} A_i\right] \geqslant 1 - \frac{q_E + q_S}{l_v},$$
$$\Pr\left[\bigwedge_{j=1}^{q_M} B_j\right] \geqslant 1 - \frac{q_S}{l_m},$$

where the last two inequalities follow from the fact that $\Pr[\bigwedge_{i=1}^{q_I} A_i] = \Pr[\bigwedge_{i=1}^{q_I} A_i | A^*]$ and $\Pr[\bigwedge_{j=1}^{q_M} B_j] = \Pr[\bigwedge_{j=1}^{q_M} B_j | B^*]$.

Since we have set $l_v = 2(q_E + q_S)$ and $l_m = 2q_S$, the resulting probability of the challenger $\mathcal{B}$ not aborting in Cases 1 and 2, respectively, of *Forgery* phase are

$$\begin{aligned}
\Pr[\neg\text{abortCase1}] &\geqslant \Pr\left[\bigwedge_{i=1}^{q_I} A_i \wedge A^*\right] \cdot \Pr\left[\bigwedge_{j=1}^{q_M} B_j \wedge B^*\right] \\
&\geqslant \frac{1}{16q_S(q_E + q_S)(m+1)(n+1)}, \\
\Pr[\neg\text{abortCase2}] &\geqslant \Pr\left[\bigwedge_{i=1}^{q_I} A_i\right] \cdot \Pr\left[\bigwedge_{j=1}^{q_M} B_j\right] \\
&\geqslant \frac{1}{4}.
\end{aligned}$$

Since the adversary $\mathcal{A}$ that has an advantage ϵ against the proposed strongly unforgeable IBS scheme, the challenger $\mathcal{B}$ has an advantage

$$\epsilon' > \frac{\epsilon}{16q_S(q_E + q_S)(m+1)(n+1)}$$

to solve the CDH problem or

$$\epsilon'' > \frac{\epsilon}{4}$$

to violate the CRH assumption.

According to the descriptions above, the challenger $\mathcal{B}$ requires $O(m)$ multiplications and $O(1)$ exponentiations in the *extract queries* as well as $O(m+n)$ multiplications and $O(1)$ exponentiations in the *signing queries*. So we have $\tau' = \tau + O((m \cdot q_E + (m + n)q_S)\tau_1 + (q_E + q_S)\tau_2)$, where τ_1 and τ_2 denote the executing time of a multiplication in $\mathbb{G}_1$ and an exponentiation in $\mathbb{G}_1$, respectively. □

6. Comparisons

Here, we compare our scheme with the IBS scheme proposed by Paterson and Schuldt (2006), the transformed strongly unforgeable IBS scheme proposed by Huang *et al*. (2007) and the strongly unforgeable IBS scheme proposed by Sato *et al*. (2009, 2010). Note that Huang *et al*. (2007) converted an existentially unforgeable IBS scheme (Paterson and Schuldt, 2006) into a strongly unforgeable one by attaching a strong onetime signature (Zhang *et al*., 2006; Boneh *et al*., 2006).

Table 1 lists the comparisons between the IBS schemes of Paterson and Schuldt, Huang *et al.*, Sato *et al.* and ours in terms of computational cost, signature size, security property and security assumption, where $|\mathbb{G}_1|$ denotes the bit length of the group $\mathbb{G}_1$. It is known that a pairing operation is more time-consuming than other kinds of operations. All the IBS

Table 1
Comparisons between our scheme and the previously proposed IBS schemes.

	Paterson and Schuldt's IBS scheme (2006)	Huang *et al.*'s transformed IBS scheme (2007)	Sato *et al.*'s IBS scheme (2009, 2010)	Our proposed IBS scheme
Pairing operation for signing	0	0	0	0
Pairing operation for verification	4	5	6	4
Signature size	$3\|\mathbb{G}_1\|$	$7\|\mathbb{G}_1\|$	$5\|\mathbb{G}_1\|$	$3\|\mathbb{G}_1\|$
Security property	Existential unforgeability	Strong unforgeability	Strong unforgeability	Strong unforgeability
Security assumption	CDH assumption	CDH assumption	vDH assumption and OWI function	CDH and CRH assumptions

schemes above require no pairing operation to sign a message. For the computational cost of the verification phase and the signature size, our scheme is better than others, except for Paterson and Schuldt's scheme which, however, possesses only existential unforgeability.

Under the CDH assumption, Paterson and Schuldt as well as Huang *et al.* demonstrated that their IBS schemes possess existential unforgeability against adaptive chosen-message attacks, respectively. Sato *et al.*'s strongly unforgeable IBS scheme is proven to be secure against adaptive chosen-message attacks under three variances related to the Diffie–Hellman (for short, vDH) assumption and one-way isomorphism (for short, OWI) function. In the previous section, under the CDH and CRH assumptions, we have demonstrated that our scheme possesses strong unforgeability against adaptive chosen-message attacks (ID-SUF-ACMA).

It is worth mentioning that Sato *et al.*'s scheme and ours are modified from Paterson and Schuldt's scheme. Sato *et al.*'s scheme requires five signature parameters and six pairing operations for the verification phase. Our proposed IBS scheme requires only three signature parameters and four pairing operations.

7. Conclusions

In this paper, we have proposed an efficient strongly unforgeable IBS scheme without random oracles. Comparisons were made to demonstrate that the proposed strongly unforgeable IBS scheme has better performance in terms of signature size and computation cost. For the security analysis, we demonstrated that the proposed strongly unforgeable IBS scheme possesses strong unforgeability against adaptive chosen-message attacks under the CDH and CRH assumptions.

Acknowledgements. The authors would like to thank the referees for their invaluable comments and constructive suggestions. This research was partially supported by National Science Council, Taiwan, R.O.C., under contract No. NSC101-2221-E-018-027.

References

Bellare, M., Namprempre, C., Neven, G. (2004). Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 22(1), 1–61.

Bellare, M., Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. In: *Proceedings of ACM CCS'93*, pp. 62–73.

Boneh, D., Boyen, X. (2004). Short signatures without random oracles. In: *Proceedings of Eurocrypt'04*, LNCS, Vol. 3027, pp. 56–73.

Boneh, D., Franklin, M. (2001). Identity-based encryption from the Weil pairing. In: *Proceedings of Crypto'01*, LNCS, Vol. 2139, pp. 213–229.

Boneh, D., Hamburg, M. (2008). Generalized identity based and broadcast encryption schemes. In: *Proceedings of Asiacrypt'08*, LNCS, Vol. 5350, pp. 455–470.

Boneh, D., Shen, E., Waters, B. (2006). Strongly unforgeable signatures based on computational Diffie–Hellman. In: *Proceedings of PKC'06*, LNCS, Vol. 3958, pp. 229–240.

Boyd, C., Choo, K.K. (2005). Security of two-party identity-based key agreement. In: *Proceedings of Mycrypt 2005*, LNCS, Vol. 3715, pp. 229–243.

Camenisch, J., Lysyanskaya, A. (2004). Signature schemes and anonymous credentials from bilinear maps. In: *Proceedings of Crypto'04*, LNCS, Vol. 3152, pp. 56–72.

Cha, J.C., Cheon, J.H. (2003). An identity-based signature from gap Diffie–Hellman groups. In: *Proceedings of PKC'03*, LNCS, Vol. 2567, pp. 18–30.

Chen, L., Cheng, Z., Smart, N.P. (2007). Identity-based key agreement protocols from pairings. *International Journal of Information Security*, 6(4), 213–241.

Choi, K.Y., Hwang, J.Y., Lee, D.H. (2008). ID-based authenticated group key agreement secure against insider attacks. *IEICE Transactions on Fundamentals*, E91-A(7), 1828–1830.

Chow, S.M., Choo, K.K. (2007). Strongly-secure identity-based key agreement and anonymous extension. In: *Proceedings of ISC 2007*, LNCS, Vol. 4779, pp. 203–220.

Damgard, I. (1987). Collision free hash functions and public key signature schemes. In: *Proceedings of Eurocrypt'87*, LNCS, Vol. 304, pp. 203–216.

Dodis, Y., Katz, J., Xu, S., Yung, M. (2003). Strong key-insulated signature schemes. In: *Proceedings of PKC'02*, LNCS, Vol. 2567, pp. 130–144.

Galindo, D., Herranz, J., Kiltz, E. (2006). On the generic construction of identity-based signatures with additional properties. In: *Proceedings of Asiacrypt'06*, LNCS, Vol. 4284, pp. 178–193.

Goldwasser, S., Micali, S., Riverst, R. (1988). A digital signature scheme secure against adaptive chosen message attacks. *SIAM Journal of Computing*, 17(2), 281–308.

Huang, Q., Wong, D.S., Zhao, Y. (2007). Generic transformation to strongly unforgeable signatures. In: *Proceedings of ACNS'07*, LNCS, Vol. 4521, pp. 1–17.

Narayan, S., Parampalli, U. (2008). Efficient identity-based signatures secure in the standard model. *IET Information Security*, 2(4), 108–118.

Paterson, K.G. (2002). Identity-based signatures from pairings on elliptic curves. *Electronics Letters*, 38(9), 1025–1026.

Paterson, K.G., Schuldt, J.C.N. (2006). Efficient identity-based signatures secure in the standard model. In: *Proceedings of ACISP'06*, LNCS, Vol. 4058, pp. 207–222.

Sato, C., Okamoto, T., Okamoto, E. (2009). Strongly unforgeable ID-based signatures without random oracles. In: *Proceedings of ISPEC'09*, LNCS, Vol. 5451, pp. 35–46.

Sato, C., Okamoto, T., Okamoto, E. (2010). Strongly unforgeable ID-based signatures without random oracles. *International Journal of Applied Cryptography*, 2(1), 35–45.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In: *Proceedings of Crypto'84*, LNCS, Vol. 196, pp. 47–53.

Shim, K.A. (2010). An ID-based aggregate signature scheme with constant pairing computations. *Journal of Systems and Software*, 83(10), 1873–1880.

Tsai, T.T., Tseng, Y.M., Wu, T.Y. (2012). A fully secure revocable ID-based encryption in the standard model. *Informatica*, 23(3), 481–499.

Tseng, Y.M., Tsai, T.T. (2012). Efficient revocable ID-based encryption with a public channel. *The Computer Journal*, 55(4), 475–486.

Tseng, Y.M., Wu, T.Y., Wu, J.D. (2008). A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 19 (2), 285–302.

Tseng, Y.M., Wu, T.Y., Wu, J.D. (2009). An efficient and provably secure ID-based signature scheme with batch verifications. *International Journal of Innovative Computing, Information and Control*, 5(11), 3911–3922.

Wang, X.A., Yang, X., Zhang, M., Yu, Y. (2012). Cryptanalysis of a fuzzy identity based encryption scheme in the standard model. *Informatica*, 23(2), 299–314.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In: *Proceedings of Eurocrypt'05*, Vol. 3494, pp. 1–33.

Wu, T.Y., Tseng, Y.M. (2010). An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, 53(7), 1062–1070.

Wu, T.Y., Tseng, Y.M. (2012). Towards ID-based authenticated group key exchange protocol with identifying malicious participants. *Informatica*, 23(2), 315–334,

Wu, T.Y., Tseng, Y.M., Yu, C.W. (2011). A secure ID-based authenticated group key exchange protocol resistant to insider attacks. *Journal of Information Science and Engineering*, 27(3), 915–932.

Yoon, H.J., Cheon, J.H., Kim, Y. (2004). Batch verifications with ID-based signatures. In: *Proceedings of ICISC'04*, pp. 233–248.

Zhang, F., Chen, X., Susilo, W., Mu, Y. (2006). A new signature scheme without random oracles from bilinear pairings. In: *Proceedings of Vietcrypt'06*, LNCS, Vol. 4341, pp. 67–80.

T.-T. Tsai received the BS degree from the Department of Applied Mathematics, Chinese Culture University, Taiwan, in 2006. He received the MS degree from the Department of Applied Mathematics, National Hsinchu University of Education, Taiwan, in 2009. He is currently a PhD candidate in the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include applied cryptography and pairing-based cryptography.

Y.-M. Tseng is currently a Professor in the Department of Mathematics, National Changhua University of Education, Taiwan. He is a member of IEEE Computer Society, IEEE Communications Society and the Chinese Cryptology and Information Security Association (CCISA). In 2006, his paper received the Wilkes Award from The British Computer Society. He has published over one hundred scientific journal and conference papers on various research areas of cryptography, security and computer network. His research interests include cryptography, network security, computer network and mobile communications. He serves as an editor of several international journals.

S.-S. Huang is currently a Professor in the Department of Mathematics, National Changhua University of Education, Taiwan. His research interests include number theory, cryptography, and network security. He received his PhD from the University of Illinois at Urbana-Champaign in 1997 under the supervision of Professor Bruce C. Berndt.

Efektyvus ypač nesuklastojamas ID pagrįstas parašas nenaudojantis juodosios dėžės modelio

Tung-Tso TSAI, Yuh-Min TSENG, Sen-Shan HUANG

Pasiūlyta daug identifikatoriumi (ID) pagrįstų schemų (IBS), kuriose naudojama bitiesinio poravimo metodas. Dauguma šių schemų užtikrina parašo nesuklastojamumą esant adaptyvioms pasirinkto pranešimo atakoms. Ypač nesuklastojamos IBS schemos gali būti naudojamos konstruojant svarbias ID pagrįstas kriptografines sistemas. Tačiau egzistuojančios IBS schemos yra neefektyvios parašo dydžio ir skaičiavimų sudėtingumo parašo patikrinimo fazėje prasmėmis. Šiame straipsnyje siūloma efektyvi ypač nesuklastojamo parašo schema IBS, nenaudojanti juodosios dėžės (Random Oracle) modelio. Parodyta, kad pasiūlyta IBS schema yra ypač nesuklastojama esant adaptyvioms pasirinkto pranešimo atakoms. Palyginus su anksčiau pasiūlytomis schemomis, ši schema yra kokybiškesnė parašo dydžio ir skaičiavimų sudėtingumo prasmėmis.