ISSN 1392–124X (print), ISSN 2335–884X (online) INFORMATION TECHNOLOGY AND CONTROL, 2014, T. 43, Nr. 3

# Strongly Secure Revocable ID-based Signature without Random Oracles

**Ying-Hao Hung, Tung-Tso Tsai, Yuh-Min Tseng*, Sen-Shan Huang**

*Department of Mathematics, National Changhua University of Education,*
*Jin-De Campus, Chang-Hua 500, Taiwan, R.O.C.*
*e-mail: ymtseng@cc.ncue.edu.tw*

crossref http://dx.doi.org/10.5755/j01.itc.43.3.5718

**Abstract**. In 2012, Tseng and Tsai presented a novel revocable ID (identity)-based public key setting that provides an efficient revocation mechanism with a public channel to revoke misbehaving or compromised users from public key systems. Subsequently, based on Tseng and Tsai's revocable ID-based public key setting, Tsai *et al*. proposed a new revocable ID-based signature (RIBS) scheme in the standard model (without random oracles). However, their RIBS scheme possesses only existential unforgeability under adaptive chosen-message attacks. In the article, we propose the first strongly secure RIBS scheme without random oracles under the computational Diffie-Hellman and collision resistant assumptions. Comparisons with previously proposed schemes are made to demonstrate the advantages of our scheme in terms of revocable functionality and security property.

**Keywords**: strong unforgeability; revocation; identity-based signature; standard model.

## 1. Introduction

Digital signature, one important cryptographic primitive, provides the integrity, authentication and non-repudiation of messages. In traditional public key systems, before verifying a signature, a user must obtain the corresponding authenticated public key (i.e. certificate) from public directories. In such a case, efficient public key management becomes an important issue. In 1984, to simplify public key management, Shamir [1] introduced the concept of identity (ID)-based cryptography (IBC), in which a user's public key is determined by his/her identity information such as social security number, e-mail address, telephone number, name, etc. Moreover, a trusted third party, called private key generator (PKG), is responsible to produce private keys which are distributed to users via secure channels. As opposed to traditional public key systems, IBC eliminates the requirement of certificates. Shamir's system was ingenious but not practical, however. In 2001, Boneh and Franklin [2] adopted Shamir's idea to propose a new ID-based public key system and the first practical ID-based encryption (IBE) based on modification of bilinear pairings defined on elliptic curves. Since then, a numerous primitives for IBC have been published such as ID-based authentication protocols [3-5], ID-based key agreement protocols [6-8], ID-based signature schemes [9-13] and ID-based encryption schemes [14-17].

In 2002, according to Boneh and Franklin's ID-based public key setting [2], Paterson [18] proposed an ID-based signature (IBS) scheme by making use of bilinear pairings. Later, Cha and Cheon [10] proposed a new IBS scheme that improved Paterson's scheme on both efficiency of computation and signature size while the security of their scheme was based on the gap Diffie-Hellman assumption. In 2009, Tseng *et al.* [19] and Shim [20], independently, proposed efficient IBS schemes that are provably secure and support variant kinds of batch verifications. Both schemes significantly improve the verification performance for many cooperative and distributed applications. The four IBS schemes mentioned above have been shown to be secure in the random oracle model. However, when random oracles are instantiated with concrete hash functions, those IBS schemes could be insecure. In 2006, to overcome this problem, Paterson and Schuldt [9] proposed an IBS scheme without random oracles which is computationally efficient and has short signature size. In 2008, Narayan et al. [21] further improved Paterson and Schuldt's scheme by reducing the size of the public parameters.

All the IBS schemes mentioned above possess existentially unforgeable under adaptive chosen-message attacks, but not strongly unforgeable. An IBS scheme is said to be strongly unforgeable if it is existentially unforgeable and an adversary who is given

[*] Corresponding author

signatures of the IBS scheme on some message $m$ is unable to generate a new signature on $m$. Strong unforgeability ensures that an adversary cannot generate a new signature for a previously signed message. Therefore, strongly unforgeable IBS schemes are important for constructing ID-based cryptographic schemes such as chosen-ciphertext secure ID-based cryptosystems and ID-based group signatures. In the past, several strongly unforgeable non-ID-based signature schemes [22-25] without random oracles have been proposed. Furthermore, the work in [26-28] provided several transformation methods to construct strongly unforgeable IBS schemes out of strongly unforgeable non-ID-based signature schemes. Recently, without applying any transformation ways, Sato *et al.* [29] proposed a strongly unforgeable IBS scheme without random oracles based on Paterson and Schuldt's IBS scheme [9]. Their scheme offered better performance in terms of signature size and computation cost when compared with the schemes in [26-28].

A public key system construction must provide a revocation mechanism to revoke misbehaving or compromised users from the system. In 2001, Boneh and Franklin [22] presented a revocation mechanism for ID-based public key systems, in which the PKG generates and sends new private keys for non-revoked users periodically. To do so, the PKG must establish a secure channel with each non-revoked user to transmit the new private key. The key update size is equal to the number of non-revoked users. Boldyreva *et al.* [30] applied a binary tree structure to construct a revocable ID-based encryption (RIBE) which reduces the key update size to the logarithm of the number of users. However, both revocation methods mentioned above need secure channels to transmit the users' new private keys periodically. This causes enormous computational load for both of encryption and decryption procedures.

In order to resolve the "secure channel" problem above, Tseng and Tsai [31] proposed a new RIBE scheme and offered a practical revocation mechanism with a "public channel". In their scheme, the PKG and non-revoked users can significantly reduce computational burden due to the absence of encryption/decryption via secure channels. Subsequently, based on Tseng and Tsai's revocable ID-based public key setting, Sun *et al.* [32] proposed a revocable ID-based signature (RIBS) scheme in the random oracle model. Although the scheme [32] based on the random oracle model can offer better performance, the resulting scheme could be insecure when random oracles are instantiated with concrete hash functions [33, 34]. Furthermore, Tsai *et al.* [12] proposed the first RIBS scheme in the standard model (without random oracles). However, their RIBS scheme possesses only existential unforgeability under adaptive chosen-message attacks. In this article, we first present a new framework and security notions for strongly unforgeable RIBS schemes with revocation via public channels. We then propose the first strongly unforgeable RIBS scheme without random oracles. Under the computational Diffie–Hellman and collision resistant assumptions, we demonstrate that our RIBS scheme possesses strong unforgeability under adaptive chosen-message attacks. When compared with previously proposed IBS and RIBS schemes without random oracles, our scheme provides better performance in terms of computational cost and revocable functionality while possessing strong unforgeability.

The remainder of the article is organized as follows. Preliminaries are given in Section 2. In Section 3, we present the framework and security notions for strongly unforgeable RIBS schemes. Section 4 presents our concrete scheme. In Section 5, we analyze the security of our scheme. Comparisons are presented in Section 6. Conclusions are given in Section 7.

## 2. Preliminaries

In the section, we will briefly review some properties of bilinear pairings. We also introduce the computational Diffie-Hellman (CDH) and collision resistant (CRH) assumptions.

### 2.1. Bilinear pairings

Let $G_1$ and $G_2$ be two multiplicative cyclic groups of large prime order $p$. Let $g$ be a generator of $G_1$. A mapping $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ is an admissible bilinear map if it satisfies the following properties:

1. Bilinearity: For every $g^a, g^b \in G_1$, $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$, where $a, b \in Z_p^*$.
2. Non-degeneracy: $\hat{e}(g, g) \neq 1$.
3. Computability: There exists an efficient algorithm to compute the value $\hat{e}(g^a, g^b)$.

### 2.2. Security assumptions

Two hard problems and their corresponding assumptions are presented here.

**Definition 1** (Computational Diffie-Hellman (CDH) Problem and Assumption). Let $G_1$ be a cyclic multiplicative group of large prime order $p$ with generator $g$. Given $g^a, g^b \in G_1$ with unknown $a, b \in Z_p^*$, the computational Diffie-Hellman (CDH) problem in $G_1$ is to compute $g^{ab}$. We say that the $(\varepsilon, t)$-CDH assumption holds in the group $G_1$ if no polynomial-time adversary $\mathcal{A}$ can solve the CDH problem in $G_1$ with non-negligible probability $\varepsilon$ within time $t$. Here, the successful probability (advantage) of the adversary $\mathcal{A}$ is presented as

$$\Pr[\mathcal{A}(g, g^a, g^b) = g^{ab}],$$

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

**Definition 2.** Collision-resistant hash (CRH) assumption. Let $H_k$:$\{0, 1\}^* \rightarrow \{0, 1\}^n$ be a collision-resistant hash family of functions, where $n$ is a fixed length and $k$ is an index. We say that the $(\varepsilon,t)$-CRH assumption holds if no polynomial-time adversary $\mathcal{A}$

running in time at most $t$ can break the collision-resistance of $H_k$ with probability $\varepsilon$. Here, the successful probability (advantage) of the adversary $\mathcal{A}$ is presented as

$$\Pr[\mathcal{A}(k) = (m_0, m_1) : m_0 \neq m_1, H_k(m_0) = H_k(m_1)],$$

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

**Remark 1.** In this paper, we use collision resistant hash (CRH) functions to construct our RIBS scheme, in which the CRH functions can be easily constructed based on the CDH assumption [23].

## 3. Framework and security notions of strongly unforgeable RIBS

In this section, we present the framework and security notion for strongly unforgeable RIBS schemes. The framework of strongly unforgeable RIBS schemes is identical to that of Tsai *et al.*'s RIBS scheme [12]. We also define a new security notion for strongly unforgeable RIBS schemes based on the notions in [9, 21, 28, 29].

**Definition 3.** A strongly secure RIBS scheme consists of five algorithms:

- *Setup algorithm* $\mathcal{G}$ is a probabilistic algorithm run by the PKG that takes as input a security parameter $\delta$ and the total number $z$ of all periods, and outputs a system secret key $s$ and public parameters *Parms*. The public parameters *Parms* are made public and the secret key $s$ is kept for the PKG itself.
- *Initial key extract algorithm* $\mathcal{IKE}$ is a deterministic algorithm run by the PKG that takes as input the system secret key $s$ and a user's identity *ID*, and returns the user's initial secret key $D_{ID}$.
- *Time key update algorithm* $\mathcal{TKU}$ is a deterministic algorithm run by the PKG that takes as input the system secret key $s$, a user's identity *ID* and a period $t$, and then returns the user's time update key $T_{ID,t}$. Then, the user can combine the initial secret key $D_{ID}$ and the time update key $T_{ID,t}$ to obtain the signing key $S_{ID,t}$.
- *Signing algorithm* $\mathcal{S}$ is a probabilistic algorithm that takes as input a period $t$, a user's signing key $S_{ID,t}$ and a message $M$, and returns a signature $\sigma$ on $M$.
- *Verification algorithm* $\mathcal{V}$ is a deterministic algorithm that takes as input a signature pair $(t, \sigma)$, a message $M$ and a user's identity *ID*, and outputs "accept" if $(t, \sigma)$ is a valid signature on the message $M$ for *ID*, and "reject" otherwise.

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

- *Setup*. The challenger $\mathcal{B}$ runs the setup algorithm $\mathcal{G}$ to generate a system secret key $s$ and public parameters *Parms*. The public parameters *Parms* are sent to the adversary $\mathcal{A}$ and the system secret key $s$ is kept by $\mathcal{B}$ itself.
- *Queries*. The adversary $\mathcal{A}$ performs the following queries adaptively:
    - *Initial key extract query* (*ID*). When $\mathcal{A}$ requests the initial secret key on an identity *ID*, the challenger $\mathcal{B}$ runs the initial key extract algorithm $\mathcal{IKE}$ to obtain $D_{ID}$ and returns it to the adversary $\mathcal{A}$.
    - *Time key update query* (*ID*, $t$). When $\mathcal{A}$ requests the time update key on (*ID*, $t$), the challenger $\mathcal{B}$ runs the time key update algorithm $\mathcal{TKU}$ to obtain the time update key $T_{ID,t}$ and returns it to the adversary $\mathcal{A}$.
    - *Signing queries* ($M$, *ID*, $t$). When $\mathcal{A}$ requests a signature on the message $M$ for an identity *ID* and a period $t$, the challenger $\mathcal{B}$ runs the initial key extract algorithm $\mathcal{IKE}$ and time key update algorithm $\mathcal{TKU}$ to obtain the user's signing key $S_{ID,t}$. Then $\mathcal{B}$ runs the signing algorithm $\mathcal{S}$ to generate a signature $\sigma$ on the message $M$ using $S_{ID,t}$ and returns $\sigma$ to $\mathcal{A}$.
- *Forgery*. We say that the adversary $\mathcal{A}$ wins the RID-SUF-ACMA game if $\mathcal{A}$ generates a tuple $(M^*, ID^*, t^*, \sigma^*)$ which satisfies the following conditions:
    1. The response of the verification algorithm $\mathcal{V}$ on $(M^*, ID^*, t^*, \sigma^*)$ is "accept".
    2. $\sigma^*$ has not been outputted in the signing query on $(M^*, ID^*, t^*)$.
    3. Either $ID^*$ or $(ID^*, t^*)$ has not appeared in the *initial key extract queries* or *the time key update queries*, respectively.

The adversary $\mathcal{A}$'s advantage is defined as the probability that $\mathcal{A}$ wins the RID-SUF-ACMA game.

**Remark 2.** An RIBS scheme is said to be strongly unforgeable if it is existentially unforgeable and an adversary who is given signatures of the RIBS scheme on some message $m$ is unable to generate a new signature on $m$. Strong unforgeability ensures that an adversary cannot generate a new signature for a previously signed message.

## 4. Strongly unforgeable RIBS scheme

In this section, we present a concrete strongly unforgeable RIBS scheme without random oracles that consists of the following algorithms:

- ***Setup***: Given a security parameter $\delta$ and the total number $z$ of all periods, the PKG chooses two cyclic groups $G_1$ and $G_2$ of sufficiently large prime order $p > 2^{\delta}$ . Let $g$ be a generator of $G_1$ and $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ be an admissible bilinear map. The PKG sets the system secret key and the public parameters by performing the following tasks.

  1. Select two secret values $\alpha, \beta \in Z_p^*$ at random and compute $g_1 = g^{\alpha+\beta} \in G_1$. Select a random $g_2 \in G_1$ and compute $g_2^{\alpha}$ and $g_2^{\beta}$.
  2. Set four collision-resistant hash functions $H_1$:$\{0, 1\}^* \rightarrow \{0, 1\}^m$, $H_2$:$\{0, 1\}^* \rightarrow \{0, 1\}^n$ and $H_3$, $H_4$:$\{0, 1\}^* \rightarrow \{0, 1\}^l$, where $m$, $n$ and $l$ are fixed lengths. Here, we assume $p > 2^m$, $p > 2^n$ and $p > 2^l$ so that the outputs of these hash functions can be directly viewed as elements of $Z_p$ without modulo $p$.
  3. Randomly choose three values $u'$, $t'$, $w' \in G_1$ and three vectors $U = (u_i)$, $T = (t_j)$, $W = (w_k)$, where $u_i$, $t_j$, $w_k \in G_1$ for $i = 1, 2,\ldots, m$, $j = 1, 2,\ldots, n$ and $k = 1, 2,\ldots, l$.

  Finally, the PKG sets the system secret key $s = (g_2^{\alpha}, g_2^{\beta})$ and the public parameters $Parms = <G_1, G_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, H_4, u', U, t', T, w', W>$.

- ***Initial key extract***: Given a user's identity $ID \in \{0, 1\}^*$, the PKG computes a string $v = H_1(ID)$ of length $m$. Let $v_i$ denote the $i$-th bit of the string $v$ and let $\mathcal{V} \subset \{1, 2,\ldots, m\}$ be the set of indices $i$ such that $v_i = 1$ for $i = 1, 2,\ldots, m$. Finally, the PKG chooses a random value $r_v \in Z_p^*$, computes the user's initial secret key $D_{ID} = (D_1, D_2) = (g_2^{\alpha} (u'\prod_{i\in\mathcal{V}} u_i)^{r_v}, g^{r_v})$ and sends $D_{ID}$ to the user via a secure channel.

- ***Time key update***: Given a user's identity $ID \in \{0,1\}^*$ and a period $t$, the PKG computes a string $vt = H_2(ID, t)$ of length $n$. Let $vt_j$ denote the $j$-th bit of the string $vt$ and let $\mathcal{T} \subset \{1, 2,\ldots, n\}$ be the set of indices $j$ such that $vt_j = 1$ for $j = 1, 2,\ldots, n$. Finally, the PKG chooses a random value $r_t \in Z_p^*$ and computes the user's time update key $T_{ID,t} = (T_1, T_2) = (g_2^{\beta} (t'\prod_{j\in\mathcal{T}} t_j)^{r_t}, g^{r_t})$. The PKG sends $T_{ID,t}$ to the user via a public channel. Upon receiving $T_{ID,t}$, the user combines it with his/her initial secret key $D_{ID} = (D_1, D_2)$ to generate the signing key $S_{ID,t} = (S_1, S_2, S_3) =(D_1T_1, D_2, T_2) =(g^{\alpha+\beta} (u'\prod_{i\in\mathcal{V}} u_i)^{r_v} (t'\prod_{j\in\mathcal{T}} t_j)^{r_t}, g^{r_v}, g^{r_v})$.

- ***Signing***: For a period $t$, given a non-revoked user's identity $ID \in \{0, 1\}^*$, a message $M \in \{0, 1\}^*$, the user first computes a string $vm = H_3(M)$ of length $l$. Let $vm_k$ denote the $k$-th bit of the string $vm$ and let $\mathcal{W} \subset \{1, 2,\ldots, l\}$ be the set of indices $k$ such that $vm_k = 1$ for $k = 1, 2,\ldots, l$. Then the user chooses a random number $r_m \in Z_p^*$ and computes $g^{r_m}$ and $h = H_4(M||g^{r_m})$. Finally, the user generates a signature $\sigma$ on the message $M$ as follows:

  $$\begin{aligned}\sigma &= (\sigma_1, \sigma_2, \sigma_3, \sigma_4)\\ &= ((S_1)^h (w'\prod_{k\in\mathcal{W}} w_k)^{r_m}, (S_2)^h, (S_3)^h, g^{r_m})\\ &= ((g_2^{\alpha+\beta} (u'\prod_{i\in\mathcal{V}} u_i)^{r_v} (t'\prod_{j\in\mathcal{T}} t_j)^{r_t})^h (w'\prod_{k\in\mathcal{W}} w_k)^{r_m},\\ &\quad g^{r_v h}, g^{r_t h}, g^{r_m}),\end{aligned}$$

where $(S_1, S_2, S_3)$ is the signing key $S_{ID,t}$ obtained above.

- ***Verification***: Given a signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ for an identity $ID$ on a message $M$ in a period $t$, a verifier computes $h = H_4(M||\sigma_4)$ and validates the signature as follows:

  $$\hat{e}(\sigma_1, g) = \hat{e}(g_2, g_1)^h \cdot \hat{e}(u'\prod_{i\in\mathcal{V}} u_i, \sigma_2) \cdot \hat{e}(t'\prod_{j\in\mathcal{T}} t_j, \sigma_3). \hat{e}(w'\prod_{k\in\mathcal{W}} w_k, \sigma_4).$$

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

In the following, we show the correctness of the checking equation in the *Verification* algorithm as follows:

$$\begin{aligned}\hat{e}(\sigma_1, g) &= \hat{e}((g_2^{\alpha+\beta} (u'\prod_{i\in\mathcal{V}} u_i)^{r_v} (t'\prod_{j\in\mathcal{T}} t_j)^{r_t})^h (w'\prod_{k\in\mathcal{W}} w_k)^{r_m}, g)\\ &= \hat{e}(g_2^{h(\alpha+\beta)}, g)\ \hat{e}((u'\prod_{i\in\mathcal{V}} u_i)^{r_v h}, g)\ \hat{e}((t'\prod_{j\in\mathcal{T}} t_j)^{r_t h}, g)\ \hat{e}((w'\prod_{k\in\mathcal{W}} w_k)^{r_m}, g)\\ &= \hat{e}(g_2, g^{\alpha+\beta})^h\ \hat{e}((u'\prod_{i\in\mathcal{V}} u_i), g^{r_v h})\ \hat{e}((t'\prod_{j\in\mathcal{T}} t_j), g^{r_t h}) \hat{e}((w'\prod_{k\in\mathcal{W}} w_k), g^{r_m})\\ &= \hat{e}(g_2, g_1)^h\ \hat{e}((u'\prod_{i\in\mathcal{V}} u_i), \sigma_2) \hat{e}((t'\prod_{j\in\mathcal{T}} t_j), \sigma_3) \hat{e}((w'\prod_{k\in\mathcal{W}} w_k), \sigma_4).\end{aligned}$$

## 5. Security analysis

In this section, we give the security analysis of our RIBS scheme. In order to simplify the security analysis, we consider two types of adversaries, namely, outside adversary and inside adversary (or revoked user). We adopt a technique similar to that used in [12] to show that the proposed scheme possesses strong unforgeability against adaptive chosen-message attacks for both types of adversaries under the CDH and CRH assumptions. Note that if the adversary is an outsider, it is allowed to issue all queries in the RID-SUF-ACMA game (mentioned in Section 3) except for the *initial key extract query* on the target identity $ID^*$. If the adversary is an inside adversary, it is allowed to issue all queries in the RID-SUF-ACMA game except for the *time key update query* on ($ID^*$, $t^*$).

***Theorem 1.*** *Under the CDH and CRH assumptions, the proposed RIBS scheme is strongly secure against adaptive chosen-message attacks (RID-SUF-ACMA) for* ***an outside adversary*** $\mathcal{A}$*. More precisely, assume that there is an outsider* $\mathcal{A}$*, with an advantage* $\varepsilon$ *against the proposed RIBS scheme, which can make at most* $q_E > 0$ *initial key extract queries,* $q_U > 0$ *time key update queries and* $q_S > 0$ *signing queries within a running time* $\tau$*. Then there is an algorithm* $\mathcal{B}$ *that has an advantage*

$$\varepsilon' \geq \varepsilon\left[\frac{1}{16(q_E+q_S)(m+1)q_S(l+1)}\right]$$

*to solve the CDH problem or*

$$\varepsilon'' \geq \frac{\varepsilon}{4}$$

*to violate the CRH assumption within a running time*

$$\tau' = \tau + O(\,(m\,q_E + n\,q_U + (m+n+l)\;q_S)\tau_1 + (q_E + q_U + q_S)\tau_2),$$

*in which* $\tau_1$ *and* $\tau_2$*, respectively, denote the executing time of a multiplication in* $G_1$ *and the executing time of an exponentiation in* $G_1$*.*

**Proof.** We assume that there exists an outside adversary $\mathcal{A}$ which succeeds in attacking the proposed RIBS scheme. We will construct an algorithm $\mathcal{B}$ to solve the CDH problem or violate CRH assumption. Assume that the algorithm $\mathcal{B}$ is given $<G_1, G_2, \hat{e}, g, g^a, g^b>$ as an instance of the CDH problem, where $a$ and $b$ are unknown to $\mathcal{B}$. To compute $g^{ab}$, the algorithm $\mathcal{B}$ simulates a challenger for $\mathcal{A}$ in the RID-SUF-ACMA game as follows.

- *Setup*. The challenger (algorithm) $\mathcal{B}$ first sets four collision-resistant hash functions as follows: $H_1$:$\{0, 1\}^* \to \{0, 1\}^m$, $H_2$:$\{0, 1\}^* \to \{0, 1\}^n$ and $H_3$, $H_4$:$\{0, 1\}^* \to \{0, 1\}^l$, where $m$, $n$ and $l$ are fixed lengths. Note that the employed collision-resistant hash functions are not seen as random oracles in our security proofs. The challenger $\mathcal{B}$ sets $l_v = 2(q_E + q_S)$ and $l_m = 2\,q_S$, and chooses two integers $k_v$ and $k_m$ at random, where $0 \leq k_v \leq m$ and $0 \leq k_m \leq l$. We assume that $l_v(m + 1) < p$ and $l_m(l + 1) < p$ for the given values of $q_E$, $q_S$, $m$ and $l$. The challenger $\mathcal{B}$ chooses a random value $\beta \in Z_p$ as the secret value of the time update key, and assigns $g_1 = g^a g^\beta$ and $g_2 = g^b$. The challenger $\mathcal{B}$ selects $x'$, $x_1,\ldots, x_m \in Z_{l_v}$, $y'$, $y_1,\ldots, y_m \in Z_p$, and computes $u' = g_2^{-l_v k_v + x'} g^{y'}$ and a vector $U = (u_i)$, where $u_i = g_2^{x_i} g^{y_i}$ for $1 \leq i \leq m$. In addition, the challenger $\mathcal{B}$ selects $z'$, $z_1,\ldots, z_n \in Z_p$, and computes $t' = g^{z'}$ and a vector $T = (t_j)$, where $t_j = g^{z_j}$ for $1 \leq j \leq n$. Moreover, the challenger $\mathcal{B}$ selects $c'$, $c_1,\ldots, c_l \in Z_{l_m}$, $d'$, $d_1,\ldots, d_l \in Z_p$, and computes $w' = g_2^{-l_m k_m + c'} g^{d'}$ and a vector $W = (w_k)$, where $w_k = g_2^{c_k} g^{d_k}$ for $1 \leq k \leq l$. Now, the challenger $\mathcal{B}$ has constructed a set of public parameters as

$Parms = <G_1, G_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, H_4, u', U, t', T, w', W>$.

Before performing *Queries* and *Forgery* between $\mathcal{A}$ and $\mathcal{B}$, we define three sets $\mathcal{V}$, $\mathcal{T}$ and $\mathcal{W}$, and five functions $F$, $J$, $E$, $K$ and $L$.

1. Let $v = H_1(ID)$ which is a bit string of length $m$. Let $\mathcal{V} \subset \{1, 2,\ldots, m\}$ be the set of indices $i$ such that $v_i = 1$, where $v_i$ denotes the $i$-th bit of the string $v$, for $i = 1, 2,\ldots, m$. Define the functions $F$ and $J$ by

$$F(v) = -l_v k_v + x' + \sum_{i\in\mathcal{V}} x_i \text{ and } J(v) = y' + \sum_{i\in\mathcal{V}} y_i\,.$$

2. Let $vt = H_2(ID, t)$ which is a bit string of length $n$. Let $\mathcal{T} \subset \{1, 2,\ldots, n\}$ be the set of indices $j$ such that $vt_j = 1$, where $vt_j$ denotes the $j$-th bit of the string $vt$, for $j = 1, 2,\ldots, n$. Define the function $E$ by

$$E(vt) = z' + \sum_{j\in\mathcal{T}} z_j\,.$$

3. Let $vm = H_3(M)$ which is a bit string of length $l$. Let $\mathcal{W} \subset \{1, 2,\ldots, l\}$ be the set of indices $k$ such that $vm_k = 1$, where $vm_k$ denotes the $k$-th bit of the string $vm$, for $k = 1, 2,\ldots, l$. Define the functions $K$ and $L$ by

$$K(vm) = -l_m k_m + c' + \sum_{k\in\mathcal{W}} c_k \quad\text{and}\quad L(vm) = d' + \sum_{k\in\mathcal{W}} d_k\,.$$

Finally, for the cumbersome notations defined above, we conclude with three relations which will be referred to frequently in the sequel, namely,

$$u'\prod_{i\in\mathcal{V}} u_i = g_2^{F(v)}g^{J(v)},\ t'\prod_{j\in\mathcal{T}} t_j = g^{E(vt)} \quad \text{and}$$

$$w'\prod_{k\in\mathcal{W}} w_k = g_2^{K(vm)}g^{L(vm)}.$$

- *Queries*. The adversary $\mathcal{A}$ may make a number of queries in an adaptive manner as follows.
  - *Initial key extract query* ($ID$): Consider a query for the initial secret key of an identity $ID$. The challenger $\mathcal{B}$ first computes $v = H_1(ID)$ and then $F(v)$ and $J(v)$. If $F(v) = 0 \bmod p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ chooses a random $r_v\in Z_p$ and computes the initial secret key $D_{ID}$ by

$$D_{ID} = (D_1, D_2) = ((g^a)^{-J(v)/F(v)}(u'\prod_{i\in\mathcal{V}} u_i)^{r_v},$$

$$(g^a)^{-1/F(v)}g^{r_v}).$$

Now, we are convinced that $D_{ID} = (D_1, D_2)$ is a valid initial secret key by

$$D_1 = (g^a)^{-J(v)/F(v)}(u'\prod_{i\in\mathcal{V}} u_i)^{r_v} = (g^a)^{-J(v)/F(v)}(g_2^{-l_vk_v+x'}g^{y'}\prod_{i\in\mathcal{V}} g_2^{x_i}g^{y_i})^{r_v}$$

$$=(g^a)^{-J(v)/F(v)}(g_2^{-l_vk_v+x'}g^{y'}\cdot g_2^{\sum_{i\in\mathcal{V}} x_i}g^{\sum_{i\in\mathcal{V}} y_i})^{r_v} = (g^{\cdot J(v)})^{-a/F(v)}(g_2^{-l_vk_v+x'+\sum_{i\in\mathcal{V}} x_i}g^{y'+\sum_{i\in\mathcal{V}} y_i})^{r_v}$$

$$=g_2^a(g_2^{F(v)}g^{J(v)})^{-a/F(v)}(g_2^{F(v)}g^{J(v)})^{r_v} = g_2^a(g_2^{F(v)}g^{J(v)})^{r_v-a/F(v)}$$

$$=g_2^a(u'\prod_{i\in\mathcal{V}} u_i)^{r_v'}$$

and

$$D_2 = (g^a)^{-1/F(v)}g^{r_v} = g^{r_v-a/F(v)} = g^{r_v'},$$

where $r_v' = r_v - a/F(v)$.

  - *Time key update query* ($ID$, $t$): Consider a query for the time update key of an identity $ID$ and a period $t$. The challenger $\mathcal{B}$ first computes $vt = H_2(ID, t)$ of length $n$. The challenger $\mathcal{B}$ then chooses a random $r_t\in Z_p$ and uses the secret value $\beta$ to compute the time update key as follows:

$$T_{ID,t} = (T_1, T_2) = (g_2^{\beta}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t},\ g^{r_t}).$$

  - *Signing query* ($M$, $ID$, $t$): Consider a query for an identity $ID$, a period $t$ and a message $M$. The challenger $\mathcal{B}$ first computes $v = H_1(ID)$ and then $F(v)$ and $J(v)$. Next, we consider two cases.

**Case 1:** If $F(v) \neq 0 \bmod l_v$, the challenger $\mathcal{B}$ can compute the initial secret key and the time update key as in the *initial key extract query* and the *time key update query*, respectively, and $\mathcal{B}$ then uses the *signing* algorithm to create a signature on $M$.

**Case 2:** If $F(v) = 0 \bmod p$, the challenger $\mathcal{B}$ first computes $vm = H_3(M)$ and then $K(vm)$ and $L(vm)$. If $K(vm) = 0 \bmod p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ chooses random values $r_v$, $r_t$, $r_m \in Z_p$ and computes $R = g^{r_m}$. The challenger $\mathcal{B}$ then computes $h = H_4(M||R)$ and constructs the signature as follows:

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$$

$$= (g_2^{\beta h}(u'\prod_{i\in\mathcal{V}} u_i)^{r_vh}(t'\prod_{j\in\mathcal{T}} t_j)^{r_th}(g^a)^{-L(vm)\cdot h/K(vm)}(w'\prod_{k\in\mathcal{W}} w_k)^{r_m},\ g^{r_vh},\ g^{r_th},\ (g^a)^{-\mathrm{h}/K(vm)}g^{r_m})$$

$$= (g_2^{\beta h}(u'\prod_{i\in\mathcal{V}} u_i)^{r_vh}(t'\prod_{j\in\mathcal{T}} t_j)^{r_th}g_2^{ah}g_2^{-ah}(g^{a\cdot L(vm)})^{-h/K(vm)}(w'\prod_{k\in\mathcal{W}} w_k)^{r_m},\ g^{r_vh},\ g^{r_th},\ g^{r_m-ah/K(vm)})$$

$$= (g_2^{\beta h}(u'\prod_{i\in\mathcal{V}} u_i)^{r_vh}(t'\prod_{j\in\mathcal{T}} t_j)^{r_th}g_2^{ah}(g_2^{K(vm)}g^{L(vm)})^{-ah/K(vm)}(g_2^{K(vm)}g^{L(vm)})^{r_m},\ g^{r_vh},\ g^{r_th},\ g^{r_m-ah/K(vm)})$$

$$= (g_2^{\beta h}(u'\prod_{i\in\mathcal{V}} u_i)^{r_vh}(t'\prod_{j\in\mathcal{T}} t_j)^{r_th}g_2^{ah}(g_2^{K(vm)}g^{L(vm)})^{r_m-ah/K(vm)},\ g^{r_vh},\ g^{r_th},\ g^{r_m-ah/K(vm)})$$

$$= (g_2^{ah}g_2^{\beta h}(u'\prod_{i\in\mathcal{V}} u_i)^{r_vh}(t'\prod_{j\in\mathcal{T}} t_j)^{r_th}(g_2^{K(vm)}g^{L(vm)})^{r_m-ah/K(vm)},\ g^{r_vh},\ g^{r_th},\ g^{r_m-ah/K(vm)})$$

$$= ((g_2^{a+\beta}(u'\prod_{i\in\mathcal{V}} u_i)^{r_v}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t})^h(w'\prod_{k\in\mathcal{W}} w_k)^{r_m'},\ g^{r_vh}\ ,g^{r_th},\ g^{r_m'}) \quad ,$$

where $r_m' = r_m - ah/K(vm)$.

- *Forgery*. Assume that the adversary $\mathcal{A}$ generates a valid signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*)$ for $(ID^*, t^*)$ on $M^*$, where $ID^*$, $t^*$ and $M^*$ are the target identity, period and message, respectively. We discuss two cases.

**Case 1:** If $(M^*, ID^*, t^*)$ did not appear in the *signing query*, the challenger $\mathcal{B}$ computes $v^* = H_1(ID^*)$, $vt^* = H_2(ID^*, t^*)$, $vm^* = H_3(M^*)$, $F(v^*)$ and $K(vm^*)$. If $F(v^*) \neq 0 \bmod p$ or $K(vm^*) \neq 0 \bmod p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ computes $h = H_4(M \| \sigma_4^*)$ and outputs $g^{ab}$ as follows:

$$\frac{(\sigma_1)^{\frac{1}{h}}}{(\sigma_2^{J(v^*)})^{\frac{1}{h}}(\sigma_3^{E(vt^*)})^{\frac{1}{h}}(\sigma_4^{L(vm^*)})^{\frac{1}{h}}g_2^{\beta}} = \frac{((g_2^{a+\beta}(u'\prod_{i\in\mathcal{V}}u_i)^{r_v}(t'\prod_{j\in\mathcal{T}}t_j)^{r_t})^{h}(w'\prod_{k\in\mathcal{W}}w_k)^{r_m})^{\frac{1}{h}}}{g^{r_v\cdot J(v^*)}g^{r_t\cdot E(vt^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\beta}}$$

$$= \frac{g_2^{a+\beta}(g_2^{F(v^*)}g^{J(v^*)})^{r_v}(g^{E(vt^*)})^{r_t}(g_2^{K(vm^*)}g^{L(vm^*)})^{r_m\frac{1}{h}}}{g^{r_v\cdot J(v^*)}g^{r_t\cdot E(vt^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\beta}}$$

$$= \frac{g_2^{a+\beta}(g_2^{0}g^{J(v^*)})^{r_v}(g^{E(vt^*)})^{r_t}(g_2^{0}g^{L(vm^*)})^{r_m\frac{1}{h}}}{g^{r_v\cdot J(v^*)}g^{r_t\cdot E(vt^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\beta}}$$

$$= g_2^{a} = g^{ab}.$$

This resolves the computational Diffie-Hellman (CDH) problem.

**Case 2:** If $(M^*, ID^*, t^*)$ has appeared in the *signing query*, adversary $\mathcal{A}$ owned a previously queried signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ of $(ID^*, t^*)$ on $M^*$. If $\sigma_2 \neq \sigma_2^*$ or $\sigma_3 \neq \sigma_3^*$, the challenger $\mathcal{B}$ can output $g^{ab}$ as in Case 1. Otherwise, if $\sigma_2 = \sigma_2^*$ and $\sigma_3 = \sigma_3^*$, then, since $\sigma_2 = g^{r_v h}$, $\sigma_2^* = g^{r_v h^*}$, $\sigma_3 = g^{r_t h}$ and $\sigma_3^* =, g^{r_t h^*}$, we have $h^* = h$, namely, $H_4(M \| g^{r_m}) = H_4(M \| g^{r_m^*})$ where $\sigma_4 = g^{r_m}$and $\sigma_4^* = g^{r_m^*}$. This causes a collision of $H_4$ which violates the CRH assumption.

Now, we analyze the probability of the event that the challenger $\mathcal{B}$ does not abort. In the phase of *initial key extract query*, if $F(v) \neq 0 \bmod p$, the challenger $\mathcal{B}$ can correctly answer queries without aborting. In the phase of *signing query*, if $F(v) \neq 0 \bmod p$ or $K(vm) \neq 0 \bmod p$, the challenger $\mathcal{B}$ can correctly respond queries without aborting. Note that by the previously mentioned assumptions $l_v(m+1) < p$ and $l_m(l+1) < p$, we have $0 \leq l_v k_v \leq p$, $0 \leq x' + \sum_{i\in\mathcal{V}} x_i \leq p$, $0 \leq l_m k_m \leq p$ and $0 \leq c' + \sum_{k\in\mathcal{W}} c_k \leq p$. Thus, $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$ and $K(vm) = 0 \bmod p$ also implies $K(vm) = 0 \bmod l_m$. Equivalently, $F(v) \neq 0 \bmod l_v$ implies $F(v) \neq 0 \bmod p$ and $K(vm) \neq 0 \bmod l_m$ also implies $K(vm) \neq 0 \bmod p$. Since the probability that $F(v) = 0 \bmod l_v$ and $K(vm) \neq 0 \bmod l_m$ occur is negligible, it suffices to consider the case $F(v) \neq 0 \bmod l_v$ in the phase of *signing query*. Obviously, the probability that both $F(v) \neq 0 \bmod l_v$ and $K(vm) \neq 0 \bmod l_m$ occur is a lower bound for the probability that the challenger $\mathcal{B}$ does not abort in the phase of *signing query*. Furthermore, we discuss a case of the challenger $\mathcal{B}$ not aborting in the phase of *Forgery*. The case is that $F(v^*) = 0 \bmod p$ and $K(vm^*) = 0 \bmod p$ must occur if $(M^*, ID^*, t^*)$ did not appear in the *signing query*. Let $v_1, \ldots, v_{q_I}$ be the identities appearing in either *initial key extract queries* or *signing queries* not involving the challenge identity $ID^*$ and let $vm_1, \ldots, vm_{q_M}$ be the messages in the *signing queries* involving the challenge identity $ID^*$. Clearly, we have $q_I < q_E + q_S$ and $q_M < q_S$. In order to simplify the analysis, we define the events as follows:

$A_i$: $F(v_i) \neq 0 \bmod l_v$,  $A^*$: $F(v^*) = 0 \bmod p$,

$B_k$: $K(vm_k) \neq 0 \bmod l_m$,  $B^*$: $K(vm^*) = 0 \bmod p$.

Hence, the probabilities of the challenger $\mathcal{B}$ not to abort for Cases 1 and 2 are presented as follows:

$$\Pr[\neg\text{abortCase1}] \geq \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{k=1}^{q_M} B_k \wedge B^*] =$$

$$\Pr[A^*]\cdot\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*]\cdot\Pr[B^*]\cdot\Pr[\bigwedge_{k=1}^{q_M} B_k \mid B^*]$$

and

$$\Pr[\neg\text{abortCase2}] \geq \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge \bigwedge_{k=1}^{q_M} B_k] = \Pr[\bigwedge_{i=1}^{q_I}$$

$$A_i]\cdot\Pr[\bigwedge_{k=1}^{q_M} B_k].$$

Here, we discuss the probabilities of the events $A^*$ and $B^*$, respectively. We have that $F(v) = 0 \bmod p$ implies $F(v) = 0 \bmod l_v$ and $K(vm) = 0 \bmod p$ also implies $K(vm) = 0 \bmod l_m$, since $l_v(m+1) < p$ and $l_m(l$

+ 1) < $p$. If $F(v) = 0 \bmod l_v$ and $K(vm) = 0 \bmod l_m$, there will be a unique choice of $k_v$ with $0 \le k_v \le m$ and $k_m$ with $0 \le k_m \le l$ such that $F(v) = 0 \bmod p$ and $K(vm) = 0 \bmod p$. Since $k_v$, $x'$, $X$, and $k_m$ are chosen randomly, we have the probabilities of the events $A^*$ and $B^*$as follows:

$$\Pr[A^*] = \Pr[F(v^*) = 0 \bmod p] = \Pr[F(v^*) = 0 \bmod p \wedge F(v^*) = 0 \bmod l_v]$$
$$= \Pr[F(v^*) = 0 \bmod l_v]\cdot\Pr[F(v^*) = 0 \bmod p \mid F(v^*) = 0 \bmod l_v]$$
$$= \frac{1}{l_v}\cdot\frac{1}{m+1}$$

and

$$\Pr[B^*] = \Pr[K(vm^*) = 0 \bmod p]= \Pr[K(vm^*) = 0 \bmod p \wedge K(vm^*) = 0 \bmod l_m]$$
$$= \Pr[K(vm^*) = 0 \bmod l_m]\cdot\Pr[K(vm^*) = 0 \bmod p \mid K(vm^*) = 0 \bmod l_m]$$
$$= \frac{1}{l_m}\cdot\frac{1}{l+1}.$$

We then have that

$$\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*] = 1 - \Pr[\bigvee_{i=1}^{q_I} \neg A_i \mid A^*] \ge 1 - \sum_{i=1}^{q_I}\Pr[\neg A_i \mid A^*] = 1 - \frac{q_I}{l_v} \ge 1 - \frac{q_E + q_S}{l_v}$$

and

$$\Pr[\bigwedge_{k=1}^{q_M} B_k \mid B^*] = 1 - \Pr[\bigvee_{k=1}^{q_M} \neg B_k \mid B^*] \ge 1 - \sum_{k=1}^{q_M}\Pr[\neg B_k \mid B^*] = 1 - \frac{q_M}{l_m} \ge 1 - \frac{q_S}{l_m}.$$

We also have $\Pr[\bigwedge_{i=1}^{q_I} A_i] = \Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*]$ and $\Pr[\bigwedge_{k=1}^{q_M} B_k] = \Pr[\bigwedge_{k=1}^{q_M} B_k \mid B^*]$ by independency, hence we can obtain both

$$\Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^*] = \Pr[A^*]\cdot\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*] \ge \left(\frac{1}{l_v}\frac{1}{m+1}\right)\cdot\left(1-\frac{q_E+q_S}{l_v}\right)$$

and

$$\Pr[\bigwedge_{k=1}^{q_S} B_k \wedge B^*] = \Pr[B^*]\cdot\Pr[\bigwedge_{k=1}^{q_S} B_k \mid B^*] \ge \left(\frac{1}{l_m}\frac{1}{l+1}\right)\cdot\left(1-\frac{q_S}{l_m}\right).$$

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

$$\Pr[\neg\text{abortCase1}] \ge \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A^* \wedge \bigwedge_{k=1}^{q_M} B_k \wedge B^*]$$
$$= \Pr[A^*]\cdot\Pr[\bigwedge_{i=1}^{q_I} A_i \mid A^*]\cdot\Pr[B^*]\cdot\Pr[\bigwedge_{k=1}^{q_M} B_k \mid B^*]$$
$$\ge \left[\frac{1}{4(q_E+q_S)(m+1)q_S 4(l+1)}\right]$$

and

$$\Pr[\neg\text{abortCase2}] \ge \Pr[\bigwedge_{i=1}^{q_I} A_i \wedge \bigwedge_{k=1}^{q_M} B_k]=\Pr[\bigwedge_{i=1}^{q_I} A_i]\cdot\Pr[\bigwedge_{k=1}^{q_M} B_k]\ge\frac{1}{4}.$$

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

$$\varepsilon' \ge \varepsilon\left[\frac{1}{16(q_E+q_S)(m+1)q_S(l+1)}\right]$$

to solve the CDH problem or

$$\varepsilon'' \ge \frac{\varepsilon}{4}$$

to violate the CRH assumption.

According to the descriptions above, $\mathcal{B}$ requires $O(m)$ multiplications and $O(1)$ exponentiations in the *initial key extract queries*. Also, $\mathcal{B}$ requires $O(n)$ multiplications and $O(1)$ exponentiations in the *time key update queries* as well as $O(m+n+l)$ multiplications and $O(1)$ exponentiations in the *signing queries*. So, the total running time required for $\mathcal{B}$ is

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

where $\tau$, $\tau_1$ and $\tau_2$ denote $\mathcal{A}$'s running time, the executing time of a multiplication in $G_1$ and the executing time of an exponentiation in $G_1$, respectively.

***Theorem 2.*** *Under the CDH and CRH assumptions, the proposed RIBS scheme is strongly secure against adaptive chosen-message attacks (RID-SUF-ACMA) for* ***an inside adversary*** *$\mathcal{A}$. More precisely, assume that there is an inside adversary $\mathcal{A}$, with an advantage $\varepsilon$ against the proposed RIBS scheme, which can make at most $q_E > 0$ initial key extract queries, $q_U > 0$ time key update queries and $q_S > 0$ signing queries within a running time $\tau$. Then there is an algorithm $\mathcal{B}$ that has an advantage*

$$\varepsilon' \ge \varepsilon\left[\frac{1}{16(q_U+q_S)(n+1)q_S(l+1)}\right]$$

*to solve the CDH problem or*

$$\varepsilon'' \ge \frac{\varepsilon}{4}$$

*to violate the CRH assumption within a running time*

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

*in which $\tau_1$ and $\tau_2$, respectively, denote the executing time of a multiplication in $G_1$ and the executing time of an exponentiation in $G_1$.*

**Proof.** We assume that there exists an inside adversary $\mathcal{A}$ which succeeds in attacking the proposed RIBS scheme. We will construct an algorithm $\mathcal{B}$ to solve the CDH problem or violate CRH assumption. Assume that the algorithm $\mathcal{B}$ is given $<G_1, G_2, \hat{e}, g, g^a, g^b>$ as an instance of the CDH problem, where $a$ and $b$ are unknown to $\mathcal{B}$. To compute $g^{ab}$, the algorithm $\mathcal{B}$ must simulate a challenger for $\mathcal{A}$ in the RID-SUF-ACMA game as follows.

- *Setup*. The challenger (algorithm) $\mathcal{B}$ sets four collision-resistant hash functions as follows: $H_1$:$\{0, 1\}^*\rightarrow\{0, 1\}^m$, $H_2$:$\{0, 1\}^*\rightarrow\{0, 1\}^n$ and $H_3$, $H_4$:$\{0, 1\}^*\rightarrow\{0, 1\}^l$, where $m$, $n$ and $l$ are fixed lengths. Note that the employed collision-resistant hash functions are not viewed as random oracles in our security proofs. The challenger $\mathcal{B}$ first sets $l_{vt} = 2(q_U + q_S)$ and $l_m = 2\,q_S$, and chooses two integers $k_{vt}$ and $k_m$ at random, where $0 \le k_{vt} \le n$ and $0 \le k_m \le l$. We assume that $l_{vt}(n + 1) < p$ and $l_m(l + 1) < p$ for the given values of $q_U$, $q_S$, $n$ and $l$. The challenger $\mathcal{B}$ chooses a random value $\alpha\in Z_p$ as the secret value of the initial secret key and assigns $g_1= g^{\alpha}g^a$, $g_2= g^b$. The challenger $\mathcal{B}$ selects $z'$, $z_1,\dots, z_m \in Z_p$, and computes $u' =g^{z'}$ and a vector $U = (u_i)$, where $u_i =g^{z_i}$ for $1 \le i \le m$. In addition, the challenger $\mathcal{B}$ selects $x'$, $x_1,\dots, x_n \in Z_{l_{vt}}$, $y'$, $y_1,\dots, y_n \in Z_p$ , and computes $t' = g_2^{-l_{vt}k_{vt}+x'}g^{y'}$ and a vector $T= (t_j)$ , where $t_j =g_2^{x_j}g^{y_j}$ for $1 \le j \le n$. Moreover, the challenger $\mathcal{B}$ selects $c'$, $c_1,\dots, c_l \in Z_{l_m}$, $d'$, $d_1,\dots, d_l \in Z_p$, and computes $w' = g_2^{-l_m k_m+c'}g^{d'}$ and a vector $W = (w_k)$, where $w_k =g_2^{c_k}g^{d_k}$ for $1 \le k \le l$. Now, the challenger $\mathcal{B}$ has constructed a set of public parameters as

  $Parms = <G_1, G_2, \hat{e}, g, g_1, g_2, H_1, H_2, H_3, H_4, u', U, t', T, w', W>.$

  Before performing *Queries* and *Forgery* between $\mathcal{A}$ and $\mathcal{B}$, we define three sets $\mathcal{V}$, $\mathcal{T}$ and $\mathcal{W}$, and five functions $E$, $F$, $J$, $K$ and $L$.

  1. Let $v= H_1(ID)$ which is a bit string of length $m$. Let $\mathcal{V} \subset \{1, 2,\dots, m\}$ be the set of indices $i$ such that $v_i = 1$, where $v_i$ denotes the $i$-th bit of the string $v$, for $i = 1, 2,\dots, m$. Define the function $E$ by

     $E(v) = z' + \sum_{i\in\mathcal{V}} z_i$ .

  2. Let $vt = H_2(ID, t)$ which is a bit string of length $n$. Let $\mathcal{T} \subset \{1, 2,\dots, n\}$ be the set of indices $j$ such that $vt_j = 1$, where $vt_j$ denotes the $j$-th bit of the string $vt$, for $j = 1, 2,\dots, n$. Define the functions $F$ and $J$ by

     $F(vt) = -l_{vt}k_{vt} + x' + \sum_{j\in\mathcal{T}} x_j$ and $J(vt) = y' + \sum_{j\in\mathcal{T}} y_j$ .

  3. Let $vm = H_3(M)$ which is a bit string of length $l$. Let $\mathcal{W} \subset \{1, 2,\dots, l\}$ be the set of indices $k$ such that $vm_k = 1$, where $vm_k$ denotes the $k$-th bit of the string $vm$, for $k = 1, 2,\dots, l$. Define the functions $K$ and $L$ by

     $K(vm) = -l_m k_m + c' + \sum_{k\in\mathcal{W}} c_k$ and $L(vm) = d' + \sum_{k\in\mathcal{W}} d_k$ .

- *Queries*. The adversary $\mathcal{A}$ may make a number of queries in an adaptive manner as follows.

  - *Initial key extract query* ($ID$): Consider a query for the initial secret key of an identity $ID$. The challenger $\mathcal{B}$ first computes $v = H_1(ID)$ of length $m$. The challenger $\mathcal{B}$ then chooses a random $r_v\in Z_p$ and uses the secret value $\alpha\in Z_p$ to compute the initial secret key by

    $D_{ID} = (D_1, D_2) = (\,g_2^{\alpha}(u'\prod_{i\in\mathcal{V}} u_i)^{r_v}, g^{r_v}).$

  - *Time key update query* ($ID$, $t$): Consider a query for the time update key of an identity $ID$ and a period $t$. The challenger $\mathcal{B}$ first computes $vt = H_2(ID, t)$ and then $F(vt)$ and $J(vt)$. If $F(vt) = 0$ mod $p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ chooses a random $r_t\in Z_p$ and computes the time update key $T_{ID,t}$ by

    $T_{ID,t} = (T_1, T_2) = (\,(g^a)^{-J(vt)/F(vt)}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t},$ $(g^a)^{-1/F(vt)}g^{r_t}).$

    Now, we are convinced that $T_{ID,t} = (T_1, T_2)$ is a valid initial secret key as follows:

$$T_1 = (g^a)^{-J(vt)/F(vt)}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t} = (g^a)^{-J(vt)/F(vt)}(g_2^{-l_{vt}k_{vt}+x'}g^{y'}\prod_{j\in\mathcal{T}} g_2^{x_j}g^{y_j})^{r_t}$$

$$= (g^a)^{-J(vt)/F(vt)}(g_2^{-l_{vt}k_{vt}+x'}g^{y'}g_2^{\sum_{j\in\mathcal{T}} x_j}g^{\sum_{j\in\mathcal{T}} y_j})^{r_t}$$

$$=(g^{J(vt)})^{-a/F(vt)}(g_2^{-l_{vt}k_{vt}+x'+\sum_{j\in\mathcal{T}} x_j} g^{y'+\sum_{j\in\mathcal{T}} y_j})^{r_t}$$

$$= g_2^a(g_2^{F(vt)}g^{J(vt)})^{-a/F(vt)}(g_2^{F(vt)}g^{J(vt)})^{r_t}$$

$$= g_2^a(g_2^{F(vt)}g^{J(vt)})^{r_t-a/F(vt)}$$

$$= g_2^a(t'\prod_{j\in\mathcal{T}} t_j)^{r_t'}$$

and

$$T_2 = g^a(g^{-1/F(vt)}g^{r_t}) = g^{r_t-a/F(vt)} = g^{r_t'},$$

where $r_t' = r_t - a/F(vt)$.

- *Signing query* ($M$, $ID$, $t$): Consider a query for an identity $ID$, a period $t$ and a message $M$. The challenger $\mathcal{B}$ first computes $v = H_1(ID)$ and $vt = H_2(ID, t)$ and then computes $F(vt)$ and $J(vt)$. Here, we consider two cases.

**Case 1**: If $F(vt) \neq 0 \bmod l_{vt}$, the challenger $\mathcal{B}$ can compute the initial secret key and the time update key as in the *initial key extract query* and the *time key update query* respectively, and $\mathcal{B}$ then uses the *signing algorithm* to create a signature on $M$.

**Case 2** : If $F(vt) = 0 \bmod p$, the challenger $\mathcal{B}$ first computes $vm = H_3(M)$ and then $K(vm)$ and $L(vm)$. If $K(vm) = 0 \bmod p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ chooses random values $r_v$, $r_t$, $r_m \in Z_p$ and computes $R=g^{r_m}$. The challenger $\mathcal{B}$ then computes $h = H_4(M||R)$ and constructs the signature as follows:

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$$
$$=((g_2^{\alpha}(u'\prod_{i\in\mathcal{U}} u_i)^{r_v}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t}(g^a)^{-L(vm)/K(vm)})^h(w'\prod_{k\in\mathcal{W}} w_k)^{r_m},\ (g^{r_v})^h,\ (g^{r_t})^h,\ (g^a)^{-\mathrm{h}/K(vm)}g^{r_m})$$
$$=((g_2^{\alpha+a}(u'\prod_{i\in\mathcal{U}} u_i)^{r_v}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t})^h(w'\prod_{k\in\mathcal{W}} w_k)^{r_m'},\ g^{r_v h},\ g^{r_t h},\ g^{r_m'}),$$

where $r_m' = r_m - ah/K(vm)$.

- *Forgery*. Assume that the adversary $\mathcal{A}$ generates a valid signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*)$ for ($ID^*$, $t^*$) on $M^*$, where $ID^*$, $t^*$ and $M^*$ are the target identity, period and message, respectively. We discuss two cases.

**Case 1:** If ($M^*$, $ID^*$, $t^*$) did not appear in the *signing query*, the challenge $\mathcal{B}$ computes $v^* = H_1(ID^*)$, $vt^* = H_2(ID^*, t^*)$, $vm^* = H_3(M^*)$, $F(vt^*)$ and $K(vm^*)$. If $F(vt^*) \neq 0 \bmod p$ or $K(vm^*) \neq 0 \bmod p$, the challenger $\mathcal{B}$ aborts. Otherwise, the challenger $\mathcal{B}$ computes $h = H_4(M|| \sigma_4^*)$ and outputs $g^{ab}$ as follows:

$$\frac{(\sigma_1)^{\frac{1}{h}}}{(\sigma_2^{J(vt^*)})^{\frac{1}{h}}(\sigma_3^{E(v^*)})^{\frac{1}{h}}(\sigma_4^{L(vm^*)})^{\frac{1}{h}}g_2^{\alpha}} = \frac{((g_2^{a+\alpha}(u'\prod_{i\in\mathcal{U}} u_i)^{r_v}(t'\prod_{j\in\mathcal{T}} t_j)^{r_t})^h(w'\prod_{k\in\mathcal{W}} w_k)^{r_m})^{\frac{1}{h}}}{g^{r_v\cdot J(vt^*)}g^{r_t\cdot E(v^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\alpha}}$$

$$= \frac{g_2^{a+\alpha}(g_2^{F(vt^*)}g^{J(vt^*)})^{r_v}(g^{E(v^*)})^{r_t}(g_2^{K(vm^*)}g^{L(vm^*)})^{r_m\frac{1}{h}}}{g^{r_v\cdot J(vt^*)}g^{r_t\cdot E(v^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\alpha}}$$

$$= \frac{g_2^{a+\alpha}(g_2^0 g^{J(vt^*)})^{r_v}(g^{E(v^*)})^{r_t}(g_2^0 g^{L(vm^*)})^{r_m\frac{1}{h}}}{g^{r_v\cdot J(vt^*)}g^{r_t\cdot E(v^*)}g^{r_m\cdot L(vm^*)\frac{1}{h}}g_2^{\alpha}}$$

$$= g_2^a = g^{ab}.$$

This resolves the computational Diffie-Hellman (CDH) problem.

**Case 2:** If ($M^*$, $ID^*$, $t^*$) has appeared in the *signing query*, adversary $\mathcal{A}$ owned a previously queried signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ of ($ID^*$, $t^*$) on $M^*$. If

$\sigma_2 \neq \sigma_2^*$ or $\sigma_3 \neq \sigma_3^*$, the challenger $\mathcal{B}$ can output $g^{ab}$ as in Case 1. Otherwise, if $\sigma_2 = \sigma_2^*$ and $\sigma_3 = \sigma_3^*$, then, since $\sigma_2 = g^{r_v h}$, $\sigma_2^* = g^{r_v h^*}$, $\sigma_3 = g^{r_t h^*}$ and $\sigma_3^* =, g^{r_t h^*}$, we have $h^* = h$, namely, $H_4(M \| g^{r_m}) = H_4(M \| g^{r_m})$ where $\sigma_4^* = g^{r_m^*}$ and $\sigma_4 = g^{r_m}$. This causes a collision of $H_4$ which violates the CRH assumption.

The probability analysis is similar to Theorem 1. We leave the details to the reader. The probabilities of the challenger $\mathcal{B}$ not aborting for Cases 1 and 2 are

$$Pr[\neg abortCase1] \geq \varepsilon \left[\frac{1}{16 q_S (q_U + q_S)(n+1)(l+1)}\right]$$

and

$$\Pr[\neg\text{abortCase2}] \geq \frac{\varepsilon}{4}.$$

Then the challenger $\mathcal{B}$ has an advantage

$$\varepsilon' \geq \varepsilon \left[\frac{1}{16 q_S (q_U + q_S)(n+1)(l+1)}\right]$$

to solve the CDH problem or

$$\varepsilon'' \geq \frac{\varepsilon}{4}$$

to violate the CRH assumption. The executing time is

$$\tau + O\left((m q_E + n q_U + (m + n + l)\, q_S)\, \tau_1 + (q_E + q_U + q_S)\, \tau_2\right),$$

where $\tau_1$ and $\tau_2$ denote the executing time of a multiplication in $G_1$ and an exponentiation in $G_1$, respectively. □

## 6. Comparisons

For convenience, the following notations are used to analyze the performance.

- $TG_e$: The time of executing a bilinear pairing operation in $G_2$.
- $T_{exp}$: The time of executing an exponentiation operation in $G_1$.
- $|\sigma|$: The bit length of a message $\sigma$.

Note that in a multiplicative cyclic group, $TG_e$ and $T_{exp}$ are more time-consuming than the multiplication operation. Here, we compare with previously proposed schemes without random oracles to demonstrate the advantages of our RIBS scheme. Table 1 lists the comparisons among the schemes of Paterson and Schuldt [9], Sato *et al.* [29], Tsai *et al.* [12] and ours in terms of computational cost, signature size, revocable functionality and security property. For the computation cost in the signing phase, our scheme requires $5T_{exp}$ to sign a message, which increases a little the computing cost in comparison to the other schemes. Nevertheless, our scheme has better performance than Sato *et al.*'s scheme in terms of the verification phase and signature size. On the other hand, we emphasize that our scheme possesses strong unforgeability, while Tsai *et al.*'s scheme offers only existential unforgeability. Note that strongly unforgeable signature schemes are important for constructing cryptographic schemes such as chosen-ciphertext secure cryptosystems and group signatures.

In the following, we show that Tsai *et al.*'s RIBS scheme [12] is ***not*** strongly secure against adaptive chosen-message attacks. Assume that an adversary received a valid signature $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4) = (g_2^{\alpha+\beta} \cdot (u' \prod_{i \in \mathcal{U}} u_i)^{r_v} \cdot (t' \prod_{j \in \mathcal{T}} t_j)^{r_t} \cdot (w' \prod_{k \in \mathcal{W}} w_k)^{r_m}, g^{r_v}, g^{r_t}, g^{r_m})$ in [12]. Certainly, the valid signature $\sigma$ can pass the following equality:

$$\hat{e}(\sigma_1, g) = \hat{e}(g_1, g_2) \cdot \hat{e}(\sigma_2, u' \prod_{i \in \mathcal{U}} u_i) \cdot \hat{e}(\sigma_3, t' \prod_{j \in \mathcal{T}} t_j) \cdot \hat{e}(\sigma_4, w' \prod_{k \in \mathcal{W}} w_k) \cdot$$

In such a case, the adversary chooses a random value $r_m' \in Z_p$ and uses the signature $\sigma$ to generate a new signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*) = (\sigma_1 (w' \prod_{k \in \mathcal{W}} w_k)^{r_m'}, \sigma_2, \sigma_3, \sigma_4 \cdot g^{r_m'})$. Obviously, $\sigma^*$ is still a valid signature since any verifier can validate the signature tuple by $\hat{e}(\sigma_1^*, g) = \hat{e}(g_1, g_2) \cdot \hat{e}(\sigma_2^*, u' \prod_{i \in \mathcal{U}} u_i) \cdot \hat{e}(\sigma_3^*, t' \prod_{j \in \mathcal{T}} t_j) \cdot \hat{e}(\sigma_4^*, w' \prod_{k \in \mathcal{W}} w_k)$. It is obvious that Tsai *et al.*'s RIBS scheme [12] violates the property of strong unforgeability in Definition 4 and Remark 2.

Indeed, Paterson and Schuldt's scheme and Sato *et al.*'s scheme may be equipped with the revocation mechanism presented by Boneh and Franklin [2]. In this case, the revocation mechanism would require a secure channel to transmit the users' new private keys periodically which causes enormous computation workload for the PKG and (non-revoked) users when encrypting and decrypting private keys. Based

on Tseng and Tsai's revocable ID-based public key setting, both RIBS schemes of Tsai *et al.* and ours adopt the revocation mechanism with a public channel, so that the computational burden can be significantly reduced due to the absence of encryption/decryption via secure channels.

## 7. Conclusions

In this article, an efficient strongly unforgeable RIBS scheme without random oracles was proposed. Comparisons with previously proposed schemes were made to demonstrate the advantages of our scheme in terms of revocable functionality and security property. In the standard model (without random oracles), we proved that our scheme possesses strong unforgeability against adaptive chosen-message attacks under the CDH and CRH assumptions. Indeed, Tseng and Tsai's

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

| | **Paterson and Schuldt's IBS scheme [9]** | **Sato *et al*.'s IBS scheme [29]** | **Tsai *et al*.'s RIBS scheme [12]** | **Our RIBS scheme** |
|---|---|---|---|---|
| Computational cost for signing | $2T_{exp}$ | $3T_{exp}$ | $2T_{exp}$ | $5T_{exp}$ |
| Computational cost for verification | $4TG_e$ | $6TG_e$ | $5TG_e$ | $5TG_e + T_{exp}$ |
| Signature size | $3\|G_1\|$ | $5\|G_1\|$ | $4\|G_1\|$ | $4\|G_1\|$ |
| Required channel for revocation | Secure channel | Secure channel | Public channel | Public channel |
| Periodical encryption/decryption for revocation | Required | Required | Not required | Not required |
| Security property | Existential Unforgeability | Strong Unforgeability | Existential Unforgeability | Strong Unforgeability |

revocable ID-based public key setting provides an efficient revocation mechanism with a public channel. Our strongly secure RIBS scheme is one of primitives for their revocable ID-based public key system and provides a fundamental to construct revocable ID-based cryptographic schemes such as chosen-ciphertext secure revocable ID-based cryptosystems and revocable ID-based group signatures.

## Acknowledgments

This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC102-2221-E-018-019.

## References

[1] **A. Shamir**. Identity-based cryptosystems and signature schemes. In: *Proc. of Crypto'84*, LNCS, 196, 1984, pp. 47-53.

[2] **D. Boneh, M. Franklin.** Identity-based encryption from the Weil pairing. In: *Proc. of Crypto'01*, LNCS, 2139, 2001, pp. 213-229.

[3] **M. Bellare, C. Namprempre, G. Neven.** Security proofs for identity-based identification and signature schemes. *Journal of Cryptology*, 2008, Vol. 22, No. 1, 1-61.

[4] **Y. M. Tseng, T. Y. Wu, J. D. Wu.** A pairing-based user authentication scheme for wireless clients with smart cards. *Informatica*, 2008, Vol. 19, No. 2, 285-302.

[5] **T. Y. Wu, Y. M. Tseng, T. T. Tsai.** A revocable ID-based authenticated group key exchange protocol with resistant to malicious participants. *Computer Networks*, 2012, Vol. 56, No. 12, 2994-3006.

[6] **T. Y. Wu, Y. M. Tseng.** An ID-based mutual authentication and key exchange protocol for low-power mobile devices. *The Computer Journal*, 2010, Vol. 53, No. 7, 1062-1070.

[7] **T. Y. Wu, Y. M. Tseng.** An efficient user authentication and key exchange protocol for mobile client-server environment. *Computer Networks*, 2010, Vol. 54, No. 9, 1520-1530.

[8] **Z. Tan.** An enhanced ID-based Authenticated Multiple Key Agreement Protocol. *Information Technology and Control*, 2013, Vol. 42, No. 1, 21-28.

[9] **K. Paterson, J. Schuldt.** Efficient identity-based signatures secure in the standard model. In: *Proc. ACISP'06*, LNCS, 4058, 2006, pp. 207-222.

[10] **J. C. Cha, J. H. Cheon.** An identity-based signature from gap Diffie-Hellman groups. In: *Proc. of PKC'03*, LNCS, 2567, 2003, pp. 18-30.

[11] **Y. F. Chang, W. L. Tai, C. Y. Lin**. A verifiable proxy signature scheme based on bilinear pairings with identity-based cryptographic approaches. *Information Technology and Control*, 2012, Vol. 41, No. 1, 60-68.

[12] **T. T. Tsai, Y. M. Tseng, T. Y. Wu.** Provably secure revocable ID-based signature in the standard model. *Security and Communication Networks*, 2013, Vol. 6, No. 10, 1250-1260.

[13] **T. Y. Wu, T. T. Tsai, Y. M. Tseng.** Revocable ID-based signature scheme with batch verifications. *IIHMSP-2012, IEEE press*, 2012, pp. 49-54.

[14] **B. Waters.** Efficient identity-based encryption without random oracles. In: *Proc. of Eurocrypt'05*, LNCS, 3494, 2005, pp. 1-33.

[15] **D. Boneh, M. Hamburg.** Generalized identity based and broadcast encryption schemes. In: *Proc. of Asiacrypt'08*, LNCS, 5350, 2008, pp. 455-470.

[16] **T. T. Tsai, Y. M. Tseng, T. Y. Wu.** Efficient revocable multi-receiver ID-based encryption. *Information Technology and Control*, 2013, Vol. 42, No. 2, 159-169.

[17] **T. T. Tsai, Y. M. Tseng, T. Y. Wu.** A fully secure revocable ID-based encryption in the standard model. *Informatica*, 2012, Vol. 23, No. 3, 487-505.

[18] **K. Paterson.** Identity-based signatures from pairings on elliptic curves. *Electronics Letters*, 2002, Vol. 38, No. 9, 1025-1026.

[19] **Y. M. Tseng, T. Y. Wu, J. D. Wu.** An efficient and provably secure ID-based signature scheme with batch verifications. *International Journal of Innovative Computing, Information and Control*, 2009, Vol. 5, No. 11, 3911-3922.

[20] **K. A. Shim.** An ID-based aggregate signature scheme with constant pairing computations. *Journal of Systems and Software*, 2010, Vol. 83, No. 10, 1873-1880.

[21] **S. Narayan, U. Parampalli.** Efficient identity-based signatures in the standard model. *IET Information Security*, 2008, Vol. 2, No. 4, 108-118.

[22] **D. Boneh, X. Boyen.** Short signatures without random oracles. In: *Proceedings of Eurocrypt'04*, LNCS, 3027, 2004, pp. 56-73.

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

[24] **J. Camenisch, A. Lysyanskaya.** Signature schemes and anonymous credentials from bilinear maps. In: *Proceedings of Crypto'04*, LNCS, 3152, 2004, pp. 56-72.

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

[26] **Q. Huang, D. S. Wong, and Y. Zhao.** Generic transformation to strongly unforgeable signatures. In: *Proceedings of ACNS* 2007, LNCS, 4521, 2007, pp. 1-17.

[27] **M. Bellare, S. Shoup.** Two-tier signatures, strongly unforgeable signatures, and fiat-shamir without random oracles. In: *Proceedings of PKC'07*, LNCS, 4450, 2007, pp. 201-216.

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

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

[30] **A. Boldyreva, V. Goyal, V. Kumar.** Identity-based encryption with efficient revocation. In: *Proceedings of CCS'08*, ACM, 2008, pp. 417-426.

[31] **Y. M. Tseng, T. T. Tsai.** Efficient revocable ID-based encryption with a public channel. *The Computer Journal*, 2012, Vol. 55, No. 4, 475-486.

[32] **Y. Sun, F. Zhang, L. Shen, R. Deng.** Revocable identity-based signature without pairing. In: *Proceedings of INCoS'13*, IEEE, 2013, pp. 363-365.

[33] **M. Bellare, A. Boldyreva, A. Palacio.** An uninstantiable random oracle model scheme for a hybrid encryption problem. In: *Proceedings of Cachin and Camenisch'04*, 2004, pp. 171-188.

[34] **D. Boneh, X. Boyen.** Efficient selective-ID identity based encryption without random oracles. In: *Proceedings of Eucrypt'04*, LNCS, 3027, 2004, pp. 223-238.

Received November 2013.