A New Construction of Short Hierarchical Identity-based Signature in the Standard Model

Leyou Zhang[†] and Yupu Hu[††],

[†]Department of Applied Mathematics, Xidian University, Xi'an 710071, China;
[††]Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an, 710071, China

Summary
In this paper, a new short hierarchical identity-based signature (HIBS) scheme is proposed in the standard model. This scheme has some advantages over the available schemes: the private keys size shrinks as the identity depth increases and the signature size is constant as it consists of three group elements. Furthermore, under the generalization selective-identity security model, we reduce the security of the new scheme to the h-*Exponent Computational Diffie-Hellman (*h-*CDH) assumption. This assumption is more natural than many of the hardness assumptions recently introduced to HIBS in the standard model*

Key words:
Hierarchical identity-based signature; the standard model; h-CDH assumption; provably secure

1. Introduction

A digital signature is an electronic signature that can be used to authenticate the identity of the sender or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. It is one of the most important developments from the work on public key cryptography. In traditional public key signature algorithms, the public keys of the signer are essentially random bit strings picked from a given set. This leads to a problem of how the public keys are associated with the physical entities which are meant to be performing the signing. In these traditional systems the binding between the public keys and the identity of the signer is obtained via a digital certificate. As noticed by Shamir [1] it would be more efficient if there was no need for such a binding, in that the users identity would be their public key, more accurately, given the users identity the public key could be easily derived using some public deterministic algorithm. It is called Identity-Based cryptography.

Identity-Based encryption (IBE) was introduced firstly in [1]. It allows for a party to encrypt a message using the recipient's identity as a public key. The ability to use identities as public keys avoids the need to distribute public key certificates. So it can simplify many applications of public key encryption (PKE) and is currently an active research area. Hierarchical IBE (HIBE) [6-12] is a generalization of IBE. It allows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. An identity at level k of the hierarchy tree can issue private keys to its descendant identities, but cannot decrypt messages intended for other identities. The first efficient construction for HIBE is due to Gentry and Silverberg [6], where security is based on the Bilinear Diffie-Hellman (BDH) assumption in the random oracle model. The first construction without random oracles due to Boneh and Boyen [8] gives an efficient HIBE based on decision BDH. The idea of hierarchical ID-Based signature (HIBS) scheme was firstly proposed by Gentry and Silverberg [6] in 2002. The first provably secure HIBS scheme was proposed by Chow *et al* [10]. Its security is proved under the random oracle and is based on the selective-ID model, which is a weaker model of security. Yuen and Wei [17] also provided a direct construction where the size of the signature is independent from the number of levels. Although their scheme can be proven secure without random oracles, it is also provably secure under a strong assumption, the *OrcYW* assumption. Recently, an efficient construction in [18] is proposed without relying on the random oracles. But it is secure under a strong assumption, q-SDH assumption.

As a natural extension of the efforts to provide a more efficient scheme in the standard model, we give a new efficient construction of HIBS scheme based on [4, 5]. Our scheme is based on the h-CDH assumption which is a modified CDH assumption and is polynomial time equivalent to CDH assumption for $h = 1$ [20]. In addition, it is based on the extension of Water's signature scheme, so the public parameters depend on the levels of the HIBS. However the private key size in our system shrinks as the identity depth increases and the signature size is constant as it consists of only three group elements. It is more efficient than the generic constructions of using certificate chain or hierarchical authentication tree. Additionally, the assumption in our scheme seems more natural than many of the hardness assumptions recently introduced to pairing based HIBS system.

Manuscript received April 5, 2009
Manuscript revised April 20, 2009

2. Preliminaries

2.1. Bilinear Map

Let G and G_1 are two (multiplicative) cyclic groups of prime order *p* and g is a generator of G. A bilinear map $\hat{e}$ is a map $\hat{e}: G \times G \to G_1$ with the properties:

(i) Bilinearity: for all *u*, $v \in G$; *a*, $b \in Z_p$, we have

$$\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab};$$

(ii) Non-degeneracy: $\hat{e}(g, g) \neq 1$;

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

2.2. Hardness Assumption

We briefly recall the definitions of some hardness assumptions:

Definition 1 (*h*-Strong Diffie-Hellman Problem (*h*-SDH)) Given (*h*+2)-tuple ($g', g, g^{\alpha}, \cdots g^{\alpha^h}$), the *h*-SDH problem is to output a pair (*A*,*c*) such that $A^{\alpha+c} = g'$, where $\alpha, c \in Z_p$ and g is generator of G.

Definition 2 (*h*-Exponent Computational Diffie-Hellman Problem, *h*-CDH) Given a group *G* of prime order *p* with generator g and elements ($g^a, g^{a^2}, \cdots, g^{a^h}$) where *a* is selected uniformly at random from Z_p and $h \geq 1$, the *h*-CDH problem in *G* is to compute $g^{a^{h+1}}$.

Definition 3 (The *h*-weak Diffie-Hellman Problem(*h*-wDH)**)** Given a group *G* of prime order *p* with generator g and elements ($g^a, g^{a^2}, \cdots, g^{a^h}$) where *a* is selected uniformly at random from Z_p and $h \geq 1$, compute $g^{\frac{1}{a}}$.

Definition 4 (The *Orc*-YW Problem) Given

(1) $l \geq 1$, $\{ g^{x^i} : 0 \leq i \leq l \}$, γ, δ, $g_4, g_5, \gamma_1, \cdots, \gamma_l$, an identity $I = \{I_1, \cdots, I_l\}$, full-domain collision-resistant hash function H,

(2) an oracle O_H which upon input a message *m* and an identity $I' = \{I_1, \cdots, I_k\}$ for $k \leq l$,outputs a tuple (D_1, D_2, Z_1, Z_2) satisfying: For some random *t, r*, which differ for each query to O_H , $D_1 = g^t, D_2 = Q^t, Z_1 = a_0^h g_4^t, Z_2 = a_1^h g_5^t$, where

$$Q = g_3 \prod_{i=1}^{k} h_i^{I_i}, \quad h_i = g^{\gamma_i} g^{-x^{l-i+1}}, \text{ for } 1 \leq i \leq l,$$

$$g_2 = g^{x^l + \gamma}, g_3 = g^{\delta + \sum_{i=1}^{l} x^{l-i+1} I_i}, \quad a_0 = g_2^x Q^r, a_1 = g^r,$$

$$h = H(D_1, D_2, I', m, param),$$

$$param = (g, g^x, g_2, g_3, g_4, g_5, h_1, \cdots, h_l).$$

The *Orc*-YW Problem is to output $(\tilde{m}, \tilde{D}_1, \tilde{D}_2, \tilde{Z}_1, \tilde{Z}_2)$ satisfying

$$\hat{e}(g, \tilde{Z}_1) \cdot \hat{e}(g_5, \tilde{D}_2) = \hat{e}(g_1, g_2)^{\bar{h}} \cdot \hat{e}(Q, \tilde{Z}_2) \cdot \hat{e}(g_4, \tilde{D}_1);$$

$$\hat{e}(Q, \tilde{D}_1) = \hat{e}(Q, \tilde{Z}_2); Q = g_3 \prod_{i=1}^{k} h_i^{I_i},$$

$\tilde{m}$ was not queried to Q_H, where

$$\bar{h} = H(D_1, D_2, I', m, param).$$

Definition 5 We say that the (t, ε) *h*-CDH assumption holds in a group *G* if no adversary running in time at most *t* can solve the *h*-CDH problem in *G* with probability at least ε.

Note that it was shown in [20] that *h*-CDH problem is equivalent to CDH problem for *h* = 1.

According [20, 21], we can obtain

$$h - wDH = (\text{polynomial time equivalent}) \, h - CDH \geq h - SDH.$$

2.3. H-level HIBS Scheme

An *h*-level HIBS scheme consists of the algorithms *Setup, Extract, Sign* and *Verify*. They are specified as follows:

***Setup*:** On input a security parameter, *PKG* returns the system parameters together with the master key. These are publicly known while the master key is known only to the *PKG*.

***Extract*:** On input an identity $ID = (v_1, \cdots, v_j)$, the public parameters of the *PKG* and the private key $d_{ID_{j-1}}$ corresponding to the identity $ID = (v_1, \cdots, v_{j-1})$, it returns a private key d_{ID} for *ID*. The identity *ID* is used as the public key while d_{ID} is the corresponding private key.

***Sign*:** On input the identity *ID*, the private key and a message *M* from the message space, it outputs a signature σ corresponding to the *M* under *ID*.

***Verify*:** On input the signature σ corresponding to the *M* under *ID*, it is accepted if it is valid. Otherwise it is rejected.

A HIBS scheme is secure if it satisfies two requirements: *Correctness* and *Existential Unforgeability.*

2.4. Existential Unforgeability

Concerning the security of the identity-Based cryptography, there are mainly two definitions:

· Full security, which means that the attacker can choose adaptively the identity he wants to attack (after having seen the parameters);

· Selective-ID security, which means that the attacker must choose the identity he wants to attack at the beginning, before seeing the parameters. The Selective-ID security is thus weaker than full security.

Recently, two new security models, $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$ have been introduced in [14], where they are called the generalization selective-identity security and full security. Here we describe only $\boldsymbol{M}_2$ since this is the model that we require. $\boldsymbol{M}_2$ is constructed for the encryption scheme. And therefore, we need to modify it to obtain the model of HIBS. Following [12, 18], we give the security model of HIBS as follows:

Init The adversary commits to sets of identities $I_1^*,\cdots,I_j^*$, where $1 \le j \le h$ and h is the maximum number of levels of the HIBS. Let $|I_i^*| = n_i$. The adversary's commitment fixes the length of the challenge identity to be h. Also, the set I_i^* corresponds to the set of committed identities for the i-th level of the HIBE.

Setup The simulator generates system parameter *param* and gives it to the adversary.

Queries The adversary queries Extraction Oracles and Signing Oracles. Note that the adversary is not allowed to query the key extraction oracle on any identity $(v_1, \ldots, v_j)$ such that $j \le h$ and $v_i \in I_i^*$ for all $1 \le i \le j$.

Forgery The adversary delivers a signature σ^* for signer identity $ID^* = (v_1^*,\cdots,v_j^*)$ and message M^*, where $v_i^* \notin I_i^*$. ID^* or its prefix have never been input to a Extraction Oracles and (ID^*, M^*) has never been input to a Signing Oracles.

Note: If $n_1=n_2=\ldots=n_l=1$, then we obtain the selective-ID secure model.

The adversary wins if he completes the Game with *Valid = Verify*($ID^*, M^* \sigma^*$). For a detail description, the readers are referred to [12 ,14, 18].

3. New Construction of HIBS Scheme

Our construction is based on the Waters's signature scheme [4] and its generalization in [5]. It works as follows:

Setup To generate system parameters for an HIBS of maximum depth h, the algorithm selects a random generator $g \in G$ and some random elements $h_{ij}, g_2, g_3, u_0, u_l$ from G for i=1,…,h, j=1,… n_i, l=1,…n_m, where $n_1,\cdots,n_h$ are some small positive integers and n_m is the length of message m. Then it picks a $\alpha \in Z_p$ at random and sets $g_1 = g^\alpha$. We set $\mathbf{H}_i$=(h_{ij}) and $\mathbf{U} = (u_l)$ for i=1,…,h, j=1,… n_i and l=1,…n_m. The system parameters are

$$param=(g, g_1, g_2, g_3, u_0, \mathbf{H}_1,\cdots,\mathbf{H}_h, \mathbf{U})$$

and master key is g_2^α.

For $i = 1,\cdots,h$, we define the function $F_i(x) = \prod_{j=1}^{n_i} h_{ij}^{x^j}$, where $x \in Z_p$.

***Extract*:** To generate a private for ID=(v_1,v_2,…,v_j), where $j \le h$ and $v_i \in Z_p$, the algorithm picks randomly a $r \in Z_p$ and outputs

$$d_{ID} = (d_0, d_1, d_{j+1}\cdots, d_l)$$

$$=(g_2^\alpha (g_3 \prod_{i=1}^{j} F_i(v_i))^r, g^r, \mathbf{H}_{j+1}^r,\cdots,\mathbf{H}_h^r),$$

where $\mathbf{H}_i^r$ denotes $(h_{i1}^r,\cdots,h_{in_i}^r)$ with $i = 1,\cdots,j$. Among these, only the first two are required in the signature, the rest are used to generate a private key for the next level.

Note: In fact, d_{ID} can be generated as follows: Given ID_{j-1}=(v_1,v_2,…,v_{j-1}) and $d_{ID|j-1} = (d_0', d_1', d_j', \cdots d_h')$, then d_{ID}= $(d_0, d_1, d_{j+1}\cdots, d_h)$ for ID=(v_1,v_2,…,v_j) can be computed in the following manners.

Let $\mathbf{d}_t' = \mathbf{H}_t^{\bar{r}} = (h_{tj}^{\bar{r}}) = (D_{tj}),\ j = 1,\cdots,n_j$ with $\bar{r} \in Z_p$. Select a random $r' \in Z_p$ and compute

$$d_0 = d_0' \prod_{k=1}^{n_j} D_{jk}^{v_j^k} (g_2 \prod_{i=1}^{j} F_i(v_i))^{r'}, d_1 = d_1' g^{r'},$$

$$\mathbf{d}_t = \mathbf{d}_t' \mathbf{H}_t^{r'} = (h_{tj}^{\bar{r}+r'}), t = j+1,\cdots,h.$$

***Sign*:** Let $m = (m_1,\cdots,m_{n_m})$ be a message to be signed and $m_i \in Z_p$. A signature of m for the identity ID=(v_1,v_2,…,v_j) is generated as follows: First, a random $s \in Z_p$ is chosen. Then the signature is constructed as

$$\sigma = (\sigma_1, \sigma_2, \sigma_3) = (d_0 (u_0 \prod_{i=1}^{n_m} u_i^{m_i})^s, g^r, g^s).$$

***Verify*:** Given a signature $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ of a message m under the identity $ID=(v_1,v_2,\ldots,v_j)$ with $j \le h$, the verifier computes $F_i(v_i)$ and accepts it if the following equation holds:

$$\hat{e}(\sigma_1,g)=\hat{e}(g_1,g_2)\hat{e}(g_3\prod_{i=1}^{j}F_i(v_i),\sigma_2)\hat{e}(u_0\prod_{i=1}^{n_m}u_i^{m_i},\sigma_3)$$

Otherwise rejects it.

3.1 Efficiency

The public parameters in our scheme are slightly larger than those in existing HIBS schemes. However, the private keys size in our scheme shrinks as the identity depth increases and the signature size is a constant consisting of three group elements. And the cost of verifying algorithm in our scheme needs three pairing operations(the value $\hat{e}(g_1,g_2)$ can be precomputed), which is more efficient than the existing HIBS schemes. In addition, if the value $u_i^{m_i}$ can be precomputed, a much more efficient signing algorithm is obtained where it only needs two exponentiation operations. Furthermore, our scheme is based on the *h*-CDH assumption instead of the other strong assumptions and is provably secure in the standard model. Table 1 compares our proposed scheme with other HIBS schemes. Tables 2-4 give the comparisons between our scheme and the others schemes in the standard model.(Note : the scheme in [12]and [18] is the same)

Table 1 Comparison of the Efficiency

Scheme	Hardness assumption	Security Model	Without Random oracles	Signature Size	Paring
[10]	CDH	s-ID	NO	$(k+2)\|G\|$	3
[11]	CDH	Gs-ID	NO	$(k+2)\|G\|$	$K+2$
[17]	*orc*YW	s-ID	YES	$4\|G\|$	7
[18]	*q*-SDH	Full	YES	$2\|G\|+\|p\|$	4
Ours	*h*-CDH	Gs-ID	YES	$3\|G\|$	3

Note: In this table, Pair denotes the number of pairing operation; s-ID denotes the security model of selective-identity [8]; Gs-ID denotes the security model of generalization selective-identity and Full denotes the security model of adaptive-identity [6].

Table 2 Comparison of the cost at the *Extract* Phase

scheme	Mul	Exp.	M.I.	Private key size
[17]	j+1	O(h)	0	O(h-j)
[18]	O(h)	O(h)	O(h)	O(h-j)
Ours	O(h)	O(h)	0	O(h- j)

Note: Mul. denotes multiplications computation, Exp. represents exponentiations computation, MI. denotes modular inverse computation and j denotes the j-level of HIBS. In addition, in our scheme, $\sum_{i=1}^{h}n_i$ is only a small multiple of h where $n_i \ge 1$. Hence we set $\sum_{i=1}^{h}n_i$ = O(h).

Table 3 Comparison of the cost at the *Sign* Phase

scheme	Mul	Exp.	M.I.	Hash	Signature size
[17]	j+4	j+7	0	1	$4\|G\|$
[18]	2j	2j-1	O(h)	0	$2\|G\|+p$
Ours	n_m or 1	2	0	0	$3\|G\|$

Note: Hash denotes the hash function and n_m denotes the length of the signed message m. When $u_0\prod_{i=1}^{n_m}u_i^{m_i}$ is precomputed, then the Mul. is 1.

Table 4 Comparison of the cost at the *Verify* Phase

scheme	Mul.	Exp.	M.I.	Hash	Pair
[17]	3	1	0	0	7
[18]	2j-3	2j-2	O(h)	0	4
Ours	$\sum_{i=1}^{h}n_i+n_m$ or 0	$\sum_{i=1}^{h}n_i+n_m$ or 0	0	0	3

Note: When $u_0\prod_{i=1}^{n_m}u_i^{m_i}$ and $F(v_i)$ are precomputed in our scheme, then Mul. and Exp. are 0.

4 Security

4.1 Correctness

Let $\sigma=(\sigma_1,\sigma_2,\sigma_3)$ be a valid signature. Then one can obtain

$$\hat{e}(\sigma_1,g)=\hat{e}(d_0(u_0\prod_{i=1}^{n_m}u_i^{m_i})^s,g)$$

$$=\hat{e}(g_2^{\alpha}(g_3\prod_{i=1}^{k}F_i(v_i))^r(u_0\prod_{i=1}^{n_m}u_i^{m_i})^s,g)$$

$$=\hat{e}(g_2^{\alpha},g)\hat{e}((g_3\prod_{i=1}^{k}F_i(v_i))^r,g)\hat{e}((u_0\prod_{i=1}^{n_m}u_i^{m_i})^s,g)$$

$$=\hat{e}(g_1,g_2)\hat{e}(g_3\prod_{i=1}^{k}F_i(v_i),\sigma_2)\hat{e}(u_0\prod_{i=1}^{n_m}u_i^{m_i},\sigma_3)$$

4.2 Existential Unforgeability

Let q_e and q_s denote the maximum time by the adversary querying the Extraction Oracles and Signing Oracles and $n = \sum_{i=1}^{h} n_i$. Then one can obtain:

Theorem 1 The proposed scheme is $(t, q_e, q_s, \varepsilon)$-secure, assume that the (t', ε') h-CDH assumption holds, where $\varepsilon \le \varepsilon'$, $t' = t + O((q_e n + q_s(n + n_m))\tilde{n} + (n q_e + q_s)\hat{o})$, t is the time taken by the adversary, $\tilde{n}$ is the time for a multiplication and $\hat{o}$ is the time for an exponentiation.

Proof: Suppose there exists a $(t, q_e, q_s, \varepsilon)$ adversary A against our scheme, then we construct an algorithm B that solves the (t', ε') h-CDH problem. Our method is based on the [14, 19]. We define the game between A and B as follows:

Init The adversary commits to sets of identities $I_1^*, \cdots, I_j^*$, where $1 \le j \le h$.

Setup B randomly picks $v_0, z_0, m_i, x_i, y_i \in Z_p$ $1 \le i \le n_M$, sets $\mathbf{M} = (m_i)$, $\mathbf{X} = (x_i)$, $\mathbf{Y} = (y_i)$. Then he defines some functions as follows:

$$f_i(x) = \begin{cases} \prod_{v \in I_i^*} (x - v) = x^{n_i} + a_{i,n_i-1} x^{n_i-1} + \cdots + a_{i,1} x + a_{i,0} & 1 \le i \le j \\ x & j+1 \le i \le h \end{cases};$$

$$J_i(x) = b_{i,n_i} x^{n_i} + b_{i,n_i-1} x^{n_i-1} + \cdots + b_{i,1} x + b_{i,0} \quad 1 \le i \le h$$

;

$$f(\mathbf{M}) = p + v_0 + \sum_{i=1}^{n_M} x_i m_i ;$$

$$J(\mathbf{M}) = z_0 + \sum_{i=1}^{n_M} m_i y_i ;$$

where $a_{ij}, b_{ij} \in Z_p$ with $1 \le j \le n_i$, $x \in Z_p^*$. Note that $a_{in_i} = 1$, where $1 \le i \le j$, $a_{il} = 0$, $j+1 \le i \le h, l \ne 1$, $a_{i1} = 1$.

Next, B constructs a set of public parameters for the HIBS scheme by making the following assignments. B takes as input a tuple $\{g, Y_1, Y_2, \cdots, Y_h\}$, where g is a random generator of G and $Y_i = g^{\alpha^i}$ for some random $\alpha \in Z_p$. Then B chooses a random $\beta \in Z_p$ and assigns:

$$g_1 = Y_1 = g^{\alpha}, g_2 = Y_h \cdot g^{\beta} = g^{\alpha^h + \beta},$$

$$g_3 = \prod_{i=1}^{h} (g^{b_{i0}} Y_{h-i+1}^{a_{i0}}).$$

Then for $1 \le i \le h, 1 \le j \le n_i$, define

$$h_{ij} = g^{b_{ij}} Y_{h-i+1}^{a_{ij}}, \; u_0 = g_2^{p+v_0} g^{z_0},$$

$$u_k = g_2^{x_k} g^{y_k}, \; 1 \le k \le n_M .$$

Finally, B sends

$$param = (g, g_1, g_2, g_3, u_0, \mathbf{H}_1, \cdots, \mathbf{H}_h, \mathbf{U})$$

to A. The master key g_2^{α} is unknown to B.

Queries: The adversary A will issue private key queries and signing queries and B answers these in the following way:

Private key queries: Suppose the adversary A issues a query for an identity *ID* = (v_1, . . . , v_j) with $j \le h$. B checks whether there exists a $k \in \{1, \cdots, j\}$ so that $f_k(v_k) \ne 0$. He aborts if there is no such *k*. In fact, there must be a $k \in \{1, \cdots, j\}$ so that $f_k(v_k) \ne 0$, otherwise $v_i \in I_i^*$ which is not allowed by the security model. Then B can construct a valid private key for *ID*. It is described as follows:(Note that this method is similar to that of [14,19])

Choose randomly a $r \in Z_p$ and define

$$A_1 = Y_1^{\beta} (\prod_{i=1}^{j} Y_k^{J_i(v_i)})^{-\frac{1}{f_k(v_k)}} (\prod_{i=1}^{j} Y_{h-i+1}^{f_i(v_i)} g^{J_i(v_i)})^r ;$$

$$A_2 = (\prod_{i=1, i \ne k}^{j} Y_{h+k-i+1}^{f_i(v_i)})^{-\frac{1}{f_k(v_k)}} ;$$

$$A_3 = \prod_{i=j+1}^{h} ((g^{b_{i0}} Y_{h-i+1}^{a_{i0}})^r (Y_k^{b_{i0}} Y_{h+k-i+1}^{a_{i0}})^{-\frac{1}{f_k(v_k)}}).$$

Then we have

$$\begin{aligned} d_0 &= A_1 A_2 A_3 \\ &= Y_{h+1} Y_{h+1}^{-1} A_1 A_2 A_3 \\ &= g_2^{\alpha} (g_3 \prod_{i=1}^{j} F_i(v_i))^{r - \frac{\alpha^k}{f_k(v_k)}} \\ &= g_2^{\alpha} (g_3 \prod_{i=1}^{j} F_i(v_i))^{r'} \end{aligned}$$

and $d_1 = Y_k^{-\frac{1}{f_k(v_k)}} g^r = g^{r - \frac{\alpha^k}{f_k(v_k)}} = g^{r'}$.

In order to obtain valid $\mathbf{H}_i^r = (h_{i1}^r, \cdots, h_{in_i}^r)$, $j+1 \le i \le h$. B computes

$$(g^{bil} Y_{h-i+1}^{ail})^r (Y_k^{b_{il}} Y_{h+k-i+1}^{a_{il}})^{-\frac{1}{f_k(v_k)}}$$

$$= (g^{b_{il}} Y_{h-i+1}^{a_{il}})^{r-\frac{\alpha^k}{f_k(v_k)}} = h_{il}^{r'}.$$

Finally, B responds with

$$d_{ID} = (d_0, d_1, d_{j+1} \cdots, d_l)$$

$$= (g_2^{\alpha} (g_3 \prod_{i=1}^{k} F_i(v_i))^{r'}, g^{r'}, \mathbf{H}_{j+1}^{r'}, \cdots, \mathbf{H}_h^{r'}).$$

Note that d_{ID} is valid private key on *ID*.

Signing queries: Consider a query for a signature of *M* under *ID*. A makes an extraction query on *ID* at first using the previous manner. Then B will construct a signature in a similar way to the construction of a private key in an extract query.

If $F(M)$ =0, then B will abort. Otherwise B selects randomly $r, s \in Z_p^*$ and computes

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

=

$$((g_3 \prod_{i=1}^{j} F_i(v_i))^r g_1^{-\frac{J(M)}{F(M)}} (u_0 \prod_{i=1}^{n_M} u_i^{m_i})^s, g_1^{-\frac{1}{F(M)}} g^s, g^r)$$

$$= (g_2^{\alpha} (g_3 \prod_{i=1}^{j} F_i(v_i))^r (g_2^{F(M)} g^{J(M)})^{s-\frac{\alpha}{F(M)}}, g^{s-\frac{\alpha}{F(M)}}, g^r)$$

$$= (g_2^{\alpha} (g_3 \prod_{i=1}^{j} F_i(v_i))^r (u_0 \prod_{i=1}^{n_M} u_i^{m_i})^{s'}, g^{s'}, g^r),$$

where $s' = s - \frac{\alpha}{F(M)}$. Note that $u_0 \prod_{i=1}^{n_M} u_i^{m_i} = g_2^{F(M)} g^{J(M)}$.

It shows that σ is a valid signature of *M* under the identity *ID*.

Forgery A outputs the challenge message $M^* = (m_1^* \cdots m_{n_M}^*)$ and an identity $ID^* = (v_1^*, \cdots, v_j^*)$, where $v_i^* \in I_i^*$. Then A outputs a valid forged signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$ of M^* for ID^*, where $v_i^* \in I_i^*$. If there exists a v_j^* such that $f_j(v_j^*) \neq 0$ or $F(M^*) \neq 0$, then B will abort. Otherwise, using the signature $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$, B can solve the *h*-CDH problem. In fact,

$$\sigma^* / (\sigma_2^{J(M^*)} \sigma_3^{\sum_{i=1}^{j} J_i(v_i^*)} Y_1^{\beta})$$

$$= (g_2^{\alpha} (g_3 \prod_{i=1}^{j} F_i(v_i^*))^r (u_0 \prod_{i=1}^{n_M} u_i^{m_i^*})^s) / (g^{sJ(M^*)} g^{r \sum_{i=1}^{j} J_i(v_i^*)} g^{\alpha\beta})$$

$$= g^{\alpha^h + 1},$$

where

$$g_3 \prod_{i=1}^{j} F_i(v_i^*) = \prod_{i=1}^{j} Y_{h-i+1}^{f_i(v_i^*)} g^{J_i(v_i^*)} = g^{\sum_{i=1}^{j} J_i(v_i^*)},$$

$$u_0 \prod_{i=1}^{n_M} u_i^{m_i^*} = g_2^{F(M^*)} g^{J(M^*)} = g^{J(M^*)}$$

and $g_2^{\alpha} = g^{\alpha^h + 1} g^{\alpha\beta}$.

One can easily obtain $\varepsilon \leq \varepsilon'$ in [14, 19]. The time complexity of the algorithm B is dominated by the exponentiations and, for larger values of $n = \sum_{i=1}^{h} n_i$ and n_M, multiplications performed in the extract and sign queries. Since there are $O(n)$ and $O(n + n_M)$ multiplications and $O(n)$ and $O(1)$ exponentiations in the extract and sign stage respectively, the time complexity of B is $t' = t + O((q_e n + q_s(n + n_M))\tilde{n} + (n q_e + q_s)\hat{o})$.

5 Conclusions

In this paper, a new short HIBS scheme is obtained based on the recent advance of the HIBE and HIBS. The new scheme is constructed in the standard model and has a constant-size signature. In addition, it has efficient signing algorithm and verifying algorithm under the precomputed, since only two exponentiation operations is needed to the signing algorithm and three pairing operations for the verifying algorithm. Furthermore, we prove the security of the new scheme under the *h*-CDH assumption instead of the other strong assumption.

Acknowledgments

This work is supported in part by the Nature Science Foundation of China under grant 60673072 and the National Basic Research Program of China(973) under grant 2007CB311201.

References

[1] A. Shamir. “Identity-based Cryptosystems and Signature Schemes”. *Proceeding of the Crypto 1984*, Blakley G. R, Chaum D, ed., Berlin: Springer-Verlage, Santa Barbara, California, USA , LNCS 196, pp. 47-53.

[2] D. Boneh, M. Franklin. “Identity Based Encryption from the Weil Pairing”. *Proceeding of the Crypto* 2001, Kilian J,ed. New York: Springer-Verlage, California, USA, LNCS 2139, pp. 213-229.

[3] D. Boneh and J. Katz. “Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption”. *Proceeding of the CT-RSA’05*, Alfred John Menezes, ed., LNCS 3376, pp. 87-103.

[4] B. Waters . "Efficient Identity-based Encryption without Random Oracles". *Proceeding of the Eurocrypt 2005,* Ronald Cramer, ed. Springer-Verlage, Aarhus, Denmark, LNCS 3494, pp. 114-127.
[5] Kenneth G. Paterson and Jacob C.N. Schuldt, "Efficient Identity-Based Signatures Secure in the Standard Model." *Proceeding of the ACISP 2006*, Batten L, Safavi-Naini R, ed., Springer-Verlag, Melbourne, Australia, LNCS 4058, pp. 207-222.
[6] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography", *Proceeding of the ASIACRYPT 2002*, Yuliang Zheng, ed., Queenstown, Springer-Verlag, LNCS 2501, pp. 548-566.
[7] J. Horwitz and B. Lynn. "Towards Hierarchical Identity-Based Encryption". *Proceeding of the EUROCRYPT 2002*, Lars Knudsen, ed., Berlin: Springer-Verlag, Amsterdam, The Netherlands, LNCS 2332, pp. 466-481.
[8] D. Boneh, X. Boyen. "Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles", *Proceeding of the EUROCRYPT 2004*, Christian Cachin and Jan Camenisch, ed., Springer-Verlag, Switzerland , LNCS 3027, pp. 223-238.
[9] D. Boneh, X. Boyen and E.Goh. "Hierarchical Identity based encryption with constant ciphertext". *Proceeding of the Eurocrypt'05*, Ronald Cramer, ed., Springer-Verlag, Denmark, LNCS 3494, pp. 440-456.
[10] Sherman S.M. Chow, Lucas C.K. Hui and S. Yiu, *et al*. "Secure Hierarchical Identity Based Signature and Its Application". *Proceeding of ICICS 2004*, Javier Lopez, Sihan Qing, Eiji Okamoto, ed., Springer-Verlag, Malaga, Spain,LNCS 3269, pp. 480-494.
[11] J. Lin and F.G.. Zhang et al. "A New Hierarchical ID-Based Cryptosystem and CCA-Secure PKE". *Proceeding of the EUCWorkshops 2006*, Xiaobo Zhou,*et al* ed. Springer-Verlag, Korea ,LNCS 4097, pp. 362-371.
[12] Man Ho Au, Joseph K. Liu, Tsz Hon Yuen, and Duncan S. Wong, "Practical Hierarchical Identity Based Encryption and Signature schemes Without Random Oracles". http://eprint.iacr.org/2006/308.
[13] Canetti, S. Halevi, and J. Katz.. "Chosen ciphertext security from identity-based encryption". *Proceeding of the EuroCrypt'04*, Christian Cachin and Jan Camenisch, ed., Springer-Verlag, Switzerland ,LNCS 3027, pp. 207-222.
[14] Sanjit Chattterjee and Palash Sarkar. "Generalization of the Selectve-ID Security Model for HIBE Protocols." *Proceeding of the PKC 2006*, Moti Yung, *et al* ed., Springer-Verlag, New York, USA, LNCS 3958, pp. 241-256.
[15] Moni Naor and Moti Yung. "Public key cryptosystems provable secure against chosen ciphertext attacks". *Proceeding of the STOC 1990*, ACM, pp. 427-437.
[16] Amit Sahai. "Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security". *Proceedings 40 IEEE Symp. on Foundations of Computer Science1999*, New York: IEEE, pp. 543-553.
[17] T.H.Yuen and V.K.Wei. "Constant-Size Hierarchical Identity-Based Signature/ Signcryption without Random Oracles". Cryptology ePrint Archive, Report 2005/412, 2005. http://eprint.iacr.org/.
[18] Man Ho Au and Joseph K.Liu *et cl*, "Efficient Hierarchical Identity Based Signature in the Standard Model". http://eprint.iacr.org/2006/080.
[19] Sanjit Chatterjee and Palash Sarkar, New Constructions of Constant Size Ciphertext HIBE Without Random Oracle, *Proceeding of the ICISC 2006*, M.S. Rhee and B. Lee ed., Springer-Verlag, LNCS 4296, pp. 310-327.
[20] F. Zhang, R. Safavi-Naini,W.Susilo. "An efficient signature scheme from bilinear pairings and its applications." *Proceeding of the PKC 2004*, Feng Bao, ed., Springer-Verlag, Singapore, LNCS 2947, pp. 277-290.
[21] Joel Reardon, The Strong Diffie-Hellman Problem. http://www.cs.uwaterloo.ca/~jreardon/ sdh.pdf.

Leyou Zhang was born in 1977. He received the Ph. D degrees in applied mathematics form Xidian University of China in 2009. Now he is an associate professor in Department of Mathematical Sciences of Xidian University. His main research interests include *secure protocol* and *public key cryptography*.

Yupu Hu was born in 1955. He received the Ph. D degrees in School of Telecommunication Engineering form Xidian University of China in 2008. Now he is a professor in School of Telecommunication Engineering of Xidian University in Xidian University. His main research interests include *information security* and *cryptography*.