A New Hierarchical ID-Based Cryptosystem and CCA-Secure PKE*

Jin Li[1], Fangguo Zhang[2,3], and Yanming Wang[1,4]

[1] School of Mathematics and Computational Science,
Sun Yat-sen University,
Guangzhou, 510275, P.R. China
sysjinli@yahoo.com.cn
[2] Department of Electronics and Communication Engineering,
Sun Yat-sen University,
Guangzhou, 510275, P.R. China
[3] Guangdong Key Laboratory of Information Security Technology,
Sun Yat-sen University,
Guangzhou, 510275, P.R. China
isszhfg@mail.sysu.edu.cn
[4] Lingnan College, Sun Yat-sen University,
Guangzhou, 510275, P.R. China
stswym@mail.sysu.edu.cn

Abstract. A new hierarchical identity based (ID-based) cryptosystem is proposed, including hierarchical identity based encryption (HIBE) and signature (HIBS) schemes. The new HIBE scheme can be proved to be secure without relying on the random oracle model. Then, a new public key encryption (PKE) scheme is constructed based on the new HIBE. It is secure against adaptively chosen ciphertext attacks (IND-CCA) and has many attractive properties, such as efficient key generation, short private key, fast encryption, and etc. Performance of the new PKE scheme is better than all the previous PKE schemes converted from IBE, and is competitive with the best provably secure solutions to date. Furthermore, a new HIBS scheme is also constructed, which shares the same parameters with the new HIBE. The new HIBS scheme is more efficient than the previous HIBS.

Keywords: Identity based, Public key encryption, Bilinear groups.

1 Introduction

ID-based cryptosystem [21] is a public key cryptosystem where the public key can be an arbitrary string such as an email address. A private key generator (PKG) uses a master secret key to issue private keys to identities that request

* This work is supported by the National Natural Science Foundation of China (No. 60403007 and No. 10571181) and Natural Science Foundation of Guangdong Province, China (No. 04205407) and the Project-sponsored by SRF for ROCS, SEM.

X. Zhou et al. (Eds.): EUC Workshops 2006, LNCS 4097, pp. 362–371, 2006.

them. Many Identity-Based signature (IBS) schemes have been proposed such as [2,13,22] since shamir proposed the ID-based notion. However, until 2001, Boneh and Franklin [9] proposed the first practical identity-based encryption scheme, which is provably secure in the random oracle model. However,using a single PKG is not efficient in large scale, so another research direction is hierarchical ID-based cryptosystem [17]. In the hierarchical version, PKGs are arranged in a tree structure, the identities of users (and PKGs) can be represented as vectors. An identity can issue private keys to its descendant identities. All the PKGs in the leaves are responsible for generating private keys for users in the corresponding domain.

Related Work. Gentry and Silverberg proposed the first scalable provably secure HIBE [16] in the random oracle model. Canetti, Halevi, and Katz [12] introduced a slightly weaker security model, called selective identity (selective-ID) IBE. In this model the adversary must commit ahead of time (non-adaptively) to the identity it intends to attack. The adversary can still issue adaptive chosen ciphertext and adaptive chosen identity queries. Later, Boneh and Boyen proposed a provably selective-ID secure HIBE [6,7] without random oracles.

Recently, Canetti et al. [12] showed a generic method to construct efficient CCA-secure PKE from selective-ID IBE combined with one-time signatures. Later, Boneh and Katz [10] improved the efficiency of the generic construction of PKE [12] by replacing the one-time signatures with message authentication code and key encapsulation. They also showed two instantiations of PKE, denoted by BK-1 scheme and BK-2 scheme, respectively. As also pointed in [10], the BK-2 scheme is more efficient than BK-1. However, the BK-2 scheme relies on the non-standard Decision q-Bilinear Diffie-Hellman Inversion (Decision q-BDHI) problem. Decision q-BDHI problem can be informally stated as follows: for $\mathbb{G} =< g >, \mathbb{G}_T$ of large prime order p, and a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, given $g, g^{\alpha}, \cdots, g^{\alpha^q}$ for unknown $\alpha \in \mathbb{Z}_p^*$, $T \in \mathbb{G}_T$, there is no probabilistic polynomial time algorithm able to decide if $T = \hat{e}(g,g)^{\frac{1}{\alpha}}$. The Decision q-BDHI assumption which BK-2 based on is very strong, for if the PKE is IND-CCA secure, then q should be greater than the decryption query times. Corresponding to HIBE, the first HIBS was proposed by Chow et al. [14]. The HIBS is provably secure against existential forgery for selective-ID, adaptive chosen-message-and-identity attack (EF-sID-CMIA) and shares the same system parameters and key generation process with [6]. However, the signature generation is inefficient and reduction is not tight for the technique of forking lemma [20] used in their construction.

Contributions

1. We propose a new HIBE scheme. It can be proved to be selective-ID secure without relying on the random oracle model.
2. A very efficient PKE scheme is constructed based on the new HIBE, which is the main contribution of this paper. Our new PKE scheme is as efficient as the best PKE [10] converted from IBE. Moreover, the new PKE is based

on Decision 1-BDHI (not q-BDHI as [10]), which is independent with the decryption query times. So, the new PKE scheme is better than BK-2 and its performance is competitive with the best provably secure solutions to date [18].
3. A corresponding HIBS scheme is also constructed, which shares the same parameters with the new HIBE. The new HIBS is very efficient: The signature generation only needs two exponentiation regardless of the hierarchy depth. It does not rely on the forking lemma [20] and it has a very tight security reduction.

Organization. The next section presents the HIBE security model and briefly explains the bilinear pairing and some problems related to pairings. Section 3 gives the new HIBE construction and security analysis. section 4 is the new PKE construction. In section 5, a new HIBS shares the same parameters with HIBE in section 3 is constructed. Its security analysis and efficiency are also given in this section. The paper ends with some concluding remarks.

2 Preliminaries

2.1 Security Model

Definition 1. (HIBE) *An ℓ-level HIBE (ℓ-HIBE) scheme handling identities of hierarchy depth ℓ consists of four algorithms:* ($\mathsf{Setup}, \mathsf{Der}, \mathsf{Enc}, \mathsf{Dec}$). *The algorithms are specified as follows:*

- **Setup.** *On input a security parameter 1^k, the PKG generates msk and $param$ where msk is the randomly generated master secret key, and $param$ is the corresponding public parameter.*
- **Der.** *On input an identity vector $ID = (I_1, \ldots, I_k)$, where all $I_k \in \mathbb{Z}_p^*$ and $k < \ell$, and the private key $S_{ID|_{k-1}}$ for its parent identity $ID|_{k-1} = (I_1, \ldots, I_{k-1})$, it returns the corresponding private key S_{ID}.*
- **Enc.** *On input ID, a message M, and a random value s, it outputs a ciphertext $\mathcal{C}$.*
- **Dec.** *On input the $\mathcal{C}$ and private key S_{ID}, it outputs M if $\mathcal{C}$ is a valid ciphertext. Otherwise, it outputs $\perp$.*

We define the following oracles:

- Extraction Oracle $\mathcal{EO}$: The Key Extraction Oracle with input ID will output the corresponding secret key S_{ID}.
- Decryption Oracle $\mathcal{DO}$: The Decryption Oracle with input $\mathcal{C}$ will output a M if $\mathcal{C}$ is a valid ciphertext. Otherwise, it outputs a distinguished symbol $\perp$.

Canetti et al. [12] defined a security notion for HIBE as chosen ciphertext for selective-ID, adaptive chosen identity and chosen ciphertext attacks (IND-sID-CCA). Its formal definition is based on the following IND-sID-CCA game involving an adversary $\mathcal{A}$.

- *Init:* The adversary $\mathcal{A}$ outputs an identity ID*, which will be used to challenge $\mathcal{A}$.
- *Setup:* Take a security parameter 1^k and run Setup to generate common public parameters params and the master secret key msk. params is sent to $\mathcal{A}$.
- $\mathcal{A}$ queries $\mathcal{EO}$ and $\mathcal{DO}$, restriction is that ID* or any prefix of ID* does not appear in any query to $\mathcal{EO}$.
- *Challenge:* $\mathcal{A}$ outputs an identity ID*, and two equal length plaintexts m_0,m_1 for challenge ciphertext. Choose a random $b \in \{0,1\}$ and send the challenge ciphertext $\mathcal{C}$=Enc(ID^*, m_b) to $\mathcal{A}$.
- $\mathcal{A}$ continues to query $\mathcal{EO}$ and $\mathcal{DO}$, restriction is that ID* or any prefix of ID*, and challenge ciphertext $\mathcal{C}$ have not been queried to $\mathcal{EO}$ and $\mathcal{DO}$, respectively.
- Finally, $\mathcal{A}$ outputs a guess bit b'.

We say that $\mathcal{A}$ wins the game if b'=b. The advantage $\mathbf{Adv}^{cca}_{\mathcal{A}}(1^k)$ of $\mathcal{A}$ is defined as the probability that it wins the game over $\frac{1}{2}$.

Definition 2. *An ℓ-HIBE scheme is secure if $\mathbf{Adv}^{cca}_{\mathcal{A}}(1^k)$ is negligible for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$.*

A weaker notion called selective identity secure against chosen plaintext attacks (IND-sID-CPA) is similar to IND-sID-CCA, except that the adversary cannot ask $\mathcal{DO}$ after the challenge ciphertext is given.

2.2 Pairings and Problems

Let $\mathbb{G}, \mathbb{G}_T$ be cyclic groups of prime order p, writing the group action multiplicatively. Let g be a generator of $\mathbb{G}$.

Definition 3. *A map $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is called a bilinear pairing if, for all $x, y \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$, we have $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$, and $\hat{e}(g, g) \neq 1$.*

Definition 4. *(**DHI** problem) The Diffie-Hellman Inversion (DHI) problem is that, given g, $g^\alpha \in (\mathbb{G})^2$ for unknown $\alpha \in \mathbb{Z}_p^*$, to compute $g^{\frac{1}{\alpha}}$.*

We say that the (t, ϵ)-DHI assumption holds in $\mathbb{G}$ if no t-time algorithm has the non-negligible probability ϵ in solving the DHI problem.

Definition 5. *(Decision **BDHI** problem) The Decision Bilinear Diffie-Hellman Inversion (Decision BDHI) problem is that, given g,$g^\alpha \in (\mathbb{G})^2$ for unknown $\alpha \in \mathbb{Z}_p^*$, $T \in \mathbb{G}_T$, to decide if $T = \hat{e}(g, g)^{\frac{1}{\alpha}}$.*

We say that the (t, ϵ) Decision BDHI assumption holds in $\mathbb{G}$ if no t-time algorithm has the probability at least $\frac{1}{2} + \epsilon$ in solving the Decision BDHI problem for non-negligible ϵ.

In fact, Boneh et al. [6] actually also defined a problem called q-BDHI. When $q = 1$, Decision 1-BDHI is exactly the definition of Decision **BDHI** problem. It was also shown in [23] that **DHI** problem is equivalent to BDH problem. Obviously, Decision **BDHI** is a weaker version of Decision q-BDHI Problem when $q > 1$.

3 A New HIBE Scheme

Let $\mathbb{G}$ be a bilinear group of prime order p. Given a pairing: $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$.

Setup. To generate system parameters, the algorithm selects a random generator g, h_1, ..., $h_\ell \in (\mathbb{G})^{\ell+1}$, picks a random $\alpha \in \mathbb{Z}_p$, and sets $g_1 = g^\alpha$. The system parameters $\mathsf{param} = (g, g_1, h_1, \ldots, h_\ell)$ and the master key is $g^{\frac{1}{\alpha}}$. Meanwhile, l functions are also defined as $F_j(x) = g^x h_j$ for $1 \leq j \leq \ell$.

Der. To generate a private key for ID $=(I_1, \ldots, I_k)$, where $k \leq \ell$, the algorithm picks random $r_1, r_2, \cdots, r_k \in (\mathbb{Z}_p)^k$ and returns $S_{ID} = (a_0, a_1, \ldots, a_k)$, where $a_0 = g^{\frac{1}{\alpha}} \prod_{i=1}^{k} (F_i(I_i))^{r_i}$, $a_1 = g_1^{r_1}$, $\cdots$, $a_k = g_1^{r_k}$. In fact, the private key for ID can also be generated as $S_{ID} = (a'_0(F_k(I_k))^{r_k}, a'_1, \ldots, a'_{k-1}, g_1^{r_k})$ by its parent $ID_{|k-1} = (I_1, \ldots, I_{k-1})$ with secret key $S_{ID_{|k-1}} = (a'_0, a'_1, \ldots, a'_{k-1})$.

Enc. To generate the ciphtertext on a plaintext $M \in \mathbb{G}_T$ with respect to ID, pick $s \in_R Z_p^*$, output ciphertext $\mathcal{C} = (A, B, C_1, \cdots, C_k)$, where $A = \hat{e}(g, g)^s \cdot M$, $B = g_1^s, C_1 = (F_1(I_1))^s, \cdots, C_k = (F_k(I_k))^s$.

Dec. On input ciphertext $\mathcal{C} = (A, B, C_1, \cdots, C_k)$, private key $S_{ID} = (a_0, a_1, \ldots, a_k)$ for ID$=(I_1, \cdots, I_k)$, output the plaintex $M = A \cdot \frac{\prod_{i=1}^{k} \hat{e}(a_i, C_i)}{\hat{e}(a_0, B)}$.

3.1 Correctness and Efficiency Analysis

Correctness is obvious. We show the efficiency analysis as follows: The new HIBE system is the first HIBE based on the Decision BDHI assumption, and it is as efficient as [6]. Boneh et al. [7] also gave a HIBE with constant ciphertext, however, it is based on a non-standard and not well-studied assumption called q-Bilinear Diffie-Hellman Exponent (q-BDHE) assumption.

3.2 Security Result

Theorem 1. *Assume the (t, ϵ) Decision BDHI assumption holds, then the new ℓ-HIBE is (t', q_E, ϵ)-sID-CPA secure, where q_E is the extraction times and $t' < t - \Theta(\ell q_E t_{exp})$, in which t_{exp} is the maximum time for an exponentiation in $\mathbb{G}$.*

Proof. Suppose for contradiction that there exists an adversary $\mathcal{A}$ breaks the scheme, then we show there exists an algorithm $\mathcal{C}$ that, by interacting with $\mathcal{A}$, solves the decision Decision BDHI problem. Our algorithm $\mathcal{C}$ described below solves Decision BDHI problem for a randomly given instance $\{g, X = g^\alpha, T\}$ and asked to decide if $T = \hat{e}(g, g)^{\frac{1}{\alpha}}$. The details are as follows.

Init: $\mathcal{A}$ first outputs target identity $ID^* = (I_1^*, \cdots, I_k^*) \in \mathbb{Z}_p^k$ of depth $k \leq l$. $\mathcal{C}$ appends random elements $(I_{k+1}^*, \cdots, I_l^*) \in \mathbb{Z}_p^{l-k}$ such that ID* is an vector of length l. Hence, from here we assume that ID* is a vector of length l.

Setup: Algorithm $\mathcal{C}$ generates the system parameters by picking $\alpha_1, \cdots, \alpha_l \in \mathbb{Z}_p$ at random and defines $g_1 = X$, $h_i = g^{-I_i^*} g_1^{\alpha_i}$ for $i = 1, 2, \cdots, l$. The system parameters $\mathsf{params}= (g, g_1, h_1, h_2, \cdots, h_l)$ are sent to $\mathcal{A}$. The corresponding master key, which is unknown to $\mathcal{C}$, is $g^{\frac{1}{\alpha}}$.

Extraction query: Let ID=$(I_1, \cdots, I_m)$ be the identity for private key query, where $t \leq l$. Assume n is the minimum value such that $I_n \neq I_n^*$. $\mathcal{C}$ computes the simulated private key for ID as follows: Pick $r_1, \cdots, r_{n-1}, r'_n, r_{n+1}, \cdots, r_m \in \mathbb{Z}_p^*$. Output the simulated private key $S_{ID} = (g^{-\frac{\alpha_n}{I_n - I_n^*}} (F_n(I_n))^{r'_n} \prod_{i=1, i\neq n}^{m} (F_i(I_i))^{r_i}$, $g_1^{r_1}, \cdots, g_1^{r_{n-1}}, g_1^{r'_n} g^{-\frac{1}{I_n - I_n^*}}, g_1^{r_{n+1}}, \cdots, g_1^{r_m})$. The correctness of the private key can be verified as follows:

Let $r_n = r'_n - \frac{1}{(I_n - I_n^*)\alpha}$ (which is not known to $\mathcal{C}$), then $g^{-\frac{\alpha_n}{I_n - I_n^*}} F_n(I_n)^{r'_n} = g^{-\frac{\alpha_n}{I_n - I_n^*}}$ $(g^{I_n - I_n^*} g_1^{\alpha_n})^{r'_n} = g^{\frac{1}{\alpha}} F_n(I_n)^{r_n}$. So, $(g^{-\frac{\alpha_n}{I_n - I_n^*}} F_n(I_n)^{r'_n} \prod_{i=1, i\neq n}^{m} F_i(I_i)^{r_i}, g_1^{r_1}, \cdots,$ $g_1^{r_{n-1}}, g_1^{r'_n} g^{-\frac{1}{I_n - I_n^*}}, g_1^{r_{n+1}}, \cdots, g_1^{r_m}) = (g^{\frac{1}{\alpha}} \prod_{i=1}^{k} (F_i(I_i))^{r_i}, a_1 = g_1^{r_1}, \cdots, a_k = g_1^{r_k})$ is a valid private key from the view of $\mathcal{A}$.

Challenge: After received $(m_0, m_1,$ ID*=$(I_1^*, \cdots, I_k^*))$ for challenge ciphertext, $\mathcal{C}$ picks a random bit $b \in \{0, 1\}$, $r \in_R Z_p^*$, and outputs the challenge ciphtertext as $\mathrm{C} = (T^r \cdot m_b, g^r, g^{\alpha_1 r}, \cdots, g^{\alpha_m r})$. The challenge ciphertext is correct if $T = \hat{e}(g, g)^{\frac{1}{\alpha}}$: Let $s = \frac{r}{\alpha}$ (which is unknown to $\mathcal{C}$), then $F_i(I_i^*)^s = g^{\alpha_i r}$ and $\mathrm{C} = (\hat{e}(g, g)^s \cdot m_b, g_1^s, F_1(I_1^*)^s, \cdots, F_k(I_k^*)^s) = (T^r \cdot m_b, g^r, g^{\alpha_1 r}, \cdots, g^{\alpha_k r})$.

$\mathcal{A}$ can continue to query $\mathcal{EO}$ on ID and the only restriction is that ID is not a prefix or equal to ID*.

After the simulation, if the adversary outputs a guess bit b'. If $b' = b$, then $\mathcal{C}$ decide that $T = \hat{e}(g, g)^{\frac{1}{\alpha}}$. Otherwise, $T \neq \hat{e}(g, g)^{\frac{1}{\alpha}}$. It is easy to verify that if the advantage of $\mathcal{A}$ is ϵ, then $\mathcal{C}$ can also have an advantage ϵ to the Decision BDHI problem.

3.3 Chosen Ciphertext Security

Canetti et al. [12] showed an generic mehtod to build an IND-sID-CCA secure ℓ-HIBE from an IND-sID-CPA secure $(\ell + 1)$-HIBE. In combination with the above construction, we obtain a IND-sID-CCA secure ℓ-HIBE.

4 An Efficient CCA Secure Public Key Encryption

Recently, Canetti, Halevi, and Katz [12] showed a general method for constructing CCA-secure encryption schemes from an IND-sID-CPA IBE in the standard model, which was later improved by Boneh and Katz [10].

A public-key encryption scheme PKE is a triple of PPT algorithms: Key generation algorithm (Gen, encryption algorithm Enc and decryption algorithm Dec).

In order to design a CCA-secure PKE from IBE, it requires a message authentication code and an encapsulation scheme. We view a message authentication code as a pair of PPT algorithms (Mac; Vrfy). The authentication algorithm Mac takes as input a key and a message M, and outputs a string tag. The verification algorithm Vrfy takes as input the same key, a message M, and a string tag, output 1 if it is valid; otherwise, it outputs 0. We only require the message authentication code is secure against a one-time chosen-message attack. Meanwhile, the encapsulation scheme of [10] is used in our paper. For more details, the reader is referred to [10].

4.1 The CCA-Secure PKE Scheme

Let $\mathbb{G}$ be a bilinear group of prime order p. Given a pairing: $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. $\mathcal{G}$ is a pseudorandom generator. H is a hash function assumed to be second-preimage resistant such that $H : \{0,1\}^{k_1} \rightarrow \{0,1\}^k$. g is a generator of $\mathbb{G}$ and $Z = \hat{e}(g, g)$. The system public parameters are $\{\mathbb{G}, \mathbb{G}_T, \hat{e}, g, Z, H\}$.

1. **Gen.** Choose $\alpha, \alpha' \in (\mathbb{Z}_p^*)^2$ and set $g_1 = g^{\alpha}$ and $g' = g^{\alpha'}$. Meanwhile, choose hash function h from a family of pairwise-independent hash functions such that h: $\{0,1\}^{k_1} \rightarrow \{0,1\}^k$. The public key is $PK = \{g_1, g', h\}$ and the secret key is $SK = (\alpha, \alpha')$.

2. **Enc.** On input public key $PK = \{g_1, g', h\}$ and a message M, choose $r \in \{0,1\}^{k_1}$, let $k' = h(r)$ and $ID = H(r)$. Pick a random $s \in Z_p$ and set $C = (g_1^s, g^{s \cdot ID} g'^s, G(Z^s) \oplus (M \circ r))$. Output the ciphertext $(ID, C, \mathsf{tag} = \mathsf{Mac}_{k'}(C))$.

3. **Dec.** To decrypt the ciphertext (ID, C, tag), first parse $C = (C_1, C_2, C_3)$, pick a random $t \in Z_p$ and get $(M \circ r) = C_3 \oplus G(\hat{e}(C_1^{t(ID+\alpha')+\alpha^{-1}} C_2^{-t\alpha}, g))$. Set $k' = h(r)$ and output the plaintext M if $\mathsf{Vrfy}(k', C, \mathsf{tag}) = 1$ and $H(r) = ID$. Otherwise, output $\perp$.

4.2 Efficiency Analysis

The new PKE has many attractive properties. First, the key generation requires only two exponentiations in $\mathbb{G}$. Meanwhile, the computations in encryption algorithm are only 3.5 exponentiations (one multi-exponentiation is counted as 1.5 exponentiations), which is the same with [10,18]. In fact, it only requires 2.5 exponentiations in encryption for Z^s can be pre-computed. The decryption needs only 1.5 exponentiations and 1 pairing computations. So, computations of key generation, encryption and decryption of the new PKE system are the same with the BK-2 scheme.

As noted by Boneh et al. [10], the most efficient PKE converted from IBE is the BK-2 scheme in [10]. From the viewpoint of efficiency, the new PKE is is as efficient as BK-2. However, the BK-2 scheme was based on the strong and non-standard Decision q-BDHI assumption, where q is not less than the number of decryption queries from adversary. Compared to BK-2, the new PKE in this paper is better for it is based on the standard and well-studied Decision

BDHI (or Decision 1-BDHI) assumption. In conclusion, the new PKE is the most efficient encryption converted from IBE without random oracles to date and is competitive with the best provably secure solutions [18].

Theorem 2. *Assume the underlying IBE scheme is IND-sID-CPA secure, the message authentication code is secure against one-time chosen message attack, and encapsulation scheme used above satisfies computationally binding and hiding, then the new PKE scheme is IND-CCA Secure.*

The underlying IBE in this PKE construction is IND-sID-CPA secure from theorem 1. Meanwhile, the message authentication code and encapsulation scheme used are the same to [10]. So, the new PKE can be proved to be secure from the generic construction method in [10].

5 An Efficient HIBS

An ℓ-level HIBS (ℓ-HIBS) scheme handling identities of hierarchy depth ℓ consists of four algorithms: $(\mathsf{Setup}, \mathsf{Der}, \mathsf{Sign}, \mathsf{Verify})$. Meanwhile, Chow et al. [14] defined the security notion for HIBS as existential forgery for selective-ID, adaptive chosen message-and-identity attack (EF-sID-CMIA). It is referred to [14] for more details.

1. **Setup.** The parameters $(\hat{e}, \mathbb{G}, \mathbb{G}_T, g, g_1, h_1, \ldots, h_\ell)$ are the same with HIBE in section 3. Meanwhile, define a hash function $H : \{0,1\}^* \rightarrow \mathbb{G}$. Meanwhile and l functions $F_j(x) = g^x h_j$ for $1 \leq j \leq l$. Then, the system parameters are $\mathsf{param} = (\hat{e}, \mathbb{G}, \mathbb{G}_T, g, g_1, h_1, \ldots, h_\ell, H)$ and the master key is $g^{\frac{1}{\alpha}}$.
2. **Der.** The generation of private key for $ID = (I_1, \ldots, I_k)$ is the same with algorithm Der of HIBE in section 3. Let $S_{ID} = (a_0, a_1, \ldots, a_k)$, where $a_0 = g^{\frac{1}{\alpha}} \prod_{i=1}^{k} (F_i(I_i))^{r_i}$, $a_1 = g_1^{r_1}, \cdots, a_k = g_1^{r_k}$.
3. **Sign.** For a user with identity ID and private key $S_{ID} = (a_0, a_1, \ldots, a_k)$, he signs a message M as follows: pick a random $s \in \mathbb{Z}_p$, compute $T = g_1^s$ and $A = a_0 \cdot [H(M,T)]^s$. Output the signature as $\sigma = (A, T, a_1, \ldots, a_k)$.
4. **Verify.** After receive a signature $\sigma = (A, T, a_1, \ldots, a_k)$ on message M for ID$=(I_1, \cdots, I_k)$, check $\hat{e}(g_1, A) \stackrel{?}{=} \hat{e}(g,g)\hat{e}(T, H(M,T)) \prod_{i=1}^{k} (\hat{e}(F_i(I_i), a_i))$. Output 1 if it is true. Otherwise, output 0.

5.1 Efficiency Analysis

The values $a_1, \ldots, a_k$ in the signature are always the same. So, signature generation requires only two exponentiation operations in $\mathbb{G}$, regardless the hierarchy depth. However, the HIBS [14], requires $(l+2)$ exponentiation operations for an l-level user, which is very inefficient.

5.2 Security Result

We show that our HIBS scheme is secure against EF-sID-CMIA with very tight security reduction.

Theorem 3. *Assuming the* (t, ϵ)*-DHI assumption holds in* $\mathbb{G}$*, then our* ℓ*-HIBS scheme is* $(t', q_S, q_H, q_E, \epsilon')$*-secure against EF-sID-CMIA , where* $t' \leq t - \Theta((q_H + q_E + q_S)lt_{exp})$ *and* $\epsilon' \approx \epsilon$*,* t_{exp} *is the maximum time for an exponentiation in* $\mathbb{G}$*.*

For the page limitation, the security proof is not given in this paper. Please contact the author for full version of this paper if needed.

6 Conclusion

We propose a new HIBE and HIBS based on Decision BDHI and DHI assumptions, respectively. The new HIBE can be proved to be selective-ID secure against adaptively chosen identity and chosen ciphertext attacks. The new HIBS shares the same parameters with the new HIBE and it is the most efficient HIBS to date.

The Most important contribution of this paper is that an efficient PKE scheme is constructed based on the new HIBE. It is well known that the BK-2 scheme [10] is based on the strong and non-standard q-BDHI assumption, which depends on the decryption query times q. The new PKE, however, is based on a better and well-studied Decision BDHI assumption.

References

1. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. *Relations Among Notions of Security for Public-Key Encryption Schemes.* Crypto'98, LNCS 1462, pp. 26-45, Springer-Verlag, 1998.
2. M. Bellare, C.Namprempre, and G.Neven. *Security Proofs for Identity-based Identification and Signature Schemes.* EuroCrypt'04, LNCS 3027, pp. 268-286. Springer-Verlag, 2004.
3. M.Bellare, P.Rogaway. *Random oracles are practical: a paradigm for designing efficient protocols.* In First ACM Conference on Computer and Communications Security, ACM, 1993.
4. D. Boneh and X. Boyen. *Short Signatures Without Random Oracles.* EUROCRYPT'04, Proceedings, LNCS 3027, pp. 56-73, Springer-Verlag, 2004.
5. D. Boneh and X. Boyen. *Secure identity based encryption without random oracles.* Crypto'04, LNCS 3152, pp. 443-59, Springer-Verlag, 2004.
6. D. Boneh and X. Boyen. *Efficient selective-ID identity based encryption without random oracles.* EuroCrypt'04, LNCS 3027, pp. 223-238. Springer-Verlag, 2004.
7. D. Boneh, X. Boyen and E.Goh. *Hierarchical Identity based encryption with constant ciphertext.* EuroCrypt'05, LNCS 3494, pp. 440-456, springer-Verlag, 2005.
8. D. Boneh, X. Boyen and S. Halevi. *Chosen ciphertext secure public key threshold encryption without random oracles.* CT-RSA'05, LNCS 3860, pp. 226-243, springer-Verlag, 2006.
9. D. Boneh and M. Franklin, *Identity-based encryption from the Weil pairing*, Crypto'01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
10. D. Boneh and J. Katz. *Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption.* CT-RSA'05, LNCS 3376, pages 87-103, springer-Verlag, 2005.

11. X. Boyen, Q. Mei, and B.Waters. *Direct Chosen ciphertext security from identity-based techniques*. CCS'05. ACM press, 2005. Full version at http://eprint.iacr.org/2005/288.
12. Canetti, S. Halevi, and J. Katz. *Chosen-ciphertext security from identity-based encryption*. EuroCrypt'04, LNCS 3027, pp. 207-22, Springer-Verlag, 2004.
13. J.C. Cha and J.H. Cheon, *An identity-based signature from gap Diffie-Hellman groups*. PKC'03, LNCS 2567, pp. 18-30, Springer-Verlag, 2003.
14. Sherman S.M. Chow, Lucas C.K. Hui, S. Yiu, and K.P. Chow. *Secure Hierarchical Identity Based Signature and Its Application*. ICICS 2004, LNCS 3269, pp. 480-494, Springer-Verlag, 2004.
15. R. Cramer and V. Shoup. *A Practical Public Key Cryptosystem Provably Secure Against Chosen Ciphertext Attack*. Crypto'98, LNCS 1462, Springer-Verlag, pp. 13-25, 1998.
16. C. Gentry and A. Silverberg. *Hierarchical ID-Based Cryptography*. AsiaCrypt'02, LNCS 2501, pp. 548-566, Springer-Verlag, 2002.
17. J. Horwitz and B. Lynn. *Toward Hierarchical Identity-Based Encryption*. EuroCrypt'02, LNCS 2332, pp. 466-481, Springer-Verlag, 2002.
18. K. Kurosawa and Y. Desmedt. *A New Paradigm of Hybrid Encryption Scheme*. Crypto'04, LNCS 3152, pp. 426-442, Springer-Verlag, 2004.
19. Y. Mu, V. Varadharajan, and K. Nguyen, *Delegated decryption*, IMA-Crypto Coding'99, LNCS 1746, pp. 258-269, Springer, 1999.
20. D. Pointcheval and J. Stern, *Security arguments for digital signatures and blind signatures*, Journal of Cryptology, Vol.13, No.3, pp. 361-396, 2000.
21. A.Shamir, *Identity-based cryptosystems and signature schemes*, Crypto'84, LNCS 196, pp.47-53, Springer-Verlag, 1984.
22. S.Tsujii and T. Itoh. *An Id-based cryptosystem based on the discrete logarithm problem*. IEEE Journal on Selected Areas in Communication, 7(4):467-473, 1989.
23. F. Zhang, R. Safavi-Naini, W.Susilo. *An efficient signature scheme from bilinear pairings and its applications*. PKC'04, LNCS 2947, pp. 277-290, Springer-Verlag, 2004.