Practical Hierarchical Identity Based Encryption and Signature schemes Without Random Oracles

Man Ho Au[1], Joseph K. Liu[2], Tsz Hon Yuen[3], and Duncan S. Wong[4]

[1] Centre for Information Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
mhaa456@uow.edu.au
[2] Department of Computer Science
University of Bristol
Bristol, UK
liu@cs.bris.ac.uk
[3] Department of Information Engineering
The Chinese University of Hong Kong
Shatin, Hong Kong
thyuen4@ie.cuhk.edu.hk
[4] Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong
duncan@cityu.edu.hk

Abstract. In this paper, we propose a Hierarchical Identity Based Encryption scheme that is proven secure under the strongest model of [5] directly, without relying on random oracles. The size of the ciphertext is a constant while the size of public parameters is independent to the number of bit representing an identity. It is the first in the literature to achieve such a high security level and space efficiency at the same time. In addition, we also propose the first Hierarchical Identity Based Signature scheme that is proven under the strongest model without relying on random oracles and using more standard q-SDH assumption. Similar to the proposed encryption scheme, the space complexity of the signature and public parameters are as efficient as the proposed encryption scheme.

1 Introduction

Identity based (ID-based) cryptosystem [15] is a public key cryptosystem where the public key can be represented as an arbitrary string such as an email address. The concept was proposed in 1984. However, practical ID-based encryption (IBE) schemes were not found until the work of Boneh and Franklin [5] in 2001. It requires a central authority called the Public Key Generator (PKG) to use a master key to issue private keys to identities that request them. It is provable secure in the random oracle model. Several IBE schemes [7, 1, 13] are

later proposed which are secure without random oracles but under a weaker "selective-ID" model [7]. [2] and [16] proposed IBE schemes which are provably secure without random oracles under the model of [5].

Hierarchical ID-based cryptography was proposed in [12] and [14] in 2002. It is a generalization of IBE that mirros an organizational hierarchy. It allows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. In a hierarchical ID-based encryption (HIBE) scheme, a root PKG only needs to generate private keys for domain-level PKGs, who in turn generate private keys for their users in the domains of the lower level. To encrypt a message to Bob, Alice only needs to obtain the public parameters of Bob's root PKG and his identity. It is especially useful in large companies or e-government structure where there are hierarchical administrative issues needed to be taken care. Another application of HIBE is to construct forward secure encryption, as suggested by Canetti, Halevi and Katz [7]. It allows users to periodically update their private keys so that a message encrypted at period n cannot be read using a private key from period $n' > n$. HIBE provides one of the most direct and practical solutions to the key exposure problem in daily life public key infrastructure applications.

Recently, Boneh et al. [4] (preliminary papers [8, 6]) suggested some methods to construct chosen ciphertext secure (CCA) ℓ-level HIBE scheme from a chosen plaintext secure (CPA) $(\ell+1)$-level HIBE scheme. Several HIBE without random oracles are proposed in [1, 2, 16, 3] using this result. However, They are all secure in the selective-ID model only. Transforming of selective-ID model into the model of [5] introduces a loss factor of about 2^{160} in the reduction [1, 3].

On the other side, the idea of hierarchical ID-based signature (HIBS) scheme was first proposed by Gentry and Silverberg [12] in 2002 while the first provable secure HIBS scheme was proposed by Chow et al [10]. It requires the random oracle to prove its security. Yuen and Wei [17] observed that HIBS can be constructed by using hierarchical authentication tree and one-time signature, although it is inefficient. They also provided a direct construction where the size of the signature is independent to the number of levels. Although their scheme can be proven without random oracles, it is either provable secure under a even weaker model called the "gauntlet-ID model" or require a specially designed strong assumption, the $OrcYW$ assumption.

Table 1 summerizes a comparison between different HIBE schemes.

Contributions. In this paper, we propose a HIBE scheme that is secure in the model of [5] directly without using random oracles. Its security is proven using the q-ABDHE assumption [11]. The size of the ciphertext is a constant. Moreover, the size of public parameters is independent to the number of bit representing an identity, while the size of public parameters of the scheme in [9] grows with a factor of h, where h is the number of block to represent an identity of n bits, with each block using n/h bits. Our scheme is the first in the literature to achieve the highest security level and most efficient space complexity which makes it more practical to be used in daily application.

	without RO	Full / Selective-ID	size of ciphertext	size of pub param	hardness assumption
Gentry-Silverberg [12]	X	Full	$\mathcal{O}(\ell)$	$\mathcal{O}(1)$	BDH
Horwitz-Lynn [14]	X	Full	$\mathcal{O}(1)$	$\mathcal{O}(1)$	BDH
Boneh-Boyen [1]	$\surd$	Selective-ID	$\mathcal{O}(\ell)$	$\mathcal{O}(\ell)$	Dec. BDH/ q-BDHI
Boneh-Boyen [2]	$\surd$	Selective-ID	$\mathcal{O}(n \times \ell)$	$\mathcal{O}(n)$	Dec. BDH
Waters [16]	$\surd$	Selective-ID	$\mathcal{O}(1)$	$\mathcal{O}(n \times \ell)$	Dec. BDH
Boneh-Boyen-Goh [3]	$\surd$	Selective-ID	$\mathcal{O}(1)$	$\mathcal{O}(\ell)$	Dec. weak BDHI
Chatterjee-Sarkar [9]	$\surd$	Full	$\mathcal{O}(1)$	$\mathcal{O}(\ell) + \mathcal{O}(h)$	Dec. BDH
This paper	$\surd$	Full	$\mathcal{O}(1)$	$\mathcal{O}(\ell)$	Dec. q-ABDHE

Table 1. ℓ is the number of level, n is the number of bit representing an identity, h is the number of block to store the identity with each block size is n/h

In addition, we also propose the first HIBS scheme that is secure in the strongest model of [5] without using random oracles as well. Its security is proven using the more standard q-SDH assumption. Similar to the proposed HIBE scheme, the size of the signature is a constant and the size of public parameters is the same as our HIBE scheme.

Organization. The rest of the paper is organized as follow. Some mathematical preliminaries are given in Section 2. Security definition is given in Section 3. Our proposed HIBE and HIBS schemes are presented in Section 4 and 5 respectively. The paper is concluded in Section 6.

2 Preliminaries

2.1 Pairings

We briefly review bilinear pairing. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}$, and e be a bilinear map such that $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ with the following properties:

1. *Bilinearity*: For all $u, v \in \mathbb{G}$, and $a, b \in \mathbb{Z}$, $e(u^a, v^b) = e(u, v)^{ab}$.
2. *Non-degeneracy*: $e(g, g) \neq 1$.
3. *Computability*: It is efficient to compute $e(u, v)$ for all $u, v \in \mathbb{G}$.

2.2 Intractability Assumption

The security of our HIBE scheme is based on a complexity assumption called "truncated decision q-ABDHE assumption" proposed by Gentry in [11]. It is extended from the q-BDHE problem.

We define the truncated decision q-ABDHE problem is as follows: Given a vector of $q + 3$ elements:

$$\left(g', g'^{(\alpha)^{q+2}}, g, g^{\alpha}, g^{(\alpha)^2}, \ldots, g^{(\alpha)^q}\right) \in \mathbb{G}^{q+3}$$

and an element $Z \in \mathbb{G}_T$ as input, output 0 if $Z = e(g^{(\alpha)^{q+1}}, g')$ and output 1 otherwise.

An algorithm $\mathcal{B}$ has advantage ϵ in solving the truncated decision q-ABDHE if:

$$\big| \Pr[\mathcal{B}(g', g'^{(\alpha)^{q+2}}, g, g^{\alpha}, \ldots, g^{(\alpha)^{q}}, e(g^{(\alpha)^{q+1}}, g')) = 0] - \Pr[\mathcal{B}(g', g'^{(\alpha)^{q+2}}, g, g^{\alpha}, \ldots, g^{(\alpha)^{q}}, Z) = 0] \big| \geq \epsilon$$

where the probability is over the random choice of generators g, g' in $\mathbb{G}$, the random choice of α in $\mathbb{Z}_p$, the random choice of Z in $\mathbb{G}_T$, and the random bits consumed by $\mathcal{B}$. We refer the distribution on the left as $\mathcal{P}_{ABDHE}$ and the distribution on the right as $\mathcal{R}_{ABDHE}$.

Definition 1 (q-Augmented Bilinear Diffie-Hellman Exponent Assumption (q-ABDHE)). *We say that the truncated decision (t, ϵ, q)-ABDHE assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the truncated decision q-ABDHE problem in $\mathbb{G}$.*

The security of our HIBS scheme is based on q-SDH assumption, which is defined as follow:

Definition 2 (q-Strong Diffie-Hellman Assumption (q-SDH)). *The q-Strong Diffie-Hellman (q-SDH) problem in $\mathbb{G}$ is defined as follow: On input a $(q+2)$-tuple $(g_0, h_0, h_0^x, h_0^{x^2}, \cdots, h_0^{x^q}) \in \mathbb{G}^{q+2}$, output a pair (A, c) such that $A^{(x+c)} = g_0$ where $c \in \mathbb{Z}_p^*$. We say that the (t, ϵ, q)-SDH assumption holds in $\mathbb{G}$ if no t-time algorithm has advantage at least ϵ in solving the q-SDH problem in $\mathbb{G}$.*

3 Security Model

3.1 Hierarchical Identity-Based Encryption (HIBE)

An ℓ-level HIBE scheme consists of four algorithms: (Setup, Extract, Encrypt, Decrypt). The algorithms are specified as follows:

- Setup: On input a security parameter 1^{λ_s}, the TA generates $\langle msk, param \rangle$ where msk is the randomly generated master secret key and $param$ is the corresponding public parameter.
- Extract: On input an identity vector ID (where $|ID| < \ell$), it returns the corresponding private key SK_{ID} (corresponds to $param$).
- Encrypt: On input the recipient identity ID (where $|ID| \leq \ell$) and a message M, it outputs a ciphertext σ corresponding to $param$.
- Decrypt: On input the private key of the recipient ID (where $|ID| \leq \ell$), SK_{ID}, and a signature σ, it decrypts to a message M.

The security of a HIBE consists of two requirements, namely *Correctness* and *Indistinguishability*. They are defined as follows:

Correctness. We require that $M \leftarrow \mathsf{Decrypt}(SK_{ID}, \mathsf{Encrypt}(ID, M))$ for any message M, any private key SK_{ID} and its corresponding identity ID.

Indistinguishability. We define the indistinguishability against adaptive identity and adaptive chosen ciphertext attack for HIBE (IND-ID-CCA), as in the following game. We define the following oracles:

- $\mathcal{KEO}(ID)$: The Key Extraction Oracle with input ID (where $|ID| \leq \ell$) will output the secret key SK_{ID} corresponding to msk.
- $\mathcal{DO}(ID, \sigma)$: The Decryption Oracle with input recipient identity ID (where $|ID| \leq \ell$) and ciphertext σ will output a message M.

The Game is defined as follows:

1. (*Phase 1.*) $\mathcal{S}$ generates system parameter $param$ and gives $param$ to Adversary $\mathcal{A}$.
2. (*Phase 2.*) $\mathcal{A}$ queries $\mathcal{KEO}$ and $\mathcal{DO}$ in arbitrary interleaf.
3. (*Phase 3.*) $\mathcal{A}$ gives two messages M_0^*, M_1^* and identity ID^* (where $|ID^*| \leq \ell$) to $\mathcal{S}$. $\mathcal{S}$ randomly picks a bit b and returns $\sigma^* = \mathsf{Encrypt}(ID^*, M_b^*)$ to $\mathcal{A}$.
4. (*Phase 4.*) $\mathcal{A}$ queries $\mathcal{KEO}$ and $\mathcal{DO}$ in arbitrary interleaf.
5. (*Phase 5.*) $\mathcal{A}$ delivers a guess $\hat{b}$.

$\mathcal{A}$ *wins* if the following holds: $\hat{b} = b$ and ID^* or its prefix has never been queried to the $\mathcal{KEO}$ and (ID^*, σ^*) has never been queried to the $\mathcal{DO}$. $\mathcal{A}$'s *advantage* is its probability that he wins over half.

Definition 3 (Chosen Ciphertext Security). *The HIBE scheme is* (t, ϵ, q_e, q_d)-IND-ID-CCA *secure if no* t*-time attacker has advantage at least* ϵ *in the Indistinguishability Game with* q_e *queries to* $\mathcal{KEO}$ *and* q_d *queries to* $\mathcal{DO}$*.*

We said that if the above Indistinguishability Game does not allow decryption oracle query, then the HIBE scheme is only chosen plaintext (IND-ID-CPA) secure.

3.2 Hierarchical Identity-Based Signatures (HIBS)

An ℓ-level HIBS scheme consists of four algorithms: (Setup, Extract, Sign, Verify). The Setup and Extract are the same as HIBE. The other algorithms are specified as follows:

- Sign: On input the private key of the signer ID, SK_{ID} and a message M, it outputs a signature σ corresponding to $param$.
- Verify: On input the signer identity vector ID, a message M and signature σ, it outputs $\top$ if σ is a valid signature of M corresponding to $ID, param$. Otherwise, it outputs $\perp$.

The security of a HIBS consists of two requirements, namely *Correctness* and *Existential Unforgeability*. They are defined as follows:

Correctness. We require that $\top \leftarrow \mathsf{Verify}(ID,\ M,\ \mathsf{Sign}(SK_{ID}, M))$ for any message M, any private key SK_{ID} and its corresponding identity ID.

Existential Unforgeability. We define the existential unforgeability against adaptive identity and adaptive chosen message attack for HIBS (EU-ID-CMA), as in the following game. We define the following oracles:

- $\mathcal{KEO}(ID)$: same as HIBE.
- $\mathcal{SO}(ID, M)$: The Signing Oracle with input signer ID (where $|ID| \leq \ell$) and message M outputs a signature σ such that $\mathsf{Verify}(ID, M, \sigma) = \top$.

The Game is defined as follows:

1. (*Phase 1.*) Simulator $\mathcal{S}$ generates system parameter *param* and gives it to Adversary $\mathcal{A}$.
2. (*Phase 2.*) $\mathcal{A}$ queries $\mathcal{KEO}(ID)$ and $\mathcal{SO}(ID, M)$, in arbitrary interleaf.
3. (*Phase 3.*) $\mathcal{A}$ delivers a signature σ^* for signer identity ID^* (where $|ID^*| \leq \ell$) and message M^*. ID^* or its prefix have never been input to a $\mathcal{KEO}$ and σ^* should not be the output of $\mathcal{SO}(ID^*, M^*)$.

$\mathcal{A}$ *wins* if he completes the Game with $\top = \mathsf{Verify}(ID^*, M^*, \sigma^*)$. Its *advantage* is its probability of winning.

Definition 4. *The HIBS scheme is* (t, ϵ, q_e, q_s)-EU-ID-CMA *secure if no* t*-time adversary* $\mathcal{A}$ *has an advantage at least* ϵ *in the EU-ID-CMA game using* q_e *queries to* $\mathcal{KEO}$ *and* q_s *queries to* $\mathcal{SO}$*.*

4 The proposed HIBE scheme

4.1 Construction of a ℓ-HIBE scheme

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear map. We use a multiplicative notation for the operation in $\mathbb{G}$ and $\mathbb{G}_T$.

Setup: The PKG selects a random generator $g \in \mathbb{G}$ and randomly chooses $h_1, \ldots, h_\ell \in_R \mathbb{G}$ and $\alpha \in_R \mathbb{Z}_p$. It sets $g_1 = g^\alpha$ and $u_i = h_i^\alpha$ for $i \in \{2, \ldots, \ell\}$. The public parameters *param* and master secret key *msk* are given by

$$param = (g, g_1, h_1, \ldots, h_\ell, u_2, \ldots, u_\ell) \qquad msk = \alpha$$

Extract for the 1st level: To generate a private key for identity $\mathsf{ID}_1 \in \mathbb{Z}_p$, the PKG generates random $r_1 \in_R \mathbb{Z}_p$ and computes

$$a_1 = \left(h_1 g^{-r_1}\right)^{1/(\alpha - \mathsf{ID}_1)}$$

and outputs private key (a_1, r_1).

Extract for other levels: To generate a private key for identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i) \in \mathbb{Z}_p^i$, the PKG generates random $r_i \in_R \mathbb{Z}_p$ and computes

$$a_i = a_1(\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^{r_i}, \qquad b_i = (g_1 g^{-\mathsf{ID}_1})^{r_i}, \qquad c_{i,i+1} = F(i{+}1)^{r_i}, \qquad \ldots, \qquad c_{i,\ell} = F(\ell)^{r_i}$$

where $F(k) = u_k {h_k}^{-\mathsf{ID}_1}$. The private key is $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell}, r_1)$. The private key can also be generated by its parent $(\mathsf{ID}_1, \ldots, \mathsf{ID}_{i-1})$ having the secret key $a_{i-1}, b_{i-1}, c_{i-1,i}, \ldots, c_{i-1,\ell}$. He generates random $t \in_R \mathbb{Z}_p$ and computes

$$a_i = a_{i-1} \cdot c_{i-1,i}^{\mathsf{ID}_i} \cdot (\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^t, \qquad b_i = b_{i-1} \cdot (g_1 g^{-\mathsf{ID}_1})^t,$$

$$c_{i,i+1} = c_{i-1,i+1} \cdot F(i+1)^t, \qquad \ldots, \qquad c_{i,\ell} = c_{i-1,\ell} \cdot F(\ell)^t$$

This private key is a properly distributed private key for $r_i = r_{i-1} + t$.

Encrypt: To encrypt $m \in \mathbb{G}_T$ using identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i) \in \mathbb{Z}_p^i$, the sender randomly chooses $s \in_R \mathbb{Z}_p$ and constructs the ciphertext

$$\mathcal{C} = (C_1, C_2, C_3, C_4) = \Big(\; g_1^s g^{-s\mathsf{ID}_1} \; , \; e(g,g)^s \; , \; m \cdot e(g,h_1)^{-s} \; , \; (\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^s \; \Big)$$

Decrypt: To decrypt the ciphertext $\mathcal{C}$ with a private key $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell}, r_1)$, he computes the plaintext as

$$m = C_3 \cdot e(C_1, a_i) \cdot {C_2}^{r_1} / e(b_i, C_4)$$

4.2 Security

Correctness. The correctness is as follows:

$$\begin{aligned} e(C_1, a_i) \cdot {C_2}^{r_1} / e(b_i, C_4) &= e(g_1^s g^{-s\mathsf{ID}_1}, a_1(\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^{r_i}) \cdot e(g,g)^{sr_1} / e(g_1 g^{-\mathsf{ID}_1}, \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^{sr_i} \\ &= e(g_1^s g^{-s\mathsf{ID}_1}, a_1) \cdot e(g,g)^{sr_1} \\ &= e(g^{s(\alpha - \mathsf{ID}_1)}, (h_1 g^{-r_1})^{1/(\alpha - \mathsf{ID}_1)}) \cdot e(g,g)^{sr_1} \\ &= e(g, h_1)^s \end{aligned}$$

Theorem 1. *The scheme is (t', ϵ', q_e)-IND-ID-CPA secure if the truncated decision (t, ϵ, q)-ABDHE assumption holds, with*

$$q = q_e + 1, \qquad t' = t - \mathcal{O}(t_{exp} \cdot q^2), \qquad \epsilon' = \epsilon + q q_e / p$$

where t_{exp} is the time required to compute the exponent in $\mathbb{G}$.

Proof. Assume there is a (t, ϵ, q_e)-adversary $\mathcal{A}$ exists. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the truncated decisional q-ABDHE problem with probability at least ϵ' and in time at most t'.

$\mathcal{B}$ takes as input a random truncated decisional q-ABDHE challenge $(g', g'_{q+2}, g, g_1, \ldots, g_q, Z)$, where Z is either $e(g_{q+1}, g')$ or a random element of $\mathbb{G}_T$ (recall that $g_i = g^{\alpha^i}$). In order to use $\mathcal{A}$ to solve for the problem, $\mathcal{B}$ needs to simulate the oracles for $\mathcal{A}$. $\mathcal{B}$ does it in the following way.

Setup. $\mathcal{B}$ generates a random polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree q. It sets $h_1 = g^{f(\alpha)}$, computing h_1 from $(g, g_1, \ldots, g_q)$. $\mathcal{B}$ picks random $\mu_i \in_R \mathbb{Z}_p^*$ and sets $h_i = g^{\mu_i}, u_i = g_1^{\mu_i}$ for $i = 2, \ldots, \ell$. It sends the $param = (g, g_1, h_1, \ldots, h_\ell, u_2, \ldots, u_\ell)$ to $\mathcal{A}$. We can see that $param$ is uniformly random and the public key has a distribution identical to that in the real world.

Oracles Simulation. $\mathcal{B}$ simulates the extraction oracle as follow:

(*Extraction oracle.*) Upon receiving a query for a private key of a first level identity I_1, if $I_1 = \alpha$, $\mathcal{B}$ uses α to solve the truncated decisional q-ABDHE problem immediately. Otherwise, let $F_{I_1}(x)$ denote the $(q-1)$-degree polynomial $(f(x) - f(I_1))/(x - I_1)$. $\mathcal{B}$ sets the private key to be:

$$r_1 = f(I_1), \qquad a_1 = g^{F_{I_1}(\alpha)}.$$

This is a valid private key as

$$g^{F_{I_1}(\alpha)} = g^{(f(\alpha)-f(I_1))/(\alpha-I_1)} = (h_1 g^{-f(I_1)})^{1/(\alpha-I_1)}.$$

Upon receiving a query for a private key of an identity $(\bar{I}_1, \ldots, \bar{I}_i)$ for some $i \in \{2, \ldots, \ell\}$, if $\bar{I}_1 = \alpha$, $\mathcal{B}$ uses α to solve the truncated decisional q-ABDHE problem immediately. Otherwise, $\mathcal{B}$ computes $A_{-1} \in \mathbb{Z}_p$ and a polynomial $g(x) \in \mathbb{Z}_p[x]$ of degree $q-1$ such that

$$f(x) = g(x)(x - \bar{I}_1) + A_{-1}.$$

Note that $\mathcal{B}$ aborts if $A_{-1} = 0$. $\mathcal{B}$ randomly picks $\bar{r} \in \mathbb{Z}_p^*$ and computes:

$$a_i = g^{g(\alpha)+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k}, \qquad b_i = g^{\bar{r}}, \qquad r_1 = A_{-1},$$
$$c_{i,i+1} = h_{i+1}^{\bar{r}}, \qquad \ldots \qquad , \qquad c_{i,\ell} = h_\ell^{\bar{r}}$$

This is a valid secret key since we set a random $r = \bar{r}/(\alpha - \bar{I}_1)$:

$$\begin{aligned}
b_i &= g^{r(\alpha-\bar{I}_1)} = (g_1 g^{-\bar{I}_1})^r \\
a_i &= g^{g(\alpha)+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k} \\
&= g^{\frac{f(\alpha)-A_{-1}}{x-\bar{I}_1}+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k} \\
&= \big(h_1 g^{-\bar{r}_1}\big)^{1/(\alpha-\bar{I}_1)} \cdot \Big(\prod_{k=2}^{i} h_k^{(\alpha-\bar{I}_1)\bar{I}_k}\Big)^r \\
&= \big(h_1 g^{-\bar{r}_1}\big)^{1/(\alpha-\bar{I}_1)} \cdot \Big(\prod_{k=2}^{i} F(k)^{\bar{I}_k}\Big)^r \\
c_{i,j} &= h_j^{\bar{r}} = h_j^{r(\alpha-\bar{I}_1)} = F(j)^r
\end{aligned}$$

Notice that $\mathcal{B}$ records the input and output of the extraction oracle, and return the same output for duplicate inputs.

Challenge. $\mathcal{A}$ outputs two messages M_0, M_1 and an identity $(I_1^*, \ldots, I_i^*)$. If $I_1^* = \alpha$, $\mathcal{B}$ uses α to solve the truncated decisional q-ABDHE problem immediately. Otherwise, $\mathcal{B}$ randomly picks a bit $b \in \{0,1\}$ and computes a private key (a_1, r_1) for I_1^* as in the extraction oracle. Let $f_2(x) = x^{q+2}$ and let $F_2(x) = (f_2(x) - f_2(I_1^*))/(x - I_1^*)$, which is a polynomial of degree $q+1$. $\mathcal{B}$ sets:

$$C_1^* = g'^{f_2(x) - f_2(I_1^*)}, \qquad C_2^* = Z \cdot e(g', \prod_{i=0}^{q} g^{F_{2,i}\alpha^i}),$$

$$C_3^* = M_b / e(C_1^*, a_1) C_2^{*r_1}, \qquad C_4^* = C_1^{* \sum_{i=2}^{\ell} \mu_k I_k^*}$$

where $F_{2,i}$ is the coefficient of x^i in $F_2(x)$. It sends $(C_1^*, C_2^*, C_3^*, C_4^*)$ to $\mathcal{A}$ as the challenge ciphertext.

Let $s = (\log_g g') F_2(\alpha)$. If $Z = e(g_{q+1}, g')$, then $C_1^* = g^{s(\alpha - I_1^*)}$, $C_2^* = e(g,g)^s$, $M_b / C_3^* = e(C_1^*, a_1) C_2^{*r_1} = e(g, h_1)^s$, and $C_4^* = g^{s(\alpha - I_1^*) \sum_{i=2}^{\ell} \mu_k I_k^*} = (\prod_{k=2}^{i} F(k)^{I_k^*})^s$. Then $(C_1^*, C_2^*, C_3^*, C_4^*)$ is a valid, appropriately-distributed challenge to $\mathcal{A}$.

Output Calculation. Finally, $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$. If $b = b'$, $\mathcal{B}$ outputs 0 as the solution to the truncated decisional q-ABDHE problem. Otherwise, $\mathcal{B}$ outputs 1.

Probability Analysis. The probability analysis follows the proof in [11]. Let $\mathcal{I}$ be a set consisting of α, I_1^* and the (first level) identities queried by $\mathcal{A}$. Then we have $|\mathcal{I}| \leq q+1$.As $f(x)$ is a uniformly random polynomial of degree q, the values $\{f(a) : a \in \mathcal{I}\}$ are uniformly random and independent. Therefore the keys issued by $\mathcal{B}$ are appropriately distributed.

$\mathcal{B}$ aborts if $A_{-1} = 0$ in the polynomial $g(\alpha)$. As f is a randomly distributed polynomial, a random input of $\bar{I}_1$ will make $A_{-1} = 0$ (that is, $\bar{I}_1$ is a root of $f(x)$) with probability q/p. Therefore $\mathcal{B}$ does not aborts with probability qq_e/p

As our security model here does not consider anonymity, the challenge ciphertext contain no information regarding the bit b.

Time Complexity Analysis. $\mathcal{B}$'s overhead is dominated by computing $g^{F_{I_1}(\alpha)}$ in the extraction oracle queries. Each such computation requires $\mathcal{O}(q)$ exponentiations in $\mathbb{G}$. Since $\mathcal{A}$ makes at most $q-1$ queries, $t = t' + \mathcal{O}(t_{exp} \cdot q^2)$. □

4.3 Full CCA Secure HIBE

Boneh et al. [4] showed that an adaptive CCA-secure ℓ-level hierarchical identity based encryption (HIBE) scheme Π can be constructed from a CPA-secure $\ell+1$-level HIBE scheme Π' and a strong one-time signature scheme Sig. Although their theorem and proof is only in the weaker "selective-ID" model, they remark that their theorem can be easily derived for the stronger model we are using now.

Boneh et al. further suggest that a secure encapsulation scheme and a secure message authentication code (MAC) can be used together in order to replace the strong one-time signature scheme. Therefore our CCA-secure HIBE has a short ciphertext. Using our CPA-secure 2-HIBE, efficient encapsulation and MAC scheme in [4], we have an efficient CCA-secure IBE scheme. It is comparable to the construction in [11] which uses Cramer-Shoup type construction to achieve CCA security.

5 The proposed HIBS scheme

5.1 Construction of a ℓ-HIBS scheme

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be the bilinear map. We use a multiplicative notation for the operation in $\mathbb{G}$ and $\mathbb{G}_T$.

Setup: The PKG selects a random generator $g \in \mathbb{G}$ and randomly chooses $h_1, \ldots, h_\ell \in_R \mathbb{G}$ and $\alpha \in_R \mathbb{Z}_p$. It sets $g_1 = g^\alpha$ and $u_i = h_i^\alpha$ for $i \in \{2, \ldots, \ell\}$. The public parameters *param* and master secret key *msk* are given by

$$param = (g, g_1, h_1, \ldots, h_\ell, u_2, \ldots, u_\ell) \qquad msk = \alpha$$

Extract for the 1st level: To generate a private key for identity $\mathsf{ID}_1 \in \mathbb{Z}_p$, the PKG generates random $r_1 \in_R \mathbb{Z}_p$ and computes

$$a_1 = \left(h_1 g^{-r_1}\right)^{1/(\alpha - \mathsf{ID}_1)}$$

and outputs private key (a_1, r_1).

Extract for other levels: To generate a private key for identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i) \in \mathbb{Z}_p^i$, the PKG generates random $r_i \in_R \mathbb{Z}_p$ and computes

$$a_i = a_1 (\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^{r_i}, \qquad b_i = (g_1 g^{-\mathsf{ID}_1})^{r_i}, \qquad c_{i,i+1} = F(i{+}1)^{r_i}, \qquad \ldots, \qquad c_{i,\ell} = F(\ell)^{r_i}$$

where $F(k) = u_k h_k{}^{-\mathsf{ID}_1}$. The private key is $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell}, r_1)$. The private key can also be generated by its parent $(\mathsf{ID}_1, \ldots, \mathsf{ID}_{i-1})$ having the secret key $a_{i-1}, b_{i-1}, c_{i-1,i}, \ldots, c_{i-1,\ell}$. He generates random $t \in_R \mathbb{Z}_p$ and computes

$$a_i = a_{i-1} \cdot c_{i-1,i}^{\mathsf{ID}_i} \cdot (\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^t, \qquad b_i = b_{i-1} \cdot (g_1 g^{-\mathsf{ID}_1})^t,$$

$$c_{i,i+1} = c_{i-1,i+1} \cdot F(i+1)^t, \qquad \ldots, \qquad c_{i,\ell} = c_{i-1,\ell} \cdot F(\ell)^t$$

This private key is a properly distributed private key for $r_i = r_{i-1} + t$.

Sign: To sign a message $m \in \mathbb{Z}_p^*$ using identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i) \in \mathbb{Z}_p^i$ with secret key $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell+1}, r_1)$, the signer randomly chooses $s \in_R \mathbb{Z}_p$ and constructs the signature

$$\sigma_1 = a_i \cdot c_{i,i+1}^m \cdot (F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^s, \qquad \sigma_2 = b_i \cdot (g_1 g^{-\mathsf{ID}_1})^s,$$

The signature is $(\sigma_1, \sigma_2, r_1)$

Verify: To verify the signature $(\sigma_1, \sigma_2, r_1)$ for message m and identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i)$, he compares if

$$e(g_1 g^{-\mathsf{ID}_1}, \sigma_1) \stackrel{?}{=} e(g, h_1) \cdot e(g, g)^{-r_1} \cdot e(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})$$

5.2 Security

Correctness. The correctness is as follows:

$$\begin{aligned} e(g_1 g^{-\mathsf{ID}_1}, \sigma_1) &= e(g^{\alpha - \mathsf{ID}_1}, a_i \cdot c_{i,i+1}^m \cdot (F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^s) \\ &= e(g^{\alpha-\mathsf{ID}_1}, a_1) \cdot e(g^{\alpha-\mathsf{ID}_1}, (\prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^{r_i} \cdot F(i+1)^{m r_i} \cdot (F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k})^s) \\ &= e(g^{\alpha-\mathsf{ID}_1}, (h_1 g^{-r_1})^{1/(\alpha-\mathsf{ID}_1)}) \cdot e(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k}) \\ &= e(g, h_1) \cdot e(g, g)^{-r_1} \cdot e(\sigma_2, F(i+1)^m \prod_{k=2}^{i} F(k)^{\mathsf{ID}_k}) \end{aligned}$$

Theorem 2. *The scheme is $(t', \epsilon', q_e, q_s)$-EU-ID-CMA secure if the (t, ϵ, q)-SDH assumption holds, with*

$$q = q_e + 1, \qquad t' = t - \mathcal{O}(t_{exp} \cdot q(q + q_s)), \qquad \epsilon' = \epsilon + q(q + q_s)/p$$

where t_{exp} is the time required to compute the exponent in $\mathbb{G}$.

Proof. Assume there is a (t, ϵ, q_e)-adversary $\mathcal{A}$ exists. We are going to construct another PPT $\mathcal{B}$ that makes use of $\mathcal{A}$ to solve the q-SDH problem.

$\mathcal{B}$ takes as input a random q-SDH challenge $(g, g_1, \ldots, g_q)$ (recall that $g_i = g^{\alpha^i}$). In order to use $\mathcal{A}$ to solve for the problem, $\mathcal{B}$ needs to simulate the oracles for $\mathcal{A}$.

Setup. $\mathcal{B}$ generates a random polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree q. It sets $h_1 = g^{f(\alpha)}$, computing h_1 from $(g, g_1, \ldots, g_q)$. $\mathcal{B}$ picks random $\mu_i \in_R \mathbb{Z}_p^*$ and sets $h_i = g^{\mu_i}, u_i = g_1^{\mu_i}$ for $i = 2, \ldots, \ell$. It sends the $param = (g, g_1, h_1, \ldots, h_\ell, u_2, \ldots, u_\ell)$

to $\mathcal{A}$. We can see that *param* is uniformly random and the public key has a distribution identical to that in the real world.

Oracles Simulation. $\mathcal{B}$ simulates the extraction oracle as follow:

(*Extraction oracle.*) Upon receiving a query for a private key of a first level identity I_1, if $I_1 = \alpha$, $\mathcal{B}$ uses α to solve the q-SDH problem immediately. Otherwise, let $F_{I_1}(x)$ denote the $(q-1)$-degree polynomial $(f(x) - f(I_1))/(x - I_1)$. $\mathcal{B}$ sets the private key to be:

$$r_1 = f(I_1), \qquad a_1 = g^{F_{I_1}(\alpha)}.$$

This is a valid private key as

$$g^{F_{I_1}(\alpha)} = g^{(f(\alpha)-f(I_1))/(\alpha-I_1)} = (h_1 g^{-f(I_1)})^{1/(\alpha-I_1)}.$$

Upon receiving a query for a private key of an identity $(\bar{I}_1, \ldots, \bar{I}_i)$ for some $i \in \{2, \ldots, \ell\}$, if $\bar{I}_1 = \alpha$, $\mathcal{B}$ uses α to solve the q-SDH problem immediately. $\mathcal{B}$ computes $A_{-1} \in \mathbb{Z}_p$ and a polynomial $g(x) \in \mathbb{Z}_p[x]$ of degree $q-1$ such that

$$f(x) = g(x)(x - \bar{I}_1) + A_{-1}.$$

Note that $\mathcal{B}$ aborts if $A_{-1} = 0$. $\mathcal{B}$ randomly picks $\bar{r} \in \mathbb{Z}_p^*$ and computes:

$$a_i = g^{g(\alpha)+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k}, \qquad b_i = g^{\bar{r}}, \qquad r_1 = A_{-1},$$
$$c_{i,i+1} = h_{i+1}^{\bar{r}}, \qquad \ldots \qquad , \qquad c_{i,\ell} = h_{\ell}^{\bar{r}}$$

This is a valid secret key since we set a random $r = \bar{r}/(\alpha - \bar{I}_1)$:

$$\begin{aligned}
b_i &= g^{r(\alpha-\bar{I}_1)} = (g_1 g^{-\bar{I}_1})^r \\
a_i &= g^{g(\alpha)+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k} \\
&= g^{\frac{f(\alpha)-A_{-1}}{x-\bar{I}_1}+\bar{r}\sum_{k=2}^{i}\mu_k \bar{I}_k} \\
&= \left(h_1 g^{-\bar{r}_1}\right)^{1/(\alpha-\bar{I}_1)} \cdot \Big(\prod_{k=2}^{i} h_k^{(\alpha-\bar{I}_1)\bar{I}_k}\Big)^r \\
&= \left(h_1 g^{-\bar{r}_1}\right)^{1/(\alpha-\bar{I}_1)} \cdot \Big(\prod_{k=2}^{i} F(k)^{\bar{I}_k}\Big)^r \\
c_{i,j} &= h_j^{\bar{r}} = h_j^{r(\alpha-\bar{I}_1)} = F(j)^r
\end{aligned}$$

Notice that $\mathcal{B}$ records the input and output of the extraction oracle, and return the same output for duplicate inputs.

(*Signing oracle.*) Upon receiving a query for a signature for users $(I_1, \ldots, I_i)$ and message m, $\mathcal{B}$ computes as if $m = ID_{i+1}$ and runs as in the extraction oracle for identity $(I_1, \ldots, I_i, I_{i+1})$.

Output Calculation. Finally, $\mathcal{A}$ outputs a signature $(\sigma_1^*, \sigma_2^*, r^*)$ for message m^* and signer $ID^* = (I_1^*, \ldots, I_i^*)$ for some $i \in \{1, \ldots, \ell\}$.

Let $G(x)$ denote the $(q-1)$-degree polynomial $(f(x)-r^*)/(x-I_1^*)$. Then we have $G(\alpha)=\sum_{k=0}^{q-1}A_k\alpha^k+A_{-1}/(\alpha-I_1^*)$. $\mathcal{B}$ aborts if $A_{-1}=0$. Otherwise, $\mathcal{B}$ computes $A_{-1},A_0,\ldots,A_{q-1}$. Therefore, we have:

$$\begin{aligned}\sigma_1^* &= a_1(F(i+1)^{m^*}\prod_{k=0}^{i}F(k)^{I_k^*})^{r_k+s}\\ &= g^{(f(\alpha)-r^*)/(\alpha-I_1^*)}(g^{\mu_{i+1}(\alpha-I_1^*)m^*}\prod_{k=0}^{i}g^{\mu_k(\alpha-I_1^*)I_k^*})^{r_i+s}\\ \sigma_2^* &= g^{(\alpha-I_1^*)(r_i+s)}\end{aligned}$$

Therefore $\mathcal{B}$ can compute:

$$\begin{aligned}W &= \frac{\sigma_1^*}{\sigma_2^{*\mu_{i+1}m^*+\sum_{k=0}^{i}\mu_kI_k^*}}\\ &= g^{(f(\alpha)-r^*)/(\alpha-I_1^*)}\\ &= g^{\sum_{k=0}^{q-1}A_k\alpha^k+A_{-1}/(\alpha-I_1^*)}\end{aligned}$$

Finally $\mathcal{B}$ computes:

$$g^{1/(\alpha-I_1^*)}=\Big(\frac{W}{g^{\sum_{k=0}^{q-1}A_k\alpha^k}}\Big)^{1/A_{-1}}$$

Then $\mathcal{B}$ returns $(g^{1/(\alpha-I_1^*)},I_1^*)$ as the solution to the q-SDH problem.

Probability Analysis. The probability analysis follows the proof in [11]. Let $\mathcal{I}$ be a set consisting of α,I_1^* and the (first level) identities queried by $\mathcal{A}$. Then we have $|\mathcal{I}|\leq q+1$.As $f(x)$ is a uniformly random polynomial of degree q, the values $\{f(a):a\in\mathcal{I}\}$ are uniformly random and independent. Therefore the keys issued by $\mathcal{B}$ are appropriately distributed.

$\mathcal{B}$ aborts if $A_{-1}=0$ in the polynomial $G(\alpha)$. As f is a randomly distributed polynomial, a random input of r^* will make $A_{-1}=0$ with probability q/p (as there is at most q roots of the polynomial in $\mathbb{Z}_p^*$). Notice that if $\mathcal{A}$ uses r^* from extraction oracle output with input $ID=\{I_1^*,I_2,\ldots,I_i\}$ (not a subset of ID^*), $\mathcal{B}$ forces $A_{-1}\neq 0$ in the above simulation. Also, neither querying extraction oracle with just ID_j^* for $j\geq 2$ nor using its output will force $\mathcal{B}$ to abort.

Similarly $\mathcal{B}$ aborts if $A_{-1}=0$ in the polynomial $g(\alpha)$. As f is a randomly distributed polynomial, a random input of $\bar{I}_1$ will make $A_{-1}=0$ (that is, $\bar{I}_1$ is a root of $f(x)$) with probability q/p.

Therefore $\mathcal{B}$ does not aborts with probability $q(q_e+q_s+1)/p=q(q+q_s)/p$.

Time Complexity Analysis. $\mathcal{B}$'s overhead is dominated by computing $g^{F_{I_1}(\alpha)}$ in the extraction oracle queries. Each such computation requires $\mathcal{O}(q)$ exponentiations in $\mathbb{G}$. Since $\mathcal{A}$ makes at most q_s+q-1 queries, $t=t'+\mathcal{O}(t_{exp}\cdot q(q+q_s))$. □

6 Conclusion

In this paper, we proposed a HIBE scheme which achieves the strongest security model without random oracles. It relies on the q-ABDHE assumption. Its ciphertext size is constant while the size of public parameters is independent to the number of bit of identity. In addition, we also proposed a HIBS scheme with same security level and space efficiency as the HIBE scheme. It relies on the q-SDH assumption. Both are the first in the literature to achieve these advantages, regardless of the scheme in [17] which requires a non-standard assumption.

References

1. D. Boneh and X. Boyen. Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In *Proc. EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer-Verlag, 2004.
2. D. Boneh and X. Boyen. Secure Identity Based Encryption Without Random Oracles. In *Proc. CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 443–459. Springer-Verlag, 2004.
3. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In *Proc. EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 440–456. Springer-Verlag, 2005.
4. D. Boneh, R. Canatti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. http://crypto.stanford.edu/ dabo/abstracts/ccaibejour.html, 2005.
5. D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *Proc. CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001.
6. D. Boneh and J. Katz. Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption. In *Proc. CT-RSA 2005*, volume 3376 of *Lecture Notes in Computer Science*, pages 87–103. Springer-Verlag, 2005.
7. R. Canetti, S. Halevi, and J. Katz. A Forward-Secure Public-Key Encryption Scheme. In *Proc. EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 255–271. Springer-Verlag, 2003.
8. R. Canetti, S. Halevi, and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In *Proc. EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 207–222. Springer, 2004.
9. S. Chatterjee and P. Sarkar. HIBE with Short Public Parameters Secure in the Full Model Without Random Oracle. To appear in ASIACRYPT 2006, 2006. Also available at http://eprint.iacr.org/2006/279.
10. S. S. Chow, L. C. K. Lui, S. Yiu, and K. P. Chow. Secure Hierarchical Identity Based Signature and Its Application. In *ICICS 2004*, volume 3269 of *Lecture Notes in Computer Science*, pages 480–494. Springer, 2004.
11. C. Gentry. Practical identity-based encryption without random oracles. In *Proc. EUROCRYPT 2006*, volume 4404 of *Lecture Notes in Computer Science*, pages 445–464. Springer-Verlag, 2006.
12. C. Gentry and A. Silverberg. Hierarchical ID-Based Cryptography. In *Proc. ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer-Verlag, 2002.

13. S.-H. Heng and K. Kurosawa. k-Resilient Identity-Based Encryption in the Standard Model. In *Proc. CT-RSA 2004*, volume 2964 of *Lecture Notes in Computer Science*, pages 67–80. Springer-Verlag, 2004.
14. J. Horwitz and B. Lynn. Toward Hierarchical Identity-Based Encryption. In *Proc. EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 466–481. Springer-Verlag, 2002.
15. A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Proc. CRYPTO 84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.
16. B. Waters. Efficient Identity-Based Encryption Without Random Oracles. In *Proc. EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer-Verlag, 2005.
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/.