Efficient Hierarchical Identity Based Signature in the Standard Model

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

[1] Centre for Information Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong 2522, Australia
mhaa456@uow.edu.au, johnyuenhk@gmail.com

[2] Department of Computer Science
University of Bristol
Bristol, UK
liu@cs.bris.ac.uk

[3] Department of Computer Science
City University of Hong Kong
Kowloon, Hong Kong
duncan@cityu.edu.hk

Abstract. The only known constructions of Hierarchical Identity Based Signatures that are proven secure in the strongest model without random oracles are based on the approach of attaching certificate chains or hierarchical authentication tree with one-time signature. Both construction methods lead to schemes that are somewhat inefficient and leave open the problem of efficient direct construction. In this paper, we propose the first direct construction of Hierarchical Identity Based Signature scheme that is proven under the strongest model without relying on random oracles and using more standard q-SDH assumption. It is computationally efficient and the signature size is constant.

When the number of hierarchical level is set to be one, our scheme is a normal identity based signature scheme. It enjoys the shortest size in public parameters and signatures when compare with others in the literature, with the same security level.

1 Introduction

Identity based (ID-based) cryptosystem [19] 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 [6] 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 [8, 2, 14] are later proposed which are secure without random oracles but under a weaker "selective-ID" model [8]. [3] and [20] proposed IBE schemes which are provably secure without random oracles under the model of [6]. On the other side, several direct constructions of ID-based signature (IBS) can be found in literature, such as [17, 15].

Hierarchical ID-based cryptography was first proposed in [12] and [16] in 2002. It is a generalization of IBE that mirrors 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 [8]. 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. [5] (preliminary papers [9, 7]) suggested some methods to construct chosen ciphertext secure (CCA) ℓ-level HIBE scheme from a chosen plaintext secure (CPA) (ℓ+1)-level HIBE scheme. Several HIBE without random oracles are proposed in [2, 3, 20, 4] using this result. However, They are all secure in the selective-ID model only. Transforming of selective-ID model into the model of [6] introduces a loss factor of about 2^{160} in the reduction [2, 4].

In parallel to HIBE, 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. It is observed that HIBS can be constructed by using hierarchical authentication tree and one-time signature [13, 21], but it is inefficient. Bellare, Namprempre and Neven [1] suggested that IBS without random oracles can be constructed by certificate chaining. Yuen and Wei [21] remarked that some of the certificate chaining instantiations [9, 7] bear a striking resemblance to the multi-level certificate chaining structure in HIBS. User identity can be certified by his parent, by signing an IBS on the user's identity. The parent's identity can be certified again by one level higher, and the process repeats up until the root. If in each level, the certification of user identity is secure in the standard model, and finally the lowest level user signature is secure against adaptive chosen message attack in the standard model, then the entire HIBS scheme is full adaptive chosen identity and message attack in the standard model. However, this solution will increase the signature size by the level of hierarchy. Yuen and Wei also provided a direct construction where the size of the signature is independent to the number of levels in the same paper. 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.

We also noted, attributed to Gentry and Silverberg [12], that IBS schemes can be constructed from a HIBE scheme. Similarly, HIBS scheme can be obtained from HIBE scheme, where signing identities are part of a hierarchy having one level less.

Contributions. In this paper, we propose the first direct construction of HIBS scheme that is secure in the strongest model of [6] without using random oracles and its security is proven using the more standard q-SDH assumption. The size of the signature is a constant while the size of public parameters is independent to the number of bit representing an identity. It is more efficient than the generic constructions of using certificate chain or hierarchical authentication tree with one-time signature.

Our scheme is based on a hierarchical extension of Gentry's IBE scheme [11], and we convert it into a HIBS scheme. However, the conversion is not straightforward. Several techniques have to be suitably combined to obtain the required proof.

When we set the number of hierarchical level to be 1, our scheme becomes a normal IBS. When compare to the IBS scheme in [18], we have a significant improvement in space efficiency. The size of public parameter is constant in our proposed scheme while they are growing linear with the number of bit of identity representation. Our signature size is just two group elements while they need three group elements to achieve the same security level as ours.

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 HIBS scheme is presented in Section 4. The paper is concluded in Section 5.

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 HIBS scheme is based on q-SDH assumption, which is defined as follow:

Definition 1 (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

An ℓ-level HIBS scheme consists of four algorithms: (Setup, Extract, Sign, Verify). They 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 $|ID| < \ell$), its associated secret key SK_{ID}, and a string r, it returns the corresponding private key $SK_{ID.r}$ (corresponds to $param$).
- 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:

- $\mathcal{KEO}(ID)$: The Key Extraction Oracle with input ID (where $|ID| \leq \ell$) will output the secret key SK_{ID} corresponding to msk.
- $\mathcal{SO}(ID, M)$: 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 (ID^*, M^*) has never been input to a $\mathcal{SO}$.

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

Definition 2. *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 HIBS scheme

4.1 Construction of a ℓ-HIBS scheme

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ 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 $h_0, \ldots, h_{\ell+1} \in_R \mathbb{G}$, $\alpha \in_R \mathbb{Z}_p$ and $r_0 \in_R \mathbb{Z}_p^*$. It sets $g_1 = g^\alpha$. Let $\mathsf{ID}_0 \in \mathbb{Z}_p^*$ be the identity of the PKG. The public parameters *param* and master secret key *msk* are given by

$$param = (g, g_1, r_0, h_0, \ldots, h_{\ell+1}, \mathsf{ID}_0) \qquad msk = \alpha$$

Extract: To generate a private key for identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i) \in \mathbb{Z}_p^{*i}$, the PKG computes:

$$a_0 = \left(h_0 g^{-r_0}\right)^{1/(\alpha - \mathsf{ID}_0)}.$$

The PKG generates random $r_i \in_R \mathbb{Z}_p$ and computes:

$$a_i = a_0 (\prod_{k=1}^{i} h_k^{\mathsf{ID}_k})^{r_i}, \qquad b_i = (g_1 g^{-\mathsf{ID}_0})^{r_i}, \qquad c_{i,i+1} = h_{i+1}^{r_i}, \qquad \ldots, \qquad c_{i,\ell+1} = h_{\ell+1}^{r_i}$$

The private key is $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell+1})$.

The private key can also be generated by its parent $(\mathsf{ID}_1, \ldots, \mathsf{ID}_{i-1})$ having the secret key $a_{i-1}, b_{i-1}, c_{i-1,i}, \ldots, c_{i-1,\ell+1}$. He generates random $t \in_R \mathbb{Z}_p$ and computes:

$$a_i = a_{i-1} \cdot c_{i-1,i}^{\mathsf{ID}_i} \cdot (\prod_{k=1}^{i} {h_k}^{\mathsf{ID}_k})^t, \qquad b_i = b_{i-1} \cdot (g_1 g^{-\mathsf{ID}_0})^t,$$

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

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 $(a_i, b_i, c_{i,i+1}, \ldots, c_{i,\ell+1})$, the signer randomly chooses $s \in_R \mathbb{Z}_p$ and constructs the signature

$$\sigma_1 = a_i \cdot c_{i,i+1}^m \cdot (h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k})^s, \qquad \sigma_2 = b_i \cdot (g_1 g^{-\mathsf{ID}_0})^s,$$

The signature is (σ_1, σ_2)

Verify: To verify the signature (σ_1, σ_2) for message m and identity $(\mathsf{ID}_1, \ldots, \mathsf{ID}_i)$, he compares if

$$e(g_1 g^{-\mathsf{ID}_0}, \sigma_1) \stackrel{?}{=} e(g, h_0) \cdot e(g, g)^{-r_0} \cdot e(\sigma_2, h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k})$$

4.2 Security Analysis

Correctness. The correctness is as follows:

$$\begin{aligned} e(g_1 g^{-\mathsf{ID}_0}, \sigma_1) &= e(g^{\alpha-\mathsf{ID}_0}, a_i \cdot c_{i,i+1}^m \cdot (h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k})^s) \\ &= e(g^{\alpha-\mathsf{ID}_0}, a_1) \cdot e(g^{\alpha-\mathsf{ID}_0}, (\prod_{k=1}^{i} h_k^{\mathsf{ID}_k})^{r_i} \cdot {h_{i+1}}^{mr_i} \cdot (h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k})^s) \\ &= e(g^{\alpha-\mathsf{ID}_0}, (h_0 g^{-r_0})^{1/(\alpha-\mathsf{ID}_0)}) \cdot e(\sigma_2, h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k}) \\ &= e(g, h_0) \cdot e(g, g)^{-r_0} \cdot e(\sigma_2, h_{i+1}^m \prod_{k=1}^{i} h_k^{\mathsf{ID}_k}) \end{aligned}$$

Theorem 1. *The scheme is $(t', \epsilon', q_e, q_s)$-EU-ID-CMA secure if the (t, ϵ, q)-SDH assumption holds, with*

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

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

Proof. Assume there is a (t, ϵ, q_e, q_s)-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 $h_0 = g^{f(\alpha)}$, which can be computed from $(g, g_1, \ldots, g_q)$. $\mathcal{B}$ randomly picks $\mathsf{ID}_0 \in_R \mathbb{Z}_p^*$. If $\mathsf{ID}_0 = \alpha$, $\mathcal{B}$ uses α to solve the q-SDH problem immediately. Otherwise, it picks random $\mu_i \in_R \mathbb{Z}_p^*$ and sets $h_i = (g^\alpha)^{\mu_i} g^{-\mathsf{ID}_0 \mu_i} = g^{\mu_i(\alpha-\mathsf{ID}_0)}$ for $i = 1, \ldots, \ell + 1$.

$\mathcal{B}$ computes a polynomial $g(x) \in \mathbb{Z}_p[x]$ of degree $q - 1$ and $r_0 \in \mathbb{Z}_p^*$ such that

$$f(x) = g(x)(x - \mathsf{ID}_0) + r_0.$$

Note that if $r_0 = 0$, $\mathcal{B}$ restarts again by picking another ID_0.

Now we have

$$a_0 = (h_0 g^{-r_0})^{1/(\alpha - \mathsf{ID}_0)} = g^{(f(\alpha)-r_0)/(\alpha - \mathsf{ID}_0)}$$

It sends the *param* $= (g, g_1, r_0, h_0, \ldots, h_{\ell+1}, \mathsf{ID}_0)$ 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 an identity $(\bar{I}_1, \ldots, \bar{I}_i)$ for some $i \in \{1, \ldots, \ell\}$, $\mathcal{B}$ randomly picks $\bar{r} \in \mathbb{Z}_p^*$ and computes:

$$\begin{array}{ccc} a_i = g^{g(\alpha) + \bar{r}\sum_{k=1}^{i} \mu_k \bar{I}_k}, & & b_i = g^{\bar{r}}, \\ c_{i,i+1} = g^{\mu_{i+1}\bar{r}}, & \ldots & , \quad c_{i,\ell+1} = g^{\mu_{\ell+1}\bar{r}} \end{array}$$

This is a valid secret key since we set a random $r = \bar{r}/(\alpha - \mathsf{ID}_0)$:

$$\begin{aligned} b_i &= g^{r(\alpha - \mathsf{ID}_0)} = (g_1 g^{-\mathsf{ID}_0})^r \\ a_i &= g^{g(\alpha) + \bar{r}\sum_{k=1}^{i} \mu_k \bar{I}_k} \\ &= g^{\frac{f(\alpha) - r_0}{\alpha - \mathsf{ID}_0} + \bar{r}\sum_{k=1}^{i} \mu_k \bar{I}_k} \\ &= \left(h_0 g^{-r_0}\right)^{1/(\alpha - \mathsf{ID}_0)} \cdot \Big(\prod_{k=1}^{i} h_k^{\bar{I}_k}\Big)^r \\ c_{i,j} &= g^{r\mu_j(\alpha - \mathsf{ID}_0)} = h_j^r \end{aligned}$$

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, $\mathcal{B}$ runs the extraction oracle for identity $(I_1, \ldots, I_i)$ and runs Sign algorithm to generate a signature for m.

Output Calculation. Finally, $\mathcal{A}$ outputs a signature (σ_1^*, σ_2^*) for message m^* and signer $ID^* = (I_1^*, \ldots, I_i^*)$ for some $i \in \{1, \ldots, \ell\}$.

Recall $g(x)$ as the $(q-1)$-degree polynomial $(f(x) - r_0)/(x - \mathsf{ID}_0)$. Then we have

$$g(\alpha) = \sum_{k=0}^{q-1} A_k \alpha^k + \frac{A_{-1}}{\alpha - \mathsf{ID}_0}$$

$\mathcal{B}$ computes $A_{-1}, A_0, \ldots, A_{q-1}$. If $A_{-1} = 0$, $\mathcal{B}$ aborts. Otherwise, we have:

$$\sigma_1^* = a_i \cdot c_{i,i+1}^{m^*} \cdot \Big(h_{i+1}^{m^*} \cdot \prod_{k=1}^{i} h_k^{I_k^*}\Big)^s$$

$$
\begin{aligned}
&= a_0 \cdot \Big(\prod_{k=1}^{i} h_k^{I_k^*}\Big)^{r_i} \cdot (h_{i+1}^{r_i})^{m^*} \cdot \Big(h_{i+1}^{m^*} \cdot \prod_{k=1}^{i} h_k^{I_k^*}\Big)^{s} \\
&= a_0 \cdot \Big(h_{i+1}^{m^*} \cdot \prod_{k=1}^{i} h_k^{I_k^*}\Big)^{r_i+s} \\
&= g^{(f(\alpha)-r_0)/(\alpha-\mathsf{ID}_0)} \cdot \Big(g^{\mu_{i+1}(\alpha-\mathsf{ID}_0)m^*} \cdot \prod_{k=1}^{i} g^{\mu_k(\alpha-\mathsf{ID}_0)I_k^*}\Big)^{r_i+s} \\
&= g^{(f(\alpha)-r_0)/(\alpha-\mathsf{ID}_0)} \cdot \Big(g^{\mu_{i+1}m^*} \cdot \prod_{k=1}^{i} g^{\mu_k I_k^*}\Big)^{(r_i+s)(\alpha-\mathsf{ID}_0)} \\
\sigma_2^* &= g^{(\alpha-\mathsf{ID}_0)(r_i+s)}
\end{aligned}
$$

Therefore $\mathcal{B}$ can compute:

$$
\begin{aligned}
W &= \frac{\sigma_1^*}{\sigma_2^{*\mu_{i+1}m^*+\sum_{k=1}^{i}\mu_k I_k^*}} \\
&= g^{(f(\alpha)-r_0)/(\alpha-\mathsf{ID}_0)} \\
&= g^{\sum_{k=0}^{q-1} A_k\alpha^k + A_{-1}/(\alpha-\mathsf{ID}_0)}
\end{aligned}
$$

Finally $\mathcal{B}$ computes:

$$
\Big(\frac{W}{g^{\sum_{k=0}^{q-1} A_k\alpha^k}}\Big)^{1/A_{-1}} = g^{1/(\alpha-\mathsf{ID}_0)}
$$

Then $\mathcal{B}$ returns $(g^{1/(\alpha-\mathsf{ID}_0)}, \mathsf{ID}_0)$ as the solution to the q-SDH problem.

Probability Analysis. As $f(x)$ is a uniformly random polynomial of degree q and ID_0 is random from $\mathbb{Z}_p^*$, the values $g(x)$ and r_0 are uniformly random. Therefore the keys issued by $\mathcal{B}$ are appropriately distributed.

$\mathcal{B}$ aborts if $A_{-1} = 0$. As f is a randomly distributed polynomial, it happens with probability q/p (as there is at most q roots of the polynomial in $\mathbb{Z}_p^*$).

Therefore $\mathcal{B}$ aborts with probability q/p.

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

Remarks. We remark that the proof is not a straight-forward extension from Gentry's IBE scheme. In our proposed scheme, we set ID_0 as the identity of the PKG. It is different from other HIBE or HIBS schemes. In our first attempt, we do not have this "dummy" identity level while allowing the first level to be a "real" user. However, in this way r_0 is different from every user. In other words, r_0 is different from every "family" but should be the same within the same "family". Moreover, r_0 is needed in the signature verification. The only way we can publish everyone's r_0 is to put r_0 as a part of the signature.

In this preliminary attempt, we have encountered a problem in the proof. We first want to follow Gentry's proof to set $r_0 = f(I_1)$ for identity I_1. That is, all children of I_1 bear the same r_0. If the adversary asks for a signature of I_1 or his children, the simulator outputs this r_0 as part of the signature. Unfortunately, if the adversary chooses I_1 as the challenged identity and output a forged signature containing the same r_0, we cannot compute the required reduction result. The reason is as follow. Let $g'(x)$ be the $(q-1)$-degree polynomial $(f(x)-r_0)/(x-I_1)$ in the output calculation part of the proof. Then we have

$$g'(\alpha) = \sum_{k=0}^{q-1} A_k \alpha^k + \frac{A_{-1}}{\alpha - I_1}$$

If $r_0 = f(I_1)$, $(x - I_1)$ can fully divide $(f(x) - r_0)$. Then we have $A_{-1} = 0$ and cannot carry out the further reduction.

We solve this problem by introducing a dummy level, ID_0 as the identity of the PKG.

5 Conclusion

In this paper, we proposed a HIBS scheme with adaptive chosen identity and message security with a constant signature size. It is proven secure in the standard mode, using the q-SDH assumption. It is the first direct implementation in the literature to achieve these efficiency and security level, regardless of the scheme in [21] which requires a non-standard assumption. When we set the number of hierarchical level is set to be one, the resulting IBS scheme enjoys significant space efficiency improvement over the scheme in [18] with the same security level.

We believe our implementation is far more efficient than the generic approach by using certificate chains or hierarchical authentication tree with one-time signature.

References

1. M. Bellare, C. Namprempre, and G. Neven. Security Proofs for Identity-Based Identification and Signature Schemes. In *Proc. EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer-Verlag, 2004.
2. 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.
3. 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.

4. 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.
5. 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.
6. 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.
7. 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.
8. 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.
9. 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.
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. O. Goldreich. *Foundations of Cryptography*, volume 1 and 2. Cambridge Univesity Press, 2001 and 2005.
14. 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.
15. F. Hess. Efficient Identity Based Signature Schemes Based on Pairings. In *Selected Area in Cryptography, SAC2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 310–324. Springer-Verlag, 2003.
16. 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.
17. K. Paterson. Id-based signatures from pairings on elliptic curves. *IEEE Communications Letters*, 38(18):1025–1026, 2002.
18. K. Paterson and J. Schuldt. Efficient identity-based signatures secure in the standard model. In *ACISP '06*, pages 207–222. Springer-Verlag, 2006. Lecture Notes in Computer Science No. 4058.
19. 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.
20. 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.

21. 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/.