Cryptanalysis of Two Efficient HIBE Schemes in the Standard Model

Xu An Wang and Xiaoyuan Yang

Key Laboratory of Information and Network Security
Engineering College of Chinese Armed Police Force, P.R. China
wangxahq@yahoo.com.cn

Abstract. In Informatica 32 (2008), Ren and Gu proposed an anonymous hierarchical identity based encryption scheme based on the q-ABDHE problem with full security in the standard model. Later in Indocrypt'08, they proposed another secure hierarchical identity based encryption scheme based on the q-TBDHE problem with full security in the standard model. They claimed that their schemes have short parameters, high efficiency and tight reduction. However, in this paper we give attacks to show their schemes are insecure at all. Concretely, from any first level private key, the adversary can easily derive a proper "private key" which can decrypt any ciphertexts for the target identity. That is to say, one key generation query on any first level identity excluding the target's first level identity, is enough to break their schemes[1].

1 Introduction

1.1 Backgroud

IBE. In 1984, Shamir [13] first proposed the concept of identity based encryption (IBE) to simplify the certificate management. In traditional public key encryption (PKE) cryptosystem, a user's public key need to be certified by an authority CA to ensure its validity. Therefore, management of certificates is heavy for PKE. However, in an IBE cryptosystem, a user's public key can be represented as an arbitrary string, certificate management can be greatly simplified. Due to this benefit, IBE attracts great attention from the cryptography community. However, the first practical IBE scheme only realized by Boneh and Franklin in 2001 by using bilinear pairings [5]. In Eurocrypt'04, Boneh and Boyen proposed two new efficient selective identity secure (the attacker must commit the target identity before attack) IBE schemes without random oracles (BB_1 IBE and BB_2 IBE) [2]. Later Boneh and Boyen [3], Waters [14] proposed new IBE schemes with full security (the attacker can adaptively choose the target identity). In Eurocrypt'06, Gentry proposed an efficient identity based encryption with tight security reduction in the standard model but based on a stronger assumption[6].

HIBE. In practice one big organization always has hierarchical structures, perhaps with one central authority, several sub-authorities and many individual users, each belonging to a small part of the organization tree. IBE technique can not directly apply to this situation, we need a solution where each authority can delegate keys to its sub-authorities, who in turn can keep delegating keys further down the hierarchy to the users. hierarchical identity based encryption (HIBE) is such a system. In HIBE cryptosystem, messages are encrypted for identity-vectors, representing nodes in the identity hierarchy. In Eurocrypt'02, Horwitz and Lynn [9]

[1] This is an independent work with [16]. After we submitting our paper to a journal, we find that work which is available online at April 1th.

first introduced the concept of HIBE, Gentry and Silverberg [8] give the first fully functional HIBE scheme in Asiacrypt'02. But their scheme was only proved secure in the random oracle. Boneh and Boyen [2] first achieved the selective-ID secure efficient HIBE scheme in the standard model in Eurocrypt'04. But the ciphertext length is linear in the depth of the hierarchy. In Eurocrypt'05, Boneh et al. [4] proposed an efficient selective-ID secure HIBE scheme in the standard model with constant size ciphertext. In 2007, Au et al. [1] claimed to construct a HIBE scheme which is fully secure, but later they found a flaw in their security proof. In Informatica 32 (2008), Ren and Gu [11] claimed to construct a fully secure HIBE scheme with short parameters, high efficiency and tight reduction. Later in Indocrypt'08, they [12] proposed another secure hierarchical identity based encryption scheme with full security in the standard model. But in this paper, we show their schemes are insecure. In TCC'09, Gentry and Halevi [7] proposed fully secure HIBE scheme by using "identity based broadcast encryption with key randomization" (KR-IBBE). In Crypto'09, Waters [15] attained the full security under simple assumption by using "dual system encryption". Recently, Lewko and Waters [10] improved Waters's result to achieve fully secure HIBE with short ciphertexts by using "dual system encryption" in the composite order group.

1.2 Our Contribution

We cryptanalysis Ren and Gu's two efficient fully secure HIBE schemes in the standard model. Concretely, from any first level private key, the adversary can easily derive a proper "private key" which can decrypt any ciphertexts for the target identity. That is to say, one query on any first level identity is enough to break their schemes.

1.3 Organization

We organize this paper as follows. In section 2, we give the definition and security model for HIBE. In section 3, we review of Ren and Gu's first HIBE scheme and give an attack on it. In section 4, we review of Ren and Gu's second HIBE scheme and give an attack on it. In section 5, we conclude our paper.

2 Definition and Security Model

2.1 Definition

A HIBE system consists of the following five algorithms:

$\mathsf{Setup}(\lambda, l)$. Takes as input a security parameter λ and the hierarchy depth l, it outputs system parameters *params* and a master secret key *mk*. The system parameters implies also a message space $\mathcal{M}(params)$ and an identity space $\mathcal{ID}(params)$, and hierarchical identities are (ordered) tuples in $\widehat{\mathcal{ID}}(params)$.

$\mathsf{KeyGen}(params, mk, \mathsf{ID})$. Takes as input the system parameters *params* and master secret key *mk*, and an identity vector $\mathsf{ID} = [ID_1, \cdots, ID_t] \in \widehat{\mathcal{ID}}(params)$, it outputs a private key K_{ID} for ID.

$\mathsf{KeyDerive}(params, \mathsf{ID}, K_{\mathsf{ID}}, \mathsf{ID}')$. Takes as input the system parameters *params*, the identity vector ID and corresponding private key K_{ID}, and another vector ID' such that ID is a prefix of ID', it outputs a private key $K_{\mathsf{ID}'}$ for ID'.

Encrypt($params$, ID, m). Takes as input the system parameters $params$ and identity vector ID and a message m, it outputs the the ciphertext C.

Decrypt($params$, C, ID, K_{ID}). Takes as input the system parameters $params$, ciphertext C, identity vector ID and corresponding private key K_{ID}, it outputs the message m (or an error message $\perp$).

2.2 Security Model

IND-ID-CCA2 security for HIBE is defined by the following game between an adversary $\mathcal{A}$ and a challenger $\mathcal{B}$.

Setup. The challenger $\mathcal{B}$ runs the Setup algorithm and gives $\mathcal{A}$ the resulting system parameters $params$, keeping the master key to itself.

Phase 1. $\mathcal{A}$ adaptively issues queries $q_1, \cdots, q_m$ where query q_i is one of the following:

Keygeneration query (ID_i). $\mathcal{B}$ responds by running algorithm KeyGen to generate the private key corresponding to ID_i and sends d_i to $\mathcal{A}$.

Decryption query (ID_i, c_i). $\mathcal{B}$ responds by running algorithm KeyGen to generate the private key corresponding to ID_i. It then runs algorithm Decrypt to decrypt the ciphertext c_i using the private key d_i and sends the resulting plaintext to $\mathcal{A}$.

Challenge. $\mathcal{A}$ outputs an identity ID^* and two equal length plaintexts m_0, m_1 on which it wishes to be challenged. The only restriction is that $\mathcal{A}$ did not previously issue a key generation query for ID or a prefix of ID. $\mathcal{B}$ picks a random bit $w \in \{0,1\}$ and sends c to $\mathcal{A}$,where $c = \mathsf{Encrypt}(params, \mathsf{ID}, m_w)$.

Phase 2. $\mathcal{A}$ issues additional queries $q_{m+1}, \cdots, q_n$,where q_i is one of:

Keygeneration query (ID_i) where $ID_i \neq ID^*$ and ID_i is not a prefix of ID^*.

Decryption query (ID_i, c_i) where $c_i \neq c^*$ for ID^* or any prefix of ID^*.

In both cases, $\mathcal{B}$ responds as in Phase 1. These queries may be adaptive.

Guess. Finally, the adversary outputs a guess $w' \in \{0,1\}$ and wins if $w = w'$. We call an adversary $\mathcal{A}$ in the above game an IND-ID-CCA2 adversary. The advantage of $\mathcal{A}$ is defined as $\mid Pr[w = w'] - \frac{1}{2} \mid$.

Definition 1. *An HIBE system is $(t, \varepsilon, q_k, q_d)$ IND-ID-CCA2 secure if all t-time IND-ID-CCA2 adversaries making at most q_k key generation queries and at most q_d encryption queries have advantage at most ε in winning the above game.*

3 Attack on Ren and Gu's First HIBE Scheme

3.1 Review of Ren and Gu's First HIBE Scheme

In this subsection, we review of Ren and Gu's first HIBE scheme in Informatica 32 (2008)[11]

Setup(λ, l). Let p be a large prime number, G_1, G_2 are groups of order p. $e : G_1 \times G_1 \to G_2$ is a bilinear map, g is a generator of G_1, $g_1 = g^{\alpha}$, where $\alpha \in Z_p^*$. l is the maximum number of levels in the HIBE, H is a hash function from $G_1^2 \times G_1^2 \to Z_p^*$. The PKG randomly choose $r_0 \in Z_p^*$, $h_i \in G_1$, $i = 1, \cdots, l$.

$$params = (g, g_1, r_0, H, h_i(i = 0, 1, \cdots, l)), \quad mk = \alpha$$

$\mathsf{KeyGen}(params,\ mk,\ \mathsf{ID})$. To a user U with identity $\mathsf{ID}_i = [ID_1, \cdots, ID_i] \in Z_p^i$, the PKG randomly choose $r_i \in Z_p^*$, and computes

$$d_{0,i} = (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (\prod_{k=1}^{i} h_k^{ID_k})^{r_i},\ d_{1,i} = g_1^{r_i},\ d_{i+1,i} = h_{i+1}^{r_i},\ \cdots,\ d_{l,i} = h_l^{r_i}$$

so the private key of U is $d = (d_{0,i}, d_{1,i}, d_{i+1,i}, \cdots, d_{l,i})$.

$\mathsf{KeyDerive}(params,\ \mathsf{ID}_{i-1},\ K_{\mathsf{ID}_{i-1}},\ \mathsf{ID}_i)$. The private key for $\mathsf{ID}_i = [ID_1, ID_2, \cdots, ID_i]$ can also be generated by its parent $\mathsf{ID}_{i-1} = [ID_1, ID_2, \cdots, ID_{i-1}]$ having the secret key $K_{\mathsf{ID}_{i-1}} = (d_{0,i-1}, d_{1,i-1}, d_{i,i-1}, \cdots, d_{l,i-1})$. It computes:

$$d_{0,i} = d_{0,i-1} \cdot d_{i,i-1}^{ID_i} \cdot (\prod_{k=1}^{i} h_k^{ID_k})^t,\ d_{1,i} = d_{1,i-1} \cdot g_1^t,\ d_{k,i} = d_{k,i-1} \cdot h_k^t (k = i+1, \cdots, l)$$

where $r_i = r_{i-1} + t$.

$\mathsf{Encrypt}(params,\ \mathsf{ID},\ m)$. To encrypt a message $m \in G_2$ for the user with identity $\mathsf{ID}_i = [ID_1, \cdots, ID_i]$, the sender randomly choose $s \in Z_p^*$ and compute

$$c_1 = (\prod_{k=1}^{i} h_k^{ID_k})^s, \quad c_2 = e(g, g)^s, \quad c_3 = g_1^s, \quad c_4 = m \cdot e(g, h_0)^s, \quad c_5 = h_1^s h_2^{s\beta}$$

where $\beta = H(c_1, c_2, c_3, c_4)$. The ciphertext is $c = (c_1, c_2, c_3, c_4, c_5)$.

$\mathsf{Decrypt}(params,\ C,\ \mathsf{ID},\ K_{\mathsf{ID}})$. The receiver computes $\beta = H(c_1, c_2, c_3, c_4)$, and verifies whether $e(g_1, c_5) = e(c_3, h_1 h_2^{\beta})$. Then he decrypts

$$m = c_4 \cdot \frac{e(d_{1,i}, c_1) c_2^{-r_0}}{e(c_3, d_{0,i})}$$

The correctness of their scheme can be verified as follows:

$$e(g_1, c_5) = e(g_1, h_1^s h_2^{s\beta}) = e(c_3, h_1 h_2^{\beta})$$

and

$$\begin{aligned}
& c_4 \cdot \frac{e(d_{1,i}, c_1) c_2^{-r_0}}{e(c_3, d_{0,i})} \\
&= m \cdot e(g, h_0)^s \cdot \frac{e(g_1^{r_i}, \prod_{k=1}^{i} h_k^{ID_k})^s e(g, g)^{-sr_0}}{e(g_1^s, (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (\prod_{k=1}^{i} h_k^{ID_k})^{r_i})} \\
&= m \cdot e(g, h_0)^s \cdot \frac{1}{e(g^s, h_0)} \\
&= m
\end{aligned}$$

3.2 Our Attack

1. In the Setup phase, the challenger $\mathcal{B}$ runs the Setup algorithm and gives $\mathcal{A}$ the resulting system parameters $params$, keeping the master key to itself.
2. In Phase 1, $\mathcal{A}$ does not issue any query.

3. In Challenge phase, $\mathcal{A}$ outputs an identity $\mathsf{ID}^* = [ID_1^*, ID_2^*, \cdots, ID_i^*]$ and two equal length plaintexts m_0, m_1 on which it wishes to be challenged. $\mathcal{B}$ picks a random bit $w \in \{0, 1\}$ and computes $C^* = \mathsf{Encrypt}(params, \mathsf{ID}^*, m_w)$, sends C^* to $\mathcal{A}$. Here

$$C^* = (c_1 = (\prod_{k=1}^{i} h_k^{ID_k^*})^s, \quad c_2 = e(g, g)^s, \quad c_3 = g_1^s, \quad c_4 = m_w \cdot e(g, h_0)^s, \quad c_5 = h_1^s h_2^{s\beta})$$

where $\beta = H(c_1, c_2, c_3, c_4)$

4. In Phase 2, $\mathcal{A}$ does as follows:
   (a) First he queries the keygeneration oracle on a first level identity $\mathsf{ID_1} = [ID_1], ID_1 \neq ID_1^*$ to the challenger $\mathcal{B}$, and $\mathcal{B}$ returns

$$K_{\mathsf{ID_1}} = (d_{0,1} = (h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (h_1^{ID_1})^{r_i}, \quad d_{1,1} = g_1^{r_i}, \quad d_{2,1} = h_2^{r_i}, \quad \cdots, \quad d_{l,1} = h_l^{r_i})$$

   to $\mathcal{A}$.
   (b) Then he computes

$$K'_{\mathsf{ID_1}} = (d'_{0,1} = d_{0,1}^{\frac{ID_1^*}{ID_1}} = ((h_0 g^{-r_0})^{\frac{1}{\alpha}} \cdot (h_1^{ID_1}))^{r_i \cdot \frac{ID_1^*}{ID_1}} = (h_0 g^{-r_0})^{\frac{ID_1^*}{\alpha ID_1}} \cdot (h_1^{ID_1^*})^{r_i},$$
$$d'_{1,1} = g_1^{r_i},\ d'_{2,1} = h_2^{r_i}, \cdots,\ d'_{l,1} = h_l^{r_i})$$

   By using the $\mathsf{KeyDerive}$ algorithm, he derives a proper "private key"

$$K'_{\mathsf{ID}^*} = (d'_{0,i} = (h_0 g^{-r_0})^{\frac{ID_1^*}{\alpha ID_1}} (\prod_{k=1}^{i} h_k^{ID_k^*})^{r'_i},\ d'_{1,i} = g_1^{r'_i},\ d'_{i+1,i} = h_{i+1}^{r'_i}, \ \cdots,\ d'_{l,i} = h_l^{r'_i})$$

   where r'_i computed following the $\mathsf{KeyDerive}$ algorithm, which is a random element in Z_p^*.
   (c) Now he can decrypt the challenge ciphertext C^* by using K'_{ID^*} as follows

$$m = c_4 \cdot \left(\frac{e(d'_{1,i}, c_1) c_2^{\frac{-r_0 ID_1^*}{ID_1}}}{e(c_3, d'_{0,i})} \right)^{\frac{ID_1}{ID_1^*}}$$

   We can verify its correctness as follows

$$\begin{aligned} & c_4 \cdot \left(\frac{e(d'_{1,i}, c_1) c_2^{\frac{-r_0 ID^*}{ID_1}}}{e(c_3, d'_{0,i})} \right)^{\frac{ID_1}{ID^*}} \\ & = m_w \cdot e(g, h_0)^s \cdot \left(\frac{e(g_1^{r'_i}, \prod_{k=1}^{i} h_k^{ID_k^*})^s e(g, g)^{\frac{-s r_0 ID_1^*}{ID_1}}}{e(g_1^s, (h_0 g^{-r_0})^{\frac{ID_1^*}{\alpha ID_1}} \cdot (\prod_{k=1}^{i} h_k^{ID_k^*})^{r'_i})} \right)^{\frac{ID_1}{ID_1^*}} \\ & = m_w \cdot e(g, h_0)^s \cdot \frac{1}{e(g^s, h_0)} \\ & = m_w \end{aligned}$$

Obviously, $\mathcal{A}$ wins the $\mathsf{IND\text{-}ID\text{-}CCA2}$ game with probability 1.

Remark 1. This attack shows that, from any first level private key, it is easy for the adversary to derive a proper "private key" which can decrypt any ciphertexts for the target identity.

4 Attack on Ren and Gu's Second HIBE Scheme

4.1 Review of Ren and Gu's Second HIBE Scheme

In this subsection, we review of Ren and Gu's second HIBE scheme in Indocrypt 2008 [12].

$\mathsf{Setup}(\lambda,\ l)$. Let p be a large prime number, G_1, G_2 are groups of order p. $e : G_1 \times G_1 \to G_2$ is a bilinear map, g is a generator of G_1, $g_1 = g^{\alpha}$, where $\alpha \in Z_p^*$. l is the maximum number of levels in the HIBE, h and H are hash functions $G_1^2 \times G_2^3 \to Z_p^*$, $G_1^2 \times G_2^5 \to Z_p^*$. The PKG randomly choose $g_2, g_3, h_i \in G_1$, $i = 0, 1 \cdots, l$ and $f(x) = ax + b$, where $a, b \in Z_p^*$. If $g_2 = g_3^{-a}$ or $h_0 = g_3^{-b}$, choose another $f(x)$ again.

$$params = (g, g_1, g_2, g_3, f(x), h, H, h_i(i = 0, 1, \cdots, l)), \quad mk = \alpha$$

$\mathsf{KeyGen}(params,\ mk,\ \mathsf{ID})$. To a user U with identity $\mathsf{ID}_i = [ID_1, \cdots, ID_i] \in Z_p^i$, the PKG randomly choose $r_{-1,i}, r_{0,i} \in Z_p^*$, and computes

$$d_{0,i} = (h_0 g_2^{r_{-1,i}} g_3^{f(r_{-1,i})})^{\alpha} \cdot (\prod_{k=1}^{i} h_l h_k^{ID_k})^{r_{0,i}},\ d_{-1,i} = r_{-1,i},\ d_{1,i} = g^{r_{0,i}},$$
$$d_{i+1,i} = h_{i+1}^{r_{0,i}},\ \cdots,\ d_{l,i} = h_l^{r_{0,i}}$$

so the private key of U is $d = (d_{0,i}, d_{-1,i}, d_{1,i}, d_{i+1,i}, \cdots, d_{l,i})$. If $h_0 g_2^{r_{-1,i}} g_3^{f(r_{-1,i})} = 1$, randomly choose $r_{-1,i}$ again.

$\mathsf{KeyDerive}(params,\ \mathsf{ID}_{i-1},\ K_{\mathsf{ID}_{i-1}},\ \mathsf{ID}_i)$. The private key for $\mathsf{ID}_i = [ID_1, ID_2, \cdots, ID_i]$ can also be generated by its parent $\mathsf{ID}_{i-1} = [ID_1, ID_2, \cdots, ID_{i-1}]$ having the secret key $K_{\mathsf{ID}_{i-1}} = (d_{0,i-1}, d_{-1,i-1}, d_{1,i-1}, d_{i,i-1}, \cdots, d_{l,i-1})$. It computes:

$$d_{0,i} = d_{0,i-1} \cdot d_{l,i-1} \cdot d_{i,i-1}^{ID_i} \cdot (\prod_{k=1}^{i} h_l h_k^{ID_k})^t,\ d_{-1,i} = d_{-1,i-1},\ d_{1,i} = d_{1,i-1} \cdot g^t,$$
$$d_{k,i} = d_{k,i-1} \cdot h_k^t (k = i + 1, \cdots, l)$$

where $r_{0,i} = r_{0,i-1} + t$.

$\mathsf{Encrypt}(params,\ \mathsf{ID},\ m)$. To encrypt a message $m \in G_2$ for the user with identity $\mathsf{ID}_i = [ID_1, \cdots, ID_i]$, randomly choose $s \in Z_p^*$ and compute

$$c_1 = (\prod_{k=1}^{i} h_l h_k^{ID_k})^s, \quad c_2 = g^s, \quad c_3 = e(g_1, g_2)^s, \quad c_4 = e(g_1, g_3)^s,$$
$$c_5 = m \cdot e(g_1, h_0)^{s+\gamma}, \quad \beta = H(c_1, c_2, c_3, c_4, c_5, m, m \cdot e(g_1, h_0)^s)$$

where $\gamma = h(c_1, c_2, c_3, c_4, e(g_1, h_0)^s)$. The ciphertext of message m is $c = (c_1, c_2, c_3, c_4, c_5, \beta)$.

$\mathsf{Decrypt}(params,\ C,\ \mathsf{ID},\ K_{\mathsf{ID}})$. The recipient computes

$$\frac{e(c_2, d_{0,i})}{c_4^{f(d_{-1,i})} c_3^{d_{-1,i}} e(c_1, d_{1,i})} = e(g_1, h_0)^s$$

and

$$\gamma = h(c_1, c_2, c_3, c_4, e(g_1, h_0)^s), \quad \frac{c_5}{e(g_1, h_0)^{\gamma}} = R, \quad \frac{R}{e(g_1, h_0)^s} = m$$

Then he computes

$$\beta' = H(c_1, c_2, c_3, c_4, c_5, m, R)$$

and verifies whether $\beta' = \beta$, if the equation holds, the ciphertext is valid. Otherwise, the recipient returns an error message.

The correctness of their scheme can be verified as follows:

$$\begin{aligned} &\frac{e(c_2, d_{0,i})}{c_4^{f(d_{-1,i})} c_3^{d_{-1,i}} e(c_1, d_{1,i})} \\ &= \frac{e(g^s, (h_0 g_2^{r_{-1,i}} g_3^{f(r_{-1,i})})^{\alpha} (\prod_{k=1}^{i} h_l h_k^{ID_k})^{r_{0,i}})}{e(g_1, g_3)^{sf(r_{-1,i})} e(g_1, g_2)^{sr_{-1,i}} e((\prod_{k=1}^{i} h_l h_k^{ID_k})^s, g^{r_{0,i}})} \\ &= e(g_1, h_0)^s \end{aligned}$$

4.2 Our Attack

1. In the Setup phase, the challenger $\mathcal{B}$ runs the Setup algorithm and gives $\mathcal{A}$ the resulting system parameters *params*, keeping the master key to itself.
2. In Phase 1, $\mathcal{A}$ does not issue any query.
3. In Challenge phase, $\mathcal{A}$ outputs an identity $\mathsf{ID}^* = [ID_1^*, ID_2^*, \cdots, ID_i^*]$ and two equal length plaintexts m_0, m_1 on which it wishes to be challenged. $\mathcal{B}$ picks a random bit $w \in \{0, 1\}$ and computes $C^* = \mathsf{Encrypt}(params, \mathsf{ID}^*, m_w)$, sends C^* to $\mathcal{A}$. Here

$$\begin{aligned} C^* = (c_1 = (\prod_{k=1}^{i} h_l h_k^{ID_k^*})^s, \quad c_2 = g^s, \quad c_3 = e(g_1, g_2)^s, \quad c_4 = e(g_1, g_3)^s, \\ c_5 = m \cdot e(g_1, h_0)^{s+\gamma}, \quad \beta = H(c_1, c_2, c_3, c_4, c_5, m, m \cdot e(g_1, h_0)^s)) \end{aligned}$$

   where $\gamma = h(c_1, c_2, c_3, c_4, e(g_1, h_0)^s)$.
4. In Phase 2, $\mathcal{A}$ does as follows:
   (a) First he queries the keygeneration oracle on a first level identity $\mathsf{ID_1} = [ID_1], ID_1 \neq ID_1^*$ to the challenger $\mathcal{B}$, and $\mathcal{B}$ returns

$$\begin{aligned} K_{\mathsf{ID_1}} = (d_{0,1} = (h_0 g_2^{r_{-1,1}} g_3^{f(r_{-1,1})})^{\alpha} \cdot (h_l h_1^{ID_1})^{r_{0,1}},\ d_{-1,1} = r_{-1,1},\ d_{1,1} = g^{r_{0,1}}, \\ d_{2,1} = h_2^{r_{0,1}}, \ \cdots, \ d_{l,1} = h_l^{r_{0,1}}) \end{aligned}$$

   to $\mathcal{A}$.
   (b) Then he computes

$$\begin{aligned} T = \frac{d_{0,1}}{d_{l,1}} = (h_0 g_2^{r_{-1,1}} g_3^{f(r_{-1,1})})^{\alpha} \cdot (h_1^{ID_1})^{r_{0,1}} \\ K'_{\mathsf{ID_1}} = (d'_{0,1} = T^{\frac{ID_1^*}{ID_1}} \cdot d_{l,1} = ((h_0 g_2^{r_{-1,1}} g_3^{f(r_{-1,1})})^{\alpha} \cdot (h_1^{ID_1})^{r_{0,1}})^{\frac{ID_1^*}{ID_1}} \cdot h_l^{r_{0,1}} \\ = (h_0 g_2^{r_{-1,1}} g_3^{f(r_{-1,1})})^{\frac{\alpha ID_1^*}{ID_1}} \cdot (h_l h_1^{ID_1^*})^{r_{0,1}}, \\ d'_{-1,1} = r_{-1,1},\ d'_{1,1} = g^{r_{0,1}}, d'_{2,1} = h_2^{r_{0,1}}, \ \cdots, \ d'_{l,1} = h_l^{r_{0,1}}) \end{aligned}$$

By using the $\mathsf{KeyDerive}$ algorithm, he derives a proper "private key"

$$K'_{\mathsf{ID}^*} = (d'_{0,i} = (h_0 g_2^{r_{-1,i}} g_3^{f(r_{-1,i})})^{\frac{\alpha ID_1^*}{ID_1}} \cdot (\prod_{k=1}^{i} h_l h_k^{ID_k^*})^{r'_{0,i}},\ d'_{-1,i} = r_{-1,1},\ d'_{1,i} = g^{r'_{0,i}},$$
$$d'_{i+1,i} = h_{i+1}^{r'_{0,i}},\ \cdots,\ d'_{l,i} = h_l^{r'_{0,i}})$$

where $r'_{0,i}$ computed following the $\mathsf{KeyDerive}$ algorithm, which is a random element in Z_p^*.

(c) Now he can decrypt the challenge ciphertext C^* by using K'_{ID^*} as follows:
  - He first computes

$$\left(\frac{e(c_2, d'_{0,i})}{(c_4^{f(d'_{-1,i})} c_3^{d'_{-1,i}})^{\frac{ID_1^*}{ID_1}} e(c_1, d'_{1,i})}\right)^{\frac{ID_1}{ID_1^*}} = e(g_1, h_0)^s$$

  We can verify its correctness as follows

$$\begin{aligned}
&\left(\frac{e(c_2, d'_{0,i})}{(c_4^{f(d'_{-1,i})} c_3^{d'_{-1,i}})^{\frac{ID_1^*}{ID_1}} e(c_1, d'_{1,i})}\right)^{\frac{ID_1}{ID_1^*}} \\
&= \left(\frac{e(g^s, (h_0 g_2^{r_{-1,1}} g_3^{f(r_{-1,1})})^{\frac{\alpha ID_1^*}{ID_1}} (\prod_{k=1}^{i} h_l h_k^{ID_k^*})^{r'_{0,i}})}{(e(g_1, g_3)^{sf(r_{-1,1})} e(g_1, g_2)^{sr_{-1,1}})^{\frac{ID_1^*}{ID_1}} e((\prod_{k=1}^{i} h_l h_k^{ID_k^*})^s, g^{r'_{0,i}})}\right)^{\frac{ID_1}{ID_1^*}} \\
&= \left(e(g_1, h_0)^{\frac{sID_1^*}{ID_1}}\right)^{\frac{ID_1}{ID_1^*}} \\
&= e(g_1, h_0)^s
\end{aligned}$$

  - Then he computes

$$\gamma = h(c_1, c_2, c_3, c_4, e(g_1, h_0)^s), \qquad \frac{c_5}{e(g_1, h_0)^\gamma} = R, \qquad \frac{R}{e(g_1, h_0)^s} = m$$

Obviously, $\mathcal{A}$ wins the $\mathsf{IND\text{-}ID\text{-}CCA2}$ game with probability 1.

Remark 2. This attack shows that, from any first level private key, it is easy for the adversary to derive a proper "private key" which can decrypt any ciphertexts for the target identity.

5 Conclusion

In this paper, we cryptanalysis two efficient HIBE schemes which claimed to be fully secure in the standard model. Our attacks show that, one key generation query on any first level identity excluding the target's first level identity, is enough to break their schemes.

Acknowledgment

The authors would like to express their gratitude thanks for Dr. Jun Shao for many helpful comments.

References

1. Au, M. H., Liu, J. K., Yuen, T. H., Wong, D.S.: Practical hierarchical identity Based encryption and signature schemes without random oracles. http://eprint.iacr.org/2006/368, 2006.
2. Boneh, D. and Boyen, X.: Efficient selective-id secure identity based encryption without random oracles. *EUROCRYPT* (C. Cachin, J. Camenisch, Ed.), LNCS 3027, Springer-Verlag, Berlin, 2004.
3. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. *CRYPTO* (M. Franklin, Ed.), LNCS 3152, Springer-Verlag, Berlin, 2004.
4. Boneh, D., Boyen, X., Goh, E.: Hierarchical identity based encryption with constant size ciphertext. *EUROCRYPT* (R. Cramer, Ed.), LNCS 3494, Springer-Verlag, Berlin, 2005.
5. Boneh, D., Franklin., M.: Identity based encryption from the Weil pairing. *CRYPTO* (J. Kilian, Ed.), LNCS 2139, Springer-Verlag, Berlin, 2001.
6. Gentry, C.: Practical identity-based encryption without random oracles. *EUROCRYPT* (S. Vaudenay, Ed.), LNCS 4004, Springer-Verlag, Berlin, 2006.
7. Gentry, C., Halevi, S.: Hierarchical identity based encryption with polynomially many levels. *TCC* (R. Reingold, Ed.), LNCS 5444, Springer-Verlag, Berlin, 2009.
8. Gentry, C., Silverberg, A.: Hierarchical id-based cryptography. *ASIACRYPT* (Y. Zheng, Ed.), LNCS 2501, Springer-Verlag, Berlin, 2002.
9. Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. *EUROCRYPT* (L.R. Knudsen, Ed.), LNCS 2332, Springer-Verlag, Berlin, 2002.
10. Lewko, A., Waters, B.: Fully secure hibe with short ciphertexts. http://eprint.iacr.org/2009/482, 2009.
11. Ren, Y., Gu, D.: Efficient hierarchical identity based encryption scheme in the standard model. *Informatica*, **32**, 2008, 207–211.
12. Ren, Y., Gu, D.: Secure hierarchical identity based encryption scheme in the standard model. *INDOCRYPT* (D. R. Chowdhury, V. Rijmen, and A. Das, Ed.), LNCS 5365, Springer-Verlag, Berlin, 2008.
13. Shamir, A.: Identity-based cryptosystems and signature Schemes. *CRYPTO* (G. R. Blakley and D. Chaum, Ed.), LNCS 196, Springer-Verlag, Berlin, 1984.
14. Waters, B.: Efficient identity-based encryption without random oracles. *EUROCRYPT* (R. Cramer, Ed.), LNCS 3494, Springer-Verlag, Berlin, 2005.
15. Waters, B.: Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. *CRYPTO* (S. Halevi, Ed.), LNCS 5677, Springer-Verlag, Berlin, 2009.
16. Weng, J., Chen, M., Chen, K., Deng, R.: Cryptanalysis of a hierarchical identity-based encryption scheme. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, Volume E93-A No.4, 2010, 854–856.