Cryptanalysis of an Efficient HIBE Scheme in the Standard Model

Xu An Wang and Xiaoyuan Yang

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

Abstract. In Informatica 32 (2008), Ren and Gu [11] proposed an anonymous hierarchical identity based encryption scheme based on the q-ABDHE problem with full security in the standard model. They also claimed that their scheme has short parameters, high efficiency and a tight reduction. However, in this paper we give an attack to show their scheme is insecure.

1 Introduction

1.1 Backgroud

IBE. In 1984, Shamir [12] 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 unavoidable for PKE. However, in an IBE cryptosystem, a user's public key can be represented as an arbitrary string such as an email address, 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]. At 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 [13] proposed new IBE schemes with full security (the attacker can adaptively choose the target identity). At 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 an encryption system. In HIBE cryptosystem, messages are encrypted for identity-vectors, representing nodes in the identity hierarchy. At Eurocrypt'02, Horwitz and Lynn [9] first introduced the concept of HIBE, Gentry and Silverberg [8] give the first fully functional HIBE scheme at 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 at Eurocrypt'04. But the ciphertext length is linear in the depth of the hierarchy. At 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 a tight reduction. But in this paper, we show that their scheme is insecure. At TCC'09, Gentry and Halevi [7] fully secure HIBE scheme by using "identity based broadcast encryption with key randomization" (KR-IBBE). At Crypto'09, Waters [14] attained the full security under simple assumption by using "dual system encryption". Very 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 efficient fully secure HIBE in the standard model. We remark that finding fully secure HIBE in the standard model without any new technique like "dual system encryption" or any new tools like "composite order group" seems to be an uneasy work.

1.3 Organization

We organize this paper as follows. In section 2, we give the definition and security model for HIBE scheme. In section 3, we review of Ren and Gu's HIBE scheme. In section 4, we give our attack to show their scheme is insecure. In section 5, we conclude our paper.

2 Definitions

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'.
- $\mathsf{Encrypt}(params, \mathsf{ID}, m)$ Takes as input the system parameters $params$ and identity vector ID and a message m. It outputs the the ciphertext C.
- $\mathsf{Decrypt}(params, C, \mathsf{ID}, K_{\mathsf{ID}})$ 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 $\perp$).

IND-ID-CCA2 security for HIBE is defined by the following game between an adversary **A** and a challenger **B**.

- Setup. The challenger **B** runs the Setup algorithm and gives **A** the resulting system parameters $params$, keeping the master key to itself.
- Phase 1. **A** adaptively issues queries $q_1, \cdots, q_m$ where query q_i is one of the following:
  - Key generation query (ID_i). **B** responds by running algorithm KeyGen to generate the private key corresponding to the system parameters ID_i and sends d_i to **A**.

Decryption query (ID_i, c_i). **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 **A**.

Challenge. **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 **A** did not previously issue a key generation query for ID or a prefix of ID. **B** picks a random bit $w \in \{0,1\}$ and sends c to **A**,where $c = \mathsf{Encrypt}(params, \mathsf{ID}, m_w)$.

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

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

Decryption query $c_i \neq c^*$ for ID^* or any prefix of ID^*. In both cases, **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 **A** in the above game an IND-ID-CCA2 adversary. The advantage of **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 Review of Ren and Gu's HIBE Scheme

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 $r_0 \in Z_p^*$, $h_i \in G_1$, $i = 1, \cdots, l$.

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

KeyGen($params$, mk, 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 $d = (d_{0,i}, d_{1,i}, d_{i+1,i}, \cdots, d_{l,i})$.

KeyDerive($params$, ID_{i-1}, $K_{\mathsf{ID}_{i-1}}$, 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 $r_i = r_{i-1} + t$.

Encrypt($params$, 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

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

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

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

4 Our Attack

1. In the Setup phase, the challenger **B** runs the Setup algorithm and gives **A** the resulting system parameters $params$, keeping the master key to itself.
2. In Phase 1, **A** does not issue any query.
3. In Challenge phase, **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. **B** picks a random bit $w \in \{0, 1\}$ and computes $C^* = \mathsf{Encrypt}(params, \mathsf{ID}^*, m_w)$, sends C^* to **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, **A** does as follows:
   (a) First he queries the key generation oracle on a first level identity $\mathsf{ID_1} = [ID_1], ID_1 \neq ID_1^*$ to the challenger **B**, and **B** returns

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

   to **A**.
   (b) Then he computes

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

   By using the $\mathsf{KeyDerive}$ algorithm, he derives a proper "private key" K'_{ID^*}

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

   where r'_i computed following the $\mathsf{KeyDerive}$ algorithm, which is a randomly element in Z_p^*.

(c) Now 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

$$\begin{aligned} c_4 \cdot \left(\frac{e(d'_{1,i}, c_1) c_2^{\frac{-r_0 ID^*}{ID_1}}}{e(c_3, d'_{0,i})} \right)^{\frac{ID_1}{ID^*}} &= m_w \cdot e(g, h_0)^s \cdot \left(\frac{e(g_1^{r'_i}, \prod_{k=1}^{i} h_k^{ID_k^*})^s e(g, g)^{\frac{-sr_0 ID_1^*}{ID_1}}}{e(g_1^s, (h_0 g^{-r_0})^{\frac{ID_1^*}{\alpha ID_1}} \cdot (\prod_{k=1}^{i} h_k^{ID_k^*})^{r'_i})} \right)^{\frac{ID_1}{ID_1^*}} \\ &= m_w \cdot e(g, h_0)^s \cdot \frac{1}{e(g^s, h_0)} = m_w \end{aligned}$$

Obviously, **A** wins the IND-ID-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.

5 Conclusion

In this paper, we cryptanalysis an efficient HIBE scheme which claimed to be fully secure in the standard model. The authors tried to embed the proof technique in Gentry's IBE scheme [6] to the BBG HIBE scheme [4], but we show this is an uneasy task.

Acknowledgment

This work is supported by the National Natural Science Foundation of China under contract no. 60842006. The authors would like to express their gratitude thanks for Dr. Jun Shao and an anonymous reviewer for many helpful comments.

References

1. M. H. Au, J. K. Liu, T. H. Yuen, and D.S. Wong. *Practical hierarchical identity Based encryption and signature schemes without random oracles.* http://eprint.iacr.org/2006/368, 2006.
2. D. Boneh and X. Boyen. *Efficient selective-id secure identity based encryption without random oracles.* In *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238, 2004.
3. D. Boneh and X. Boyen. *Secure identity based encryption without random oracles.* In *CRYPTO 2004*, volume 3152 of *LNCS*, pages 443–459, 2004.
4. D. Boneh, X. Boyen, and E. Goh. *Hierarchical identity based encryption with constant size ciphertext.* In *EUROCRYPT 2005*, volume 3493 of *LNCS*, pages 440–456, 2005.
5. D. Boneh and M. Franklin. *Identity based encryption from the Weil pairing.* In *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229, 2001.
6. C. Gentry. *Practical identity-based encryption without random oracles.* In *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 445–464, 2006.
7. C. Gentry and S. Halevi. *Hierarchical identity based encryption with polynomially many levels.* In *TCC 2009*, volume 5444 of LNCS, pages 437–456, 2009.

8. C. Gentry and A. Silverberg. *Hierarchical id-based cryptography.* In *ASIACRYPT 2002*, volume 2501 of LNCS, pages 548–566, 2002.
9. J. Horwitz and B. Lynn. *Toward hierarchical identity-based encryption.* In *EUROCRYPT 2002*, volume 2332 of LNCS, pages 466–481, 2002.
10. A. Lewko and B. Waters. *Fully secure hibe with short ciphertexts.* http://eprint.iacr.org/2009/482, 2009.
11. Y. Ren and D. Gu. *Efficient hierarchical identity based encryption scheme in the standard.* In *Informatica* No. 32, pages 207–211, 2008.
12. A. Shamir. *Identity-based cryptosystems and signature Schemes.* In *CRYPTO 1984*, volume 196 of *LNCS*, pages 47–53, 1984.
13. B. Waters. *Efficient identity-based encryption without random oracles.* In *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127, 2005.
14. B. Waters. *Dual system encryption: realizing fully secure ibe and hibe under simple assumptions.* In *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636, 2009.