2012

Further analysis of a practical hierarchical identity-based encryption scheme

Ying SUN
Sichuan Elect Power Res Inst, China

Yong Yu
Univ Elect Sci & Technol, China

Yi Mu
University of Wollongong, ymu@uow.edu.au

Publication Details

SUN, Y., Yu, Y. & Mu, Y. (2012). Further analysis of a practical hierarchical identity-based encryption scheme. IEICE Transactions on Information and Systems, E95-D (6), 1690-1693.

Further analysis of a practical hierarchical identity-based encryption scheme

Publication Details
SUN, Y., Yu, Y. & Mu, Y. (2012). Further analysis of a practical hierarchical identity-based encryption scheme. IEICE Transactions on Information and Systems, E95-D (6), 1690-1693.

IEICE TRANSACTIONS

on Information and Systems

VOL.E95-D
NO.6
JUNE 2012

A PUBLICATION OF THE INFORMATION AND SYSTEMS SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

IEICE TRANS. INF. & SYST., VOL.E95–D, NO.6 JUNE 2012

LETTER

Further Analysis of a Practical Hierarchical Identity-Based Encryption Scheme*

Ying SUN[†a)], *Student Member*, Yong YU[††], *and* Yi MU[†††], *Nonmembers*

SUMMARY Hu, Huang and Fan proposed a fully secure hierarchical identity-based encryption (IEICE Trans. Fundamentals, Vol.E92-A, No.6, pp.1494–1499, 2009) that achieves constant size of ciphertext and tight security reduction. Unfortunately, Park and Lee (IEICE Trans. Fundamentals, Vol.E93-A, No.6, pp.1269–1272, 2010) found that the security proof of Hu et al.'s scheme is incorrect; that is, the security of Hu et al.'s scheme cannot be reduced to their claimed q-ABDHE assumption. However, it is unclear whether Hu et al.'s scheme is still secure. In this letter, we provide an attack to show that the scheme is not secure against the chosen-plaintext attack.

key words: *cryptanalysis, encryption, hierarchical identity-based cryptography*

1. Introduction

The notion of identity-based (ID-based) cryptography [1] was introduced by Shamir in 1984. The useful feature of ID-based cryptosystems is that an entity's public key can be determined from his identity such as an email address and the corresponding private key is generated by a private key generator (PKG). Using identities as public keys eliminates the need of public-key certificates used in the traditional public key infrastructure. ID-based cryptography is supposed to provide an alternative to conventional public key infrastructure from the viewpoint of efficiency and convenience. Shamir presented an ID-based signature scheme in his pioneer work [1], but ID-based encryption (IBE) was not introduced. Later, Boneh and Franklin presented a practical IBE scheme [2] from bilinear pairings in 2002. Since then, ID-based encryption has become a hot research topic.

Although a single PKG was usually used in an IBE scheme, it is undesirable for a large network because the PKG might become a bottleneck. To reduce the workload of the PKG, hierarchical ID-based encryption (HIBE) [3], a generalization of IBE that mirrors an organizational hierarchy, was proposed. In a HIBE scheme, an identity is assigned with a vector, representing nodes in the identity hierarchy. HIBE allows a root PKG to delegate private key generation and identity authentication to lower-level PKGs. A root PKG needs only to generate private keys for domain-level PKGs, which in turn generate private keys for entities in their domains in the next level.

Horwitz and Lynn introduced the notion of HIBE [3] for the first time in 2002, and then, Gentry and Silverberg gave the first fully functional HIBE scheme [4], whose security was only proved in the ideal random oracle model. Secure HIBE schemes without random oracles were proposed Boneh, Boyen and Goh [5], [6]. However, these schemes are proved secure only in the weak selective-ID model. In Eurocrypt 2005, Waters [7] described a method to extend his ID-based encryption to an efficient HIBE scheme which is secure in the standard model, but suffers a long public parameters. In Asiacrypt 2006, Chatterjee and Sarkar presented a HIBE scheme [8] that is secure without random oracles in the full model with short public parameters. However, the length of private keys and ciphertext, and the time required for encryption and decryption, grow linearly in the depth of the hierarchy in their scheme. An open problem in the construction of HIBE [8] is to avoid or control the security degradation which is exponential in the number of levels of the HIBE. Au, Liu and Yuen proposed a HIBE scheme which is secure in the full model without random oracles with a tight security reduction in their unpublished paper [9]. Unfortunately, Hu, Huang and Fan [10] showed that Au et al.'s scheme [9] is not secure and gave a new practical HIBE scheme. They claimed their scheme achieves two advantages over the previous ones. Firstly, it can be proven secure in the full model without random oracles with a tight security reduction. Secondly, the ciphertext consists of just four elements and decryption needs only two pairing computations, both of which are independent of the hierarchy depth. However, Park and Lee [11] pointed out that the security proof of Hu et al.'s scheme [10] is incorrect, that is, the security of Hu et al.'s scheme cannot be reduced to their claimed complexity assumption, q-ABDHE assumption. Now one may have the doubt that whether Hu et al.'s scheme is really secure or not. To our knowledge, no paper has addressed this issue. Therefore, in this letter, we aim to address the issue and get a negative answer. By giving a concrete attack, we indicate that Hu et al.'s scheme is not secure against chosen-plaintext attack.

Manuscript received October 31, 2011.

[†]The author is with Sichuan Electric Power Research Institute, Chengdu, 610072, China.

[††]The author is with School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China.

[†††]The author is with Centre for Computer and Information Security Research, School of Computer Science and Software Engineering, University of Wollongong, NSW 2522, Australia.

*This work was supported by the National Natural Science Foundation of China under Grants 61003232, 61073176, the National Research Foundation for the Doctoral Program of Higher Education of China under Grant 20100185120012, and the Fundamental Research Funds for the Central Universities under Grant ZYGX2010J066.

a) E-mail: ysun008@gmail.com

DOI: 10.1587/transinf.E95.D.1690

2. Review of Hu et al.'s HIBE Scheme

Let G be a cyclic additive group generated by g, whose order is a prime p, and G_T be a cyclic multiplicative group of the same order. $e : G \times G \rightarrow G_T$ denotes a bilinear pairing with the following properties [2]: (1) Bilinearity: $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in Z_p$; (2) Non-degeneracy: $e(g, g) \neq 1_{G_T}$; (3) Computability: e is efficiently computable.

In Hu et al.'s HIBE scheme [10], the message space is G_T, and the identity space is Z_p. l is a positive integer which specifies the maximum level of the HIBE. The HIBE scheme due to Hu et al. consists of the following algorithms.

Setup: The PKG randomly chooses generators $g, g_0 \in G$, and randomly picks $g_2, g_3, h_1, \cdots, h_l, u_1, \cdots, u_l \in G$, $\alpha, r, u \in Z_p$ and sets $g_1 = g^\alpha$, $F(k) = u_k h_k^{-u}$ for $1 \leq k \leq l$, $g_4 = g_1 g^{-u}$ and $g_5 = g_2 g_3^{-u}$. The public parameters are $params = \{r, g, g_0, g_4, g_5, F(1), \cdots, F(l)\}$ and the master secret key is α, u.

Extraction: Let $ID = (ID_1, ID_2, \cdots, ID_i) \in Z_p^i$, $1 \leq i \leq l$, be the identity for which the private key is required. Choose r_i randomly from Z_p^*, and define $d_{ID} = (a_0, a_1, b_{i+1}, \cdots, b_l)$ where

$$a_0 = (g_0 g^{-r})^{1/(\alpha - u)} \cdot \left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5 \right)^{r_i},$$

$$a_1 = (g_4)^{r_i},$$

$$b_{i+1} = F(i+1)^{r_i}, \cdots, b_l = F(l)^{r_i}.$$

d_{ID} is the private key for the identity ID.

Key delegation can be done as follows. Suppose $(a'_0, a'_1, b'_i, \cdots, b'_l)$ is a private key for the identity $(ID_1, ID_2, \cdots, ID_{i-1})$. To generate a private key $(a_0, a_1, b_i, \cdots, b_l)$ for the identity $(ID_1, ID_2, \cdots, ID_{i-1}, ID_i)$, first pick a random $t \in Z_p$ and compute

$$a_0 = a'_0 \cdot b_i'^{ID_i} \cdot \left(\prod_{k=1}^{i} F(k)^{ID_k} \cdot g_5 \right)^t,$$

$$a_1 = a'_1 \cdot (g_4)^t,$$

$$b_{i+1} = b'_{i+1} \cdot F(i+1)^t, \cdots, b_l = b'_l \cdot F(l)^t.$$

It is obvious that $(a_0, a_1, b_{i+1}, \cdots, b_l)$ is a valid private key of the identity $(ID_1, ID_2, \cdots, ID_i)$ for $r_i = r'_{i-1} + t$.

Encryption: Let $ID = (ID_1, ID_2, \cdots, ID_l)$ be the identity under which a message $m \in G_T$ is to be encrypted. Choose a random elements $s \in Z_p$ and the ciphertext is

$$CT = (A, B, C, D)$$

$$= \left(m \cdot e(g, g)^{-s}, e(g, g)^s, (g_4)^s, \left(\prod_{k=1}^{l} F(k)^{ID_k} \cdot g_5 \right)^s \right).$$

Decryption: Let $CT = (A, B, C, D)$ be a ciphertext on the identity $ID = (ID_1, ID_2, \cdots, ID_l)$, and $(a_0, a_1, b_{i+1}, \cdots, b_l)$ be the corresponding private key, where $1 \leq i \leq l$. The decryption steps are as follows. Check whether A and B are elements of G_T and C, D are in G. If any of the conditions does not hold, the ciphertext is invalid; Otherwise, compute the plaintext

$$A \cdot B^r \cdot \frac{e(C, a_0)}{e(a_1, D)}.$$

3. Analysis of Hu et al.'s HIBE Scheme

In this section, we analyze the security of Hu et al.'s HIBE scheme an give an attack to show that their scheme is not secure under their security model.

3.1 Security Model for HIBE

The chosen-ciphertext security for an HIBE scheme in the full model is defined by the game between an adversary $\mathcal{A}$ and a challenger C below.

Setup: The challenger C runs the setup algorithm and forwards the system parameters *param* to adversary $\mathcal{A}$, keeping the master secret key *msk* to himself.

Phase 1: Adversary $\mathcal{A}$ adaptively performs a polynomially bounded number of queries, i.e. each query may depend on the answers to the previous queries.

- **Key extraction query:** On input an identity ID of depth $i (1 \leq i \leq l)$, C generates the corresponding secret key for ID and returns it to $\mathcal{A}$.
- **Decryption query:** On input a ciphertext C as well as an identity ID of depth $i (1 \leq i \leq l)$, C decrypts the ciphertext using the private key of ID, and forwards the resulting plaintext to $\mathcal{A}$.

Challenge: Once adversary $\mathcal{A}$ decides that Phase 1 is over, he outputs a target identity ID^* of depth $i (1 \leq i \leq l)$ and two equal-length messages M_0, M_1. The only restriction is that, $\mathcal{A}$ did not previously issue a key extraction query for ID^* or a prefix of ID^*. The challenger C flips a fair coin $b \in \{0, 1\}$ and computes the challenge ciphertext $CT^* = Encrypt(params, M_b, ID^*)$ and send CT^* to $\mathcal{A}$.

Phase 2: This is identical to Phase 1 except that $\mathcal{A}$ can not perform a key extraction query for ID^* or a prefix of ID^*, and $\mathcal{A}$ can not issue a decryption query for (ID^*, CT^*).

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ of b and wins the game if $b' = b$.

We say that a HIBE scheme is (t, ϵ, q_e, q_d)-CCA secure, if no t-time adversary has advantage at least ϵ in the game with making at most q_e key extraction queries and q_d decryption queries.

If we restrict the adversary from performing the decryption queries, then a HIBE is said to be (t, ϵ, q_e)-CPA

(chosen plaintext attack) secure. Some standard techniques for converting a CPA-secure HIBE into a CCA-secure HIBE have been given.

3.2 Cryptanalysis of Hu et al.'s HIBE Scheme

Hu, Huang and Fan claimed that their HIBE scheme [10] is IND-CPA secure in the standard model. However, we here demonstrate that their scheme can not reach their security goal. Specifically, there exists an adversary $\mathcal{A}$ who can break the IND-CPA security of their scheme below:

1. In Setup stage, the adversary $\mathcal{A}$ is given the parameter *params*.
2. In Phase 1, $\mathcal{A}$ does not perform any queries.
3. In Challenge phase, $\mathcal{A}$ outputs a target identity $ID^* = (ID_1^*, ID_2^*, \cdots, ID_{i-1}^*, ID_i^*)$ and two equal-length plaintexts M_0, M_1. Then he is given the challenge ciphertext $CT^* = (A^*, B^*, C^*, D^*)$. According to the encryption algorithm in Hu et al.'s HIBE scheme, CT^* is of the following forms:

$$A^* = M_b \cdot e(g,g)^{-s^*}, B^* = e(g,g)^{s^*},$$
$$C^* = (g_4)^{s^*}, D^* = \left(\prod_{k=1}^{i} F(k)^{ID_k^*} \cdot g_5\right)^{s^*},$$

where b and s^* are chosen randomly by the challenger. $\mathcal{A}$'s task is to correctly guess the random bit b.
4. In Phase 2, $\mathcal{A}$ picks two identities

$$ID0 = (ID_1^*, ID_2^*, \cdots, ID_{i-1}^*, ID_{i0}),$$
$$ID1 = (ID_1^*, ID_2^*, \cdots, ID_{i-1}^*, ID_{i1}),$$

where ID_{i0}, ID_{i1} and ID_i^* are pairwise different and $ID_{i0} + ID_{i1} \neq 2ID_i^*$. Namely, $ID^*, ID0$ and $ID1$ locate in the same level in the hierarchy and share the same prefixes $(ID_1^*, ID_2^*, \cdots, ID_{i-1}^*)$, but they represent different identities. Then, $\mathcal{A}$ computes a new identity $ID2$ as follows:

$$ID2 = ID0 + ID1 - ID^*$$
$$= (ID_1^*, ID_2^*, \cdots, ID_{i-1}^*, ID_{i0} + ID_{i1} - ID_i^*).$$

Because ID_{i0}, ID_{i1} and ID_i^* are pairwise different, and $ID_{i0} + ID_{i1} \neq 2ID_i^*$, we can conclude that none of the identities $ID0, ID1, ID2$ is the target identity ID^*. Therefore, $\mathcal{A}$ can issue key extraction queries on $ID0, ID1$ and $ID2$ and get their secret keys respectively. According to Hu et al.'s HIBE scheme [10], we know the secret keys of the identities at depth i are of the following forms. $d_{ID0} = (a_{0,0}, a_{1,0}, b_{i+1,0}, \cdots, b_{l,0})$ where

$$a_{0,0} = (g_0 g^{-r})^{1/(\alpha-u)} \cdot \left(\prod_{k=1}^{i-1} F(k)^{ID_k^*} \cdot F(i)^{ID_{i0}} \cdot g_5\right)^{r_i},$$
$$a_{1,0} = (g_4)^{r_i},$$
$$b_{i+1,0} = F(i+1)^{r_i}, \cdots, b_{l,0} = F(l)^{r_i},$$

and $d_{ID1} = (a_{0,1}, a_{1,1}, b_{i+1,1}, \cdots, b_{l,1})$ where

$$a_{0,1} = (g_0 g^{-r})^{1/(\alpha-u)} \cdot \left(\prod_{k=1}^{i-1} F(k)^{ID_k^*} \cdot F(i)^{ID_{i1}} \cdot g_5\right)^{r_i},$$
$$a_{1,1} = (g_4)^{r_i},$$
$$b_{i+1,1} = F(i+1)^{r_i}, \cdots, b_{l,1} = F(l)^{r_i}.$$

And $d_{ID2} = (a_{0,2}, a_{1,2}, b_{i+1,2}, \cdots, b_{l,2})$ where

$$a_{0,2} = (g_0 g^{-r})^{1/(\alpha-u)} \cdot \left(\prod_{k=1}^{i-1} F(k)^{ID_k^*} \cdot F(i)^{ID_{i0}+ID_{i1}-ID_i^*} \cdot g_5\right)^{r_i},$$
$$a_{1,2} = (g_4)^{r_i},$$
$$b_{i+1,2} = F(i+1)^{r_i}, \cdots, b_{l,2} = F(l)^{r_i}.$$

Now, after obtaining d_{ID0}, d_{ID1} and d_{ID2}, $\mathcal{A}$ computes $d_{ID0} \cdot d_{ID1} / d_{ID2}$ as a valid private key for the target identity ID^*. This is true because

$$\frac{a_{0,0} \cdot a_{0,1}}{a_{0,2}} = (g_0 g^{-r})^{1/(\alpha-u)} \cdot \left(\prod_{k=1}^{i} F(k)^{ID_k^*} \cdot g_5\right)^{r_i},$$
$$\frac{a_{1,0} \cdot a_{1,1}}{a_{1,2}} = (g_4)^{r_i},$$
$$\frac{b_{i+1,0} \cdot b_{i+1,1}}{b_{i+1,2}} = F(i+1)^{r_i}, \cdots,$$
$$\frac{b_{l,0} \cdot b_{l,1}}{b_{l,2}} = F(l)^{r_i}.$$

Obviously, this is a valid private key for the target identity ID^*. Now $\mathcal{A}$ is able to decrypt the target ciphertext CT^* with this private key to obtain the message M_b, and can answer the correct b' to the Challenger with probability 1.

4. Conclusion

In this letter, we analyzed the security of Hu, Huang and Fan's HIBE [10] and gave a concrete attack to show their scheme is not secure. Since the adversary in our attack did not issue any decryption queries, it means that Hu et al.'s HIBE scheme does not achieve the IND-CPA security.

References

[1] A. Shamir, "Identity-based cryptosystem and signature scheme," Crypto'84, LNCS 196, pp.47–53, Springer-Verlag, 1984.
[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Crypto'01, LNCS 2139, pp.213–229, Springer-Verlag, 2001.
[3] J. Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," Eurocrypt'02, LNCS 2332, pp.466–481, Springer-Verlag, 2002.
[4] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," Asiacrypt'02, LNCS 2501, pp.548–566, Springer-Verlag, 2002.

[5] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," Crypto'04, LNCS 3152, pp.443–459, Springer-Verlag, 2004.
[6] D. Boneh, X. Boyen, and E.J. Goh, " Hierarchical identity based encryption with constant size ciphertext," Eurocrypt'05, LNCS 3494, pp.440–456, Springer-Verlag, 2005.
[7] B. Waters, "Efficient identity-based encryption without random oracles," Eurocrypt'05, LNCS 3494, pp.114–127, Springer-Verlag, 2005.
[8] S. Chatterjee and P. Sarkar, " HIBE with short public parameters without random oracle," Asiacrypt'06, LNCS 4284, pp.145–160, Springer-Verlag, 2006.
[9] M. Au, J. Liu, and T. Yuen, "Practical hierarchical identity based encryption and signature schemes without random oracles," http://eprint.iacr.org/2006/386, 2006.
[10] X. Hu, S. Huang, and X. Fan, "Practical hierarchical identity-based encryption scheme without random oracles," IEICE Trans. Fundamentals, vol.E92-A, no.6, pp.1494–1499, June 2009.
[11] J.H. Park and D.H. Lee, "Analysis of Hu-Huang-Fan practical hierarchical identity-based encryption scheme," IEICE Trans. Fundamentals, vol.E93-A, no.6, pp.1269–1272, June 2010.