2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)
IPCSIT vol. 53 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V53.No.2.34

On the Security of An Identity Based Broadcast Encryption Scheme

Zhang Xi[+] and Yang Ling

College of Computer science and Software Engineering, Shenzhen University

Shen Zhen, China

Abstract-Recently, Ren and Gu proposed a new identity-based broadcast encryption scheme, and claimed that their scheme is secure against chosen-ciphertext attack in the standard model. However, by giving a concrete attack, we indicate that Ren and Gu's scheme is even not secure against chosen-plaintext attack.

Keywords- identity based broadcast encryption, chosen-ciphertext attack, chosen-plaintext attack, cryptanalysis

1. Introduction

Broadcast encryption, introduced by Fiat and Noar [1], allows a centralized transmitter to send encrypted messages to a collection of users such that only a privileged subset of users can decrypt them. Broadcast encryption has found many interesting applications, such as access control in encrypted file systems, satellite TV subscription services, and DVD content protection. In the past nearly two decades, broadcast encryption has attracted great interest, and many elegant broadcast encryption schemes have been proposed, e.g., [2–7].

Identity based broadcast encryption (IBBE), is an extension of broadcast encryption to identity based scenarios, where the users' identity information such as email or IP addresses instead of digital certificates can be used as public key. As a result, identity-based cryptography significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as Public Key Infrastructure (PKI).

In 2007, Sakai and Furukawa [8] and Delerablee [9] independently proposed an IBBE scheme with constant size ciphertexts and private keys. The security of both schemes in [8, 9] are only proved in the weak selectiveID model, where the adversary must declare the set of identities she intends to attack even before seeing the public parameters of the system. In [9], Delerablee left an open question to construct an IBBE scheme secure in the adaptive-ID model, i.e., the adversary needs not to declare the target set of identities in advance. Recently, Ren and Gu [10] proposed a new IBBE scheme, and claimed that their scheme is chosen-ciphertext secure in the adaptive-ID model without random oracles. However, in this paper, we indicate that Ren-Wu scheme is even not chosen-plaintext secure.

2. Preliminaries

2.1. BilinearPairing

[+] Corresponding author.
E-mail address: zxsay@126.com

We here first review the definition for bilinear pairing, since it is used in Ren-Gu IBBE scheme. Let G_1 and G_2 be two multiplicative cyclic groups with prime order p. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ with the following properties:

- Bilinearity: $\forall g_1, g_2 \in G_1, \forall a, b \in Z_p^*$, we have $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$;
- Non-degeneracy: There exist $\forall g_1, g_2 \in G_1$ such that $e(g_1, g_2) \neq 1_{G_2}$, where 1_{G_2} denotes the identity of group G_2;
- Computability: There exists an efficient algorithm to

$$\text{Compute } e(g_1, g_2) \text{ for } \forall g_1, g_2 \in G_1$$

2.2. Definition of IBBE

In this section, we review the definition of IBBE as defined in [10]. Concretely, an IBBE scheme is a tuple of algorithms specified as below:

- Setup(n): On input the number of receivers n, this algorithm outputs a master secret key msk and a public parameter $param$.
- KeyGen(msk, ID_i): On input the master secret key msk and a user identity ID_i with $i \in \{1,2,...,n\}$, this algorithm generates a private key $skID_i$ for the user with identity IDi。
- Encrypt(S, param): On input the public parameter param and a set $S \subseteq \{1,\ldots,n\}$, this algorithm outputs a pair (Hdr, K), where Hdr is called the header and K is a message encryption key. We will often refer to Hdr as the broadcast ciphertext. Let M be a message to be broadcast to the set S and let CM be the encryption of M under the symmetric key K. The broadcast to users in S consists of (S, Hdr, CM).The pair (S, Hdr) is usually called the full header and CM is often called the broadcast body.
- Decrypt(S, IDi, skIDi, Hdr, param): On input a subset $S \subseteq \{1,...,n\}$, an identity ID_i and the corresponding private key sk_{IDi}, a header Hdr and the public parameter $param$. If $ID_i \in S$, this algorithm outputs the message key K. Note that K can be used to decrypt the broadcast body CM and obtain the message M.

2.3. Chosen-Ciphertext Security for IBBE

In this subsection, we review the chosen-ciphertext security notion (referred to as IND-ID-CCA2) for IBBE as defined by Ren and Gu in [10]. Formally, the IND-ID-CCA2 security is defined via the following game between an adversary A and a challenger B.

Setup. Challenger B runs algorithm $(param, msk) \leftarrow$ Setup(n), and gives $param$ to adversary A.

Phase 1. The adversary A adaptively issues polynomial number of queries as below:

- Key generation query (ID_i): Challenger B runs $sk_{IDi} \leftarrow$ KeyGen(msk, ID_i), and gives sk_{IDi} i to adversary A.
- Decryption query, which consists of a tuple (ID_i, S, Hdr): The challenger returns the result of Decrypt(S, ID_i,sk_{IDi}, Hdr, $param$) to A, where sk_{IDi} is the private key of ID_i.

Challenge. Once A decides that Phase 1 is over, it returns a tuple (S^*, k_0, k_1) to B, where $S^* \subseteq \{1,...,n\}$ and the identities of S^* have never been queried the private keys in Phase 1. Challenger B randomly chooses $w \in \{0, 1\}$ and runs algorithm Encrypt to obtain (Hdr^*, K_w). It then gives Hdr^* to adversary A.

Phase 2. A issues additional queries as follows:

- Key generation query (ID_i), where $ID_i \notin S^*$.
- Decryption query $Hdr \neq Hdr^*$ for any identity of S^*.

In both cases, B responds as in Phase 1. These queries may be adaptive.

Guess. Finally, adversary A outputs a guess $w' \in \{0, 1\}$ and wins if $w = w'$.

We refer to the above game as an IND-ID-CCA2 game, and adversary *A* as an IND-ID-CCA2 adversary. The advantage of *A* is defined as $|\Pr[w'=w]-\frac{1}{2}|$. An IBBE system is said to be IND-ID-CCA2 secure, if for any polynomial time IND-ID-CCA2 adversary, his advantage is negligible.

Remark: the chosen-plaintext security for IBBE systems can be similarly defined as above, except that *A* is disallowed to issue any decryption queries.

3. Review of Ren-Gu Scheme

In this section ,were view Ren-Gu IBBE scheme, which is specified by the following four algorithms:

- Setup(n): Let G_1 and G_2 be bilinear groups with prime order p, and g is a generator of G_1. $g_1 = g^{\alpha}$, where $\alpha \in_R Z_P^*$. h and H are collision resistant hash functions such that $h: Z_p^* \times \{1,...,n\} \to Z_p^*$, $H: G_1^2 \times G_2^t \to Z_p^*$, where $t \in Z_p^*$. The PKG randomly chooses $g_2, g_3, h_0, h_1, h_2 \in G_1$, and a polynomial $f(x) = ax + b$, where $a, b \in Z_p^*$. If $g_2 = g_3^{-a}$ or $h_0 = g_3^{-b}$,choose another $f(x)$ again. Finally, output the public parameter $param = (g, g_1, g_2, g_3, h_0, h_1, h_2, f(x), h, H)$ and the master secret key $msk = \alpha$
- KeyGen(msk, ID_i). To generate the private key for identity $ID_i \in Z_p^*$, this algorithm randomly chooses $r_i, r_i' \in Z_p^*$, such that $h_0 g_2^{r_i'} g_3^{f(r')} \neq 1$, and then sets

$$d_{-1} = r_i', d_0 = g^{r_i},$$
$$d_i = (h_0 g_2^{r_i'} g_3^{f(r_i')})^{\alpha} (h_2^{h(ID_i,i)} h_1^{ID_i})^{r_i},$$
$$d_j = (h_2^{h(ID_j,j)} h_1^{ID_j})^{r_i} \ (j \in \{1,...,n\}, j \neq i).$$

  The private key for ID_i is $sk_{IDi} = (d_{-1}, d0, d1, \cdots, d_n)$.
- Encrypt(S, $param$). To broadcast a message for a set $S \subseteq \{1, \cdots, n\}$ randomly choose $s \in Z_p^*, K \in G_2$, and compute

$$c_1 = \prod_{i \in s} (h_2^{h(ID_i,i)} h_1^{ID_i})^s, c_2 = g^s, c_3 = e(g_1, g_2)^s$$
$$c_4 = e(g_1, g_3)^s, c_5 = K \cdot e(g_1, h_0)^{s+\gamma}$$
$$\beta = H(c_1, c_2, c_3, c_4, c_5, K \cdot e(g_1, h_0)^s),$$

  where $\gamma = H(c_1, c_2, c_3, c_4, e(g_1, h_0)^s)$.
  The ciphertext is (Hdr, S), where $Hdr = (c_1, c_2, c_3, c_4, c_5, \beta)$. Note that K is used to encrypt the message.
- Decrypt(S, ID_i, sk_{IDi}, Hdr, $param$). Any receiver with identity ID_i in the set S can decrypt Hdr as follows: First compute

$$e(g_1, h_0)^s \leftarrow \frac{e(c_2, d_i \cdot \prod_{j \in S, j \neq i} d_j)}{c_3^{d_{-1}} \cdot c_4^{f(d_{-1})} \cdot e(c_1, d_0)}, R \leftarrow \frac{c_5}{e(g_1, h_0)^{\gamma}}$$

  where $\gamma = H(c_1, c_2, c_3, c_4, e(g_1, h_0)^s)$. Then compute $\beta' \leftarrow H(c_1, c_2, c_3, c_4, c_5, R)$ and verify whether $\beta' = \beta$ holds. If yes, compute $K \leftarrow \frac{R}{e(g_1, h_0)^s}$. Otherwise, return an error message.

4. Attack on Ren-Gu IBBE Scheme

Ren and Gu claimed that their IBBE scheme is INDID-CCA2 secure without random oracles. However, in this section, we indicate that this is not true. Concretely, there exists an IND-ID-CCA2 adversary *A* who can break the IND-ID-CCA2 security of Ren-Gu scheme with non-negligible advantage as follows:

(1). In the Setup phase, *A* obtain the public parameter *param* from the challenger.
(2) In Phase 1, *A* needs not issue any query.

(3) In the Challenge phase, according to the constrictions specified in the IND-ID-CCA2 game, adversary A returns a tuple (s^*, k_0, k_1) to β. Then the challenger randomly chooses w$\in$ {0, 1}, runs algorithm Encrypt to obtain (Hdr^*, *Kw*), and gives Hdr^* to A. Recall that *A*'s goal is to correctly guess the bit *w*.

(4)In Phase 2, *A* first chooses an identity ID_j such that $ID_j \notin s^*$, and issues a key generation query on ID_i to obtain the corresponding private key *skIDi* =($d_{-1,} d0, d1, \cdots, d_n$). Note that it is legal for *A* issue this key generation query. According to algorithm KeyGen, the private key sk_{IDi} is of the following forms:

$$d_{-1} = r_i^{'}, d_0 = g^{r_i}, d_i = (h_0 g_2^{r_i^{'}} g_3^{f(r_i^{'})})^{\alpha} (h_2^{h(ID_i,i)} h_1^{ID_i})^{r_i}, d_j = (h_2^{h(ID_j,j)} h_1^{ID_j})^{r_i} (j \in \{1,...n\}, j \neq i).$$

where $r_i, r_i^{'} \in Z_p^*$.

For any distinct $j_1, j_2 \in \{1,...,n\}$ such that $j_1 \neq i.$ and $j_2 \neq i.$ adversary *A* knows that

$$d_{j_1} = (h_2^{h(ID_{j_1}, j_1)} h_1^{ID_{j_1}})^{r_i}, \tag{1}$$

$$d_{j_2} = (h_2^{h(ID_{j_2}, j_2)} h_1^{ID_{j_2}})^{r_i}, \tag{2}$$

By $(1)^{ID_{j_2}}$ and $(2)^{ID_{j_1}}$, adversary A obtains

$$d_{i_1}^{ID_{j_2}} = (h_2^{r_i})^{h(ID_{j_1}, j_1) \cdot ID_{j_2}} \cdot (h_1^{r_i})^{ID_{J_1} \cdot ID_{j_2}}, \tag{3}$$

$$d_{j_2}^{ID_{j_1}} = (h_2^{r_i})^{h(ID_{j_2}, j_2) \cdot ID_{j_1}} \cdot (h_1^{r_i})^{ID_{j_2} \cdot ID_{j_1}}, \tag{4}$$

From $\frac{(3)}{(4)}$, adversary A obtains

$$\frac{d_{j_1}^{ID_{j_2}}}{d_{j_2}^{ID_{j_1}}} = (h_2^{r_i})^{h(ID_{j_1}, j_1) \cdot ID_{j_2} - h(ID_{j_2}, j_2) \cdot ID_{j_1}}. \tag{5}$$

Then the adversary A can obtain $h_2^{r_i}$ as below

$$h_2^{r_i} = (\frac{d_{j_1}^{ID_{j_2}}}{d_{j_2}^{ID_{j_1}}})^{\frac{1}{h(ID_{j_1}, j_1) \cdot ID_{j_2} - h(ID_{j_2}, j_2) \cdot ID_{j_1}}} \tag{6}$$

Similarly, by $\frac{(1)^{h(ID_{j_2}, j_2)}}{(2)^{h(ID_{j_1}, j_1)}}$, adversary A obtains

$$\frac{d_{j_1}^{h(ID_{j_2}, j_2)}}{d_{j_2}^{h(ID_{j_1}, j_1)}} = (h_1^{r_i})^{ID_{j_1} \cdot h(ID_{j_2}, j_2) - ID_{j_2} \cdot h(ID_{j_1}, j_1)}, \tag{7}$$

and then obtains

$$h_1^{r_i} = (\frac{d_{j_1}^{h(ID_{j_2}, j_2)}}{d_{j_2}^{h(ID_{j_1}, j_1)}})^{\frac{1}{ID_{j_1} \cdot h(ID_{j_2}, j_2) - ID_{j_2} \cdot h(ID_{j_1}, j_1)}}. \tag{8}$$

Now, using $h_1^{r_i}$ and $h_2^{r_i}$, adversary A can readily derive the private key $sk_{ID_{i^*}} = (d_{-1}^*, d_0^*, d_1^*, ..., d_n^*)$ for a target identity $ID_{i^*} \in S^*$ as below:

$$d_{-1}^* = d_{-1} = r_i^{'}, d_0^* = d_0 = g^{r_i},$$

$$d_{i^*}^* = \frac{d_i \cdot (h_2^{r_i})^{h(ID_{i^*}, i^*)} (h_1^{r_i})^{ID_{i^*}}}{(h_2^{r_i})^{h(ID_i, i)} (h_1^{r_i})^{ID_i}}$$

$$= (h_0 g_2^{r_i'} g_3^{f(r_i')})^{\alpha} (h_2^{h(ID_{i^*}, i^*)} h_1^{ID_{i^*}})^{r_i},$$

$$d_j^* = (h_2^{r_i})^{h(ID_j, j)} (h_1^{r_i})^{ID_j}$$

$$= (h_2^{h(ID_j, j)} h_1^{ID_j})^{r_i} (j \in \{1,...n\}, j \neq i^*).$$

Observe that $sk_{ID_k} = (d_{-1}^*, d_0^*, d_1^*, ..., d_n^*)$ is indeed a valid private key identity ID_{i^*} Using $sk_{ID_{i^*}}$, adversary A can certainly decrypt Hdr^*. to obtain K_w and hence determines the bit w. Thus adversary A can break the IND-ID-CCA2 security of Ren-Gu IBBE scheme with non-negligible advantage. Therefore ,Ren-Gu IBBE scheme is not IND-ID-CCA2 secure.

Remark: The above adversary A does not issue any decryption query. This means that Ren-Gu IBBE scheme is even not secure against chosen-plaintext attack.

5. Acknowledgment

The author would like to thank the anonymous referees for helpful comments. This work is supported by the National Science Foundation of China under Grant Nos. 60903178.

6. References

[1] A. Fiat and M. Naor, “Broadcast encryption,” CRYPTO, ed. D.R.Stinson,LectureNotesComputerScience,vol.773,pp.480-491. Springer,1993.

[2] Y. Dodis and N. Fazio, “Public key trace and revoke scheme secure against adaptive chosen ciphertext attack,” Public Key Cryptography,ed. Y. Desmedt, Lecture Notes in Computer Science, vol.2567, pp.100–115, Springer, 2003.

[3] D. Halevy and A. Shamir, “The lsd broadcast encryption scheme,”CRYPTO, ed. M. Yung, Lecture Notes in Computer Science, vol.2442, pp.47–60, Springer, 2002.

[4] N. Attrapadung, J. Furukawa, and H. Imai, “Forwardsecure and searchable broadcast encryption with short ciphertexts and private keys,” ASIACRYPT, ed. X. Lai and K. Chen, Lecture Notes inComputer Science, vol.4284, pp.161–177, Springer, 2006.

[5] T. Asano and K. Kamio, “A lightweight tree based one-key broadcast encryption scheme,” IEICE Transactions, vol.89A, no.7,pp.2019-2028.2006

[6] N. Attrapadung and H. Imai, “Practical broadcast encryption from graph-theoretic techniques and subset-incremental- chainstructure,”IEICETransactions,vol.90A,no.1,pp.187-203,2007.

[7] C. Delerabl´ee, P. Paillier, and D. Pointcheval, “Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys,” Pairing, ed. T. Takagi,T. Okamoto,E. Okamoto, and T.Okamoto, Lecture Notes in Computer Science, vol.4575, pp.39–59, Springer, 2007.

[8] R. Sakai and J. Furukawa, “Identity-based broadcast encryption.” Cryptology ePrint Archive, Report 2007/217, 2007.http://eprint.iacr.org/.

[9] C. Delerabl´ee, “Identity-based broadcast encryption with constant size ciphertextsandprivatekeys,”ASIACRYPT,pp.200-215, 2007.

[10] Y. Ren and D. Gu, “Fully cca2 secure identity based broadcast encryption without random oracles,” Inf. Process. Lett., vol.109,no.11, pp.527–533, 2009.