Security analysis of a fuzzy identity-based encryption scheme

Miaomiao Tian*, Liusheng Huang, and Wei Yang

School of Computer Science and Technology, University of Science and Technology of China, Hefei, 230026, China
Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou, 215123, China

Abstract. A fuzzy identity-based encryption scheme allows a ciphertext encrypted under an identity ID^* to be decrypted using a secret key corresponding to the identity ID which is close to ID^* as measured by some metric. Recently, Ren et al. proposed a new fuzzy identity-based encryption scheme and proved that it is fully chosen-ciphertext secure in the standard model. However, in this paper, we will show that their fuzzy identity-based encryption scheme is even not chosen-plaintext secure.

Keywords: Cryptanalysis; Fuzzy identity-based encryption; Chosen-ciphertext secure; Chosen-plaintext secure

1 Introduction

To simplify the certificate management in traditional public key infrastructure, Shamir [1] first introduced the concept of identity-based (ID-based) cryptography in 1984. In this scenario, a user's public key is derived from his identity, e.g., his e-mail address, and his secret key is generated by a trusted third party called private key generator (PKG) who has knowledge of a master secret key. In 2001, the first two practical identity-based encryption (IBE) schemes were presented in [2] and [3], respectively.

The notion of fuzzy identity-based encryption (fuzzy IBE) was introduced by Sahai and Waters [4] in 2005. A fuzzy IBE scheme is very similar to a standard IBE scheme except that a ciphertext encrypted under an identity ID^* can be decrypted using the secret key associated with the identity ID which is close to ID^* as judged by some metric. The error-tolerance property of fuzzy IBE enables it to possess a number of applications, such as using biometric identities in a standard IBE scheme. Up to now, several fuzzy IBE schemes have been proposed, e.g., [4–6]. Recently, Ren et al. [6] presented an efficient fuzzy IBE scheme and proved that it is fully chosen-ciphertext secure in the standard model. Unfortunately, in this paper, we will show that their scheme is even not chosen-plaintext secure.

* Corresponding author. E-mail: miaotian@mail.ustc.edu.cn (M. Tian).

The rest of this paper is organized as follows. Section 2 introduces some preliminaries required in this paper. In Section 3, we review Ren et al.'s fuzzy IBE scheme. In section 4, we present an attack on their fuzzy IBE scheme. Finally, we conclude the paper in Section 5.

2 Preliminaries

In this section, we present the definition of bilinear pairing and the syntax of fuzzy IBE.

2.1 Bilinear pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups with the same prime order p. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is called a bilinear map if it satisfies the following three properties.

1. Bilinearity: For all $a, b \in \mathbb{Z}_p$ and $u, v \in \mathbb{G}$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy: There exists $u, v \in \mathbb{G}$ such that $e(u, v) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(u, v)$ for any $u, v \in \mathbb{G}$.

2.2 Fuzzy identity-based encryption

A fuzzy IBE scheme consists of the following four algorithms [4]:

- **Setup:** On input a security parameter k, the PKG generates a master secret key MSK and the public parameters PP which contains a threshold d. The PKG publishes the public parameters PP and keeps the master key MSK secret.
- **Extract:** Given the public parameters PP, the master secret key MSK and a user's identity ID, the PKG generates a secret key sk_{ID} for the user.
- **Encrypt:** On input the public parameters PP, a message m and an identity ID^*, it returns a ciphertext C^*.
- **Decrypt:** On input the public parameters PP, a secret key sk_{ID} corresponding to an identity ID, and a ciphertext C^* encrypted under identity ID^*, it outputs the message if and only if $|ID^* \bigcap ID| \geq d$.

The standard fuzzy IBE security notion proposed in [4] is indistinguishability of ciphertext under fuzzy selective-ID chosen plaintext attack (IND-FSID-CPA). Its formal definition is based on the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- **Init.** The adversary $\mathcal{A}$ outputs a target identity $ID^* = (id_1^*, \cdots, id_n^*)$.
- **Setup.** The challenger $\mathcal{C}$ runs the **Setup** algorithm and sends the system parameters PP to the adversary $\mathcal{A}$.
- **Phase 1.** The adversary $\mathcal{A}$ adaptively delivers secret key extraction queries on many identities ID_i, where $|ID^* \bigcap ID_i| < d$ for all i. The challenger $\mathcal{C}$ runs the **Extract** algorithm to obtain a private key S_{ID_i} for each ID_i and sends the result to $\mathcal{A}$.

– **Challenge.** The adversary $\mathcal{A}$ submits two equal length messages m_0 and m_1. The challenger $\mathcal{C}$ picks a random bit $b \in \{0,1\}$ and encrypts m_b under ID^*. Then $\mathcal{C}$ sends the ciphertext to $\mathcal{A}$.
– **Phase 2.** The adversary $\mathcal{A}$ issues additional secret key extraction queries as in Phase 1.
– **Guess.** The adversary $\mathcal{A}$ outputs a guess b' of b and wins if $b' = b$.

The advantage of an adversary $\mathcal{A}$ in this game is defined as $|Pr[b' = b] - 1/2|$.
Definition 1. A fuzzy IBE scheme is IND-FSID-CPA secure if there is no polynomial-time adversary that succeeds in the above game with a non-negligible advantage.

A stronger fuzzy IBE security notion proposed by Ren et al. [6] is indistinguishability of ciphertext under fuzzy chosen-ID chosen ciphertext attack (IND-FID-CCA2), where $\mathcal{A}$ may attack any identity and may issue any decryption query.

3 Review of Ren et al.'s fuzzy IBE scheme

Let $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$ denote the Lagrange coefficient for $i \in \mathbb{Z}_p^*$ and a set S of elements in $\mathbb{Z}_p^*$. For a positive integer l, $[l]$ denotes $\{1, \ldots, l\}$. The Ren et al.'s fuzzy IBE [6] is specified as follows.

Setup: Given a security parameter k, the PKG does:

1. Choose two groups $\mathbb{G}$ and $\mathbb{G}_T$ with the same prime order p, a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ and a generator g of $\mathbb{G}$.
2. Select three cryptographic hash functions $H_1 : \mathbb{Z}_p^* \times [n] \to \mathbb{Z}_p^*$, $H_2 : [n] \to \mathbb{Z}_p^*$ and $H_3 : \mathbb{G}^n \times \mathbb{G}_T^l \to \mathbb{Z}_p^*$, where n is the length of the identities and l is some positive integer.
3. Pick $\alpha \in \mathbb{Z}_p^*$ and $h_0, h_1, h_2 \in \mathbb{G}$ uniformly at random, and select two random polynomials $f(x) = ax + b$ and $q(x)$ of degree $d-1$ over $\mathbb{Z}_p^*[x]$ respectively. If $h_0 = h_2^{-b}$ or $h_1 = h_2^{-a}$, select a new $f(x)$.
4. Set $g_1 = g^\alpha$, $g_2 = g^{q(0)}$ and $g_3 = g_1^{q(0)}$.
5. The public key is $PP = (g, g_1, g_2, g_3, d, h_0, h_1, h_2, H_1, H_2, H_3, f(x))$ and the master secret key is $MSK = (\alpha, q(x))$.

Extract: Given a user's identity $ID = (id_1, \cdots, id_n)$, the PKG does:

1. Choose a random value $r \in \mathbb{Z}_p^*$.
2. For each $i \in [n]$, compute $sk_i = \left(h_0 h_1^r h_2^{f(r)}\right)^{\frac{\alpha \cdot q(i)}{q(0) \cdot H_1(id_i, i) + H_2(i)}}$.
3. Output the private key $sk_{ID} = (r, sk_1, \cdots, sk_n)$.

Encrypt: On input the public parameters PP, a message $m \in \mathbb{G}_T$ and an identity $ID^* = (id_1^*, \cdots, id_n^*)$, the sender does:

1. Choose $s \in \mathbb{Z}_p^*$ and a $d-1$ degree polynomial $E(x) \in \mathbb{Z}_p^*[x]$ uniformly at random.

2. For each $i \in [n]$, compute $u_i = (g_2^{H_1(id_i^*, i)} \cdot g^{H_2(i)})^{s \cdot E(i)}$.
3. Set $v_i = e(g_3, h_i)^{s \cdot E(0)} (i \in [2])$, $\gamma = H_3(u_1, \cdots, u_n, v_1, v_2, e(g_3, h_0)^{s \cdot E(0)})$ and $w = m \cdot e(g_3, h_0)^{s \cdot E(0) + \gamma}$.
4. Send $C^* = (u_1, \cdots, u_n, v_1, v_2, w, \beta)$, where $\beta = H_3(u_1, \cdots, u_n, v_1, v_2, w, m \cdot e(g_3, h_0)^{s \cdot E(0)})$.

Decrypt: To decrypt the ciphertext C^* encrypted under identity ID^*, a user with identity ID satisfying $|ID^* \bigcap ID| \geq d$ does:

1. Choose an arbitrary set $S \subseteq ID^* \bigcap ID$ such that $|S| = d$.
2. Set $\Delta'_{i,S}(0) = \Delta_{i,S}(0)/(i^d + 1)$.
3. Compute $e(g_3, h_0)^{s \cdot E(0)} = \prod_{i \in S} e(u_i, sk_i)^{\Delta'_{i,S}(0)} / (v_1^r \cdot v_2^{f(r)})$ and $R = w / e(g_3, h_0)^{\gamma}$, where $\gamma = H_3(u_1, \cdots, u_n, v_1, v_2, e(g_3, h_0)^{s \cdot E(0)})$.
4. Output $m = R / e(g_3, h_0)^{s \cdot E(0)}$ if $\beta = H_3(u_1, \cdots, u_n, v_1, v_2, w, R)$. Otherwise, output $\perp$.

The **Decrypt** algorithm works since

$$
\begin{aligned}
& \frac{\prod_{i \in S} e(u_i, sk_i)^{\frac{\Delta_{i,S}(0)}{i^d+1}}}{v_1^r \cdot v_2^{f(r)}} \\
= & \frac{\prod_{i \in S} e\Big((g_2^{H_1(id_i^*, i)} \cdot g^{H_2(i)})^{s \cdot E(i)}, (h_0 h_1^r h_2^{f(r)})^{\frac{\alpha \cdot q(i)}{q(0) \cdot H_1(id_i^*, i) + H_2(i)}}\Big)^{\frac{\Delta_{i,S}(0)}{i^d+1}}}{e(g_3, h_1)^{r \cdot s \cdot E(0)} \cdot e(g_3, h_2)^{f(r) \cdot s \cdot E(0)}} \\
= & \frac{\prod_{i \in S} e\Big(g^s, h_0 h_1^r h_2^{f(r)}\Big)^{\frac{\alpha \cdot E(i) \cdot q(i) \cdot \Delta_{i,S}(0)}{i^d+1}}}{\Big(e(g_3, h_1)^r \cdot e(g_3, h_2)^{f(r)}\Big)^{s \cdot E(0)}} \\
= & \frac{e\Big(g^s, h_0 h_1^r h_2^{f(r)}\Big)^{\alpha \cdot E(0) \cdot q(0)}}{e\Big(g_3, h_1^r h_2^{f(r)}\Big)^{s \cdot E(0)}} \\
= & \frac{e\Big(g^{\alpha \cdot q(0)}, h_0 h_1^r h_2^{f(r)}\Big)^{s \cdot E(0)}}{e\Big(g_3, h_1^r h_2^{f(r)}\Big)^{s \cdot E(0)}} \\
= & \, e(g_3, h_0)^{s \cdot E(0)}
\end{aligned}
$$

Remark 1. Compared to the original scheme in [6], there is a small (but important) modification in the above scheme. Namely, we calculate $\prod_{i \in S} e(u_i, sk_i)^{\Delta'_{i,S}(0)}$ rather than $\prod_{i \in S} e(u_i, sk_i)^{\Delta_{i,S}(0)}$ in the **Decrypt** algorithm. Let $f_1(x) = E(x)q(x)$ and $f_2(x) = E(x)q(x)/(x^d + 1)$. We know that the degree of $f_1(x)$ is greater than d and thus $\sum_{i \in S} f_1(i)\Delta_{i,S}(0) = f_1(0)$ cannot be true in general. Therefore, the **Decrypt** algorithm in [6] may fail. On the other hand, $f_2(x)$ is a $d-1$ degree polynomial and $\sum_{i \in S} f_2(i)\Delta_{i,S}(0) = f_2(0) = E(0)q(0)$. As a result, the **Decrypt** algorithm in our modified scheme will work pretty well.

4 An attack on Ren et al.'s fuzzy IBE scheme

Ren et al. [6] proved that their scheme is IND-FID-CCA2 secure in the standard model. However, in this section, we show that their scheme is even not IND-FSID-CPA secure. Let the target identity is $ID^* = (id_1^*, \cdots, id_n^*)$. A polynomial time adversary $\mathcal{A}$ attacks Ren at al.'s fuzzy IBE scheme as follows:

1. In the Setup phase, the adversary $\mathcal{A}$ obtains the system parameters PP from a challenger $\mathcal{C}$.
2. In Phase 1, for each $i \in [4]$, $\mathcal{A}$ makes secret key extraction query on identity $ID_i = (id_{i,1}, \cdots, id_{i,n})$ such that $|ID_i \bigcap ID^*| < d$, where d is the threshold of the scheme. Additional restrictions on these identities are $id_1^* = id_{1,1} = id_{2,1}$ and $(id_2^*, \cdots, id_d^*) = (id_{3,2}, \cdots, id_{3,d}) = (id_{4,2}, \cdots, id_{4,d})$. Then, for each $i \in [4]$, the challenger $\mathcal{C}$ returns the secret key $sk_{ID_i} = (r_i, sk_{i,1}, \cdots, sk_{i,n})$ associated with ID_i to $\mathcal{A}$.
3. In Challenge phase, $\mathcal{A}$ submits two equal length messages m_0 and m_1. The challenger $\mathcal{C}$ picks a random bit $b \in \{0, 1\}$ and runs algorithm $\mathbf{Encrypt}(m_b, ID^*)$ to obtain a ciphertext C_b^*. Then $\mathcal{C}$ sends C_b^* to $\mathcal{A}$.
4. In Phase 2, $\mathcal{A}$ does not issue any query.
5. $\mathcal{A}$ obtains a proper "secret key" sk_{ID^*} of ID^* by performing the following steps:
   (a) Compute $c_1 = (\frac{sk_{1,1}}{sk_{2,1}})^{(r_1 - r_2)^{-1}}$ and $c_i = (\frac{sk_{3,i}}{sk_{4,i}})^{(r_3 - r_4)^{-1}}$ for $2 \leq i \leq d$.
   (b) Set $t_1 = sk_{1,1}/{c_1}^{r_1}$ and $t_i = sk_{3,i}/{c_i}^{r_3}$ for $2 \leq i \leq d$.
   (c) Pick a random value $r \in \mathbb{Z}_p^*$ and compute $sk_i^* = {c_i}^r \cdot t_i$ for $i \in [d]$.
   (d) Let $sk_{ID^*} = (r, sk_1^*, \cdots, sk_d^*)$.

Remark 2. In fact, $\mathcal{A}$ does be able to obtain a full private key of ID^* using the above method, however, we will show in the following that sk_{ID^*} is enough to decrypt the ciphertext C_b^*.

According to the above steps, for each $i \in [d]$, we know that

$$\begin{aligned} sk_i^* &= {c_i}^r \cdot t_i \\ &= \left(h_1^r h_2^{ar}\right)^{\frac{\alpha \cdot q(i)}{q(0) \cdot H_1(id_i^*, i) + H_2(i)}} \cdot \left(h_0 h_2^b\right)^{\frac{\alpha \cdot q(i)}{q(0) \cdot H_1(id_i^*, i) + H_2(i)}} \\ &= \left(h_0 h_1^r h_2^{f(r)}\right)^{\frac{\alpha \cdot q(i)}{q(0) \cdot H_1(id_i^*, i) + H_2(i)}} \end{aligned}$$

Now, we show that $\mathcal{A}$ is able to decrypt the ciphertext C_b^* using sk_{ID^*} and hence he determines the bit b.

Upon receiving the ciphertext $C_b^* = (u_1, \cdots, u_n, v_1, v_2, w, \beta)$, $\mathcal{A}$ performs as follows:

1. Let $\Delta'_{i,[d]}(0) = \Delta_{i,[d]}(0)/(i^d + 1)$.
2. Compute $\prod_{i \in [d]} e(u_i, sk_i^*)^{\Delta'_{i,[d]}(0)} / (v_1^r \cdot v_2^{f(r)}) = e(g_3, h_0)^{s \cdot E(0)}$.

We can verify its correctness as follows:

$$
\begin{aligned}
&\frac{\prod_{i\in[d]} e(u_i, sk_i^*)^{\Delta'_{i,[d]}(0)}}{v_1^r \cdot v_2^{f(r)}} \\
&= \frac{\prod_{i\in[d]} e\Big((g_2^{H_1(id_i^*,i)} \cdot g^{H_2(i)})^{s\cdot E(i)}, (h_0 h_1^r h_2^{f(r)})^{\frac{\alpha\cdot q(i)}{q(0)\cdot H_1(id_i^*,i)+H_2(i)}}\Big)^{\Delta'_{i,[d]}(0)}}{e(g_3,h_1)^{r\cdot s\cdot E(0)} \cdot e(g_3,h_2)^{f(r)\cdot s\cdot E(0)}} \\
&= \frac{\prod_{i\in[d]} e\Big(g^s, h_0 h_1^r h_2^{f(r)}\Big)^{\alpha\cdot E(i)\cdot q(i)\cdot \Delta'_{i,[d]}(0)}}{\Big(e(g_3,h_1)^r \cdot e(g_3,h_2)^{f(r)}\Big)^{s\cdot E(0)}} \\
&= \frac{e\Big(g^{\alpha\cdot q(0)}, h_0 h_1^r h_2^{f(r)}\Big)^{s\cdot E(0)}}{e\Big(g_3, h_1^r h_2^{f(r)}\Big)^{s\cdot E(0)}} \\
&= e(g_3,h_0)^{s\cdot E(0)}
\end{aligned}
$$

3. Set $\gamma = H_3(u_1, \cdots, u_n, v_1, v_2, e(g_3,h_0)^{s\cdot E(0)})$.
4. Output $m_b = w/\Big(e(g_3,h_0)^{s\cdot E(0)} \cdot e(g_3,h_0)^{\gamma}\Big)$.

It's clear that Ren et al.'s fuzzy IBE scheme is broken. That is their scheme is even not chosen-plaintext secure. Notice that this attack is actually a collusion attack [4]. The inherent reason why the above attack works is that the polynomial $q(x)$ is the same for all identities in Ren et al.'s scheme.

5 Conclusion

Recently, Ren et al. [6] proposed a new fuzzy IBE scheme and proved that it is chosen-ciphertext secure in the standard model. In this paper, however, we have indicated that their scheme is even not chosen-plaintext secure.

Acknowledgements

This work is supported by the Major Research Plan of the National Natural Science Foundation of China No. 90818005, the National Natural Science Foundation of China No. 60903217, No. 60773032 and by the Postdoctoral Science Foundation of China No. 20090450701.

References

1. A. Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO84, LNCS 196, Springer-Verlag, pp.47–53, 1985.
2. D. Boneh, M. Franklin, Identity-based encryption from the Weil Pairing, in: CRYPTO 2001, LNCS 2139, Springer-Verlag, pp.213–229, 2001.

3. C. Cocks, An identity based encryption scheme based on quadratic residues, in: IMA International Conference on Cryptography and Coding 2001, LNCS 2260, Springer-Verlag, pp.360–363, 2001.
4. A. Sahai, B. Waters, Fuzzy Identity-Based Encryption, in: EUROCRYPT 2005, LNCS 3494, Springer-Verlag, pp.457–473, 2005.
5. J. Baek, W. Susilo, J. Zhou, New constructions of fuzzy identity-based encryption, in: ASIACCS'07, pp. 368–370, 2007.
6. Y. Ren, D. Gu, S. Wang, X. Zhang, New Fuzzy Identity-Based Encryption in the Standard Model, Informatica, vol. 21, no. 3, pp. 393–407, 2010.