Security of a Biometric Identity-based Encryption Scheme

Miaomiao Tian, Wei Yang, and Liusheng Huang
(Corresponding author: Miaomiao Tian)

School of Computer Science and Technology, University of Science and Technology of China
Hefei 230026, P.R. China (Email: miaotian@mail.ustc.edu.cn)

(Received Oct. 13, 2011; revised and accepted Mar. 6, 2012)

Abstract

Biometric identity-based encryption (Bio-IBE) is a kind of fuzzy identity-based encryption (fuzzy IBE) where a ciphertext encrypted under an identity w' can be decrypted using a secret key corresponding to the identity w which is close to w' as measured by some metric. Recently, Yang et al. proposed a constant-size Bio-IBE scheme and proved that it is secure against adaptive chosen-ciphertext attack (CCA2) in the random oracle model. Unfortunately, in this paper, we will show that their Bio-IBE scheme is even not chosen-plaintext secure. Specifically, user w using his secret key is able to decrypt any ciphertext encrypted under an identity w' even though w is not close to w'.

Keywords: Biometric identity-based encryption, chosen-ciphertext secure, chosen-plaintext secure, cryptanalysis

1 Introduction

To simplify the certificate management in traditional public key infrastructure, Shamir [7] first introduced the concept of identity-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 [1] and [3], respectively.

The notion of fuzzy identity-based encryption (fuzzy IBE) was introduced by Sahai and Waters [4] in 2005, where each identity is viewed as a set of descriptive attributes. A fuzzy IBE scheme is very similar to a standard IBE scheme except that a ciphertext encrypted under an identity w' can be decrypted using the secret key associated with the identity w which is close to w' as judged by some metric. The error-tolerance property of fuzzy IBE enables biometric attributes to be used in a standard IBE scheme. In 2007, Burnett et al. [2] proposed the first biometric identity-based signature (Bio-IBS) scheme, where they used biometric information to construct the identity of a user. The first biometric identity-based encryption (Bio-IBE) scheme was proposed by Sarier [5] in 2008. It absorbed the advantage of Burnett et al.'s Bio-IBS scheme. Subsequently, Sarier [6] presented an improved Bio-IBE scheme which is secure against a new type of denial of service attack. Recently, Yang et al. [8] presented a constant-size Bio-IBE scheme and proved that it is secure against adaptive chosen-ciphertext attack (CCA2) in the random oracle model. Unfortunately, in this paper, we will show that their scheme is even not chosen-plaintext secure.

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

2 Preliminaries

2.1 Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups with the same prime order p. A map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ 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 Biometric Identity-based Encryption

As mentioned above, a Bio-IBE scheme is essentially a fuzzy IBE scheme, with the only difference that it uses a set of biometric attributes as a user's identity. Therefore, a Bio-IBE scheme also consists of the following four algorithms [4]:

- **Setup:** Given 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 biometric attribute set $w = (\mu_1, \cdots, \mu_n)$, the PKG generates a secret key sk_w for the user.
- **Encrypt:** On input the public parameters PP, a message m and a user's biometric attribute set $w' = (\mu'_1, \cdots, \mu'_n)$, it returns a ciphertext C'.
- **Decrypt:** On input the public parameters PP, a secret key sk_w corresponding to the user w, and a ciphertext C' encrypted under the set of attributes w', it outputs the message if and only if $|w' \bigcap w| \geq d$.

The security notion for Bio-IBE proposed by Yang et al. [8] is indistinguishability of ciphertext under adaptive chosen ciphertext attack (IND-sID-CCA2). A weaker security notion proposed in [4] is indistinguishability of ciphertext under chosen plaintext attack (IND-sID-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 attribute set $w' = (\mu'_1, \cdots, \mu'_n)$.
- **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 attribute sets w_i, where $|w' \bigcap w_i| < d$ for all i. The challenger $\mathcal{C}$ runs the **Extract** algorithm to obtain a private key sk_{w_i} for each w_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 w'. 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 Bio-IBE scheme is IND-sID-CPA secure if there is no polynomial-time adversary that succeeds in the above game with a non-negligible advantage.

2.3 Fuzzy Extraction

Fuzzy extraction process is essential for many Bio-IBE schemes such as [5, 6, 8]. Let $\mathcal{M} = \{0,1\}^k$ be a finite dimensional metric space with a distance function $\mathsf{dis} : \mathcal{M} \times \mathcal{M} \longrightarrow Z^+$. An $(\mathcal{M}, l, t)$ fuzzy extractor consists of the following two functions Gen and Rep:

- Gen: This function takes as input a biometric template $b \in \mathcal{M}$. It outputs an identity $ID \in \{0,1\}^l$ and a public parameter PAR. The biometric template b is unique for each user since it is a concatenation of user's biometric attributes.
- Rep: This function takes as input a biometric template $b' \in \mathcal{M}$ and the public parameter PAR. It outputs the identity ID if $\mathsf{dis}(b, b') \leq t$. In other words, we can obtain the same identity ID as long as b' is "close" to b.

For two biometric attribute sets w and w', we assume that $\mathsf{dis}(b, b') \leq t$ if $|w' \bigcap w| \geq d$ and thus we have $ID = ID'$, where (b, ID) and (b', ID') are extracted from w and w', respectively.

3 Review of Yang et al.'s Bio-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 $\mathbb{Z}_p^*$. The Yang et al.'s Bio-IBE [8] 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 $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ and a generator g of $\mathbb{G}$.
2) Select two hash functions $H : b \rightarrow \{0,1\}^*$ and $H_1 : \mathbb{Z}_p^* \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$.
3) Pick $s \in \mathbb{Z}_p^*$ and $g_1 \in \mathbb{G}$ uniformly at random, and set $g_2 = g^s$.
4) Publish the public parameters $PP = (\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, d, H, H_1)$ and keep the master key s secret.

Extract: Given a user's biometric attribute set $w = (\mu_1, \cdots, \mu_n)$, the PKG does:

1) Compute $ID = H(b)$ and $PAR = \mathsf{Gen}(b)$, where b is a concatenation of each μ_i $(1 \leq i \leq n)$.
2) Choose a random $d-1$ degree polynomial $q(x) \in \mathbb{Z}_p^*[x]$ such that $q(0) = s$.
3) For each $i \in [n]$, compute $d_{i,1} = (g_1 \cdot g^{H_1(ID)})^{q(\mu_i)}$ and $d_{i,2} = g^{q(\mu_i)}$.
4) Send the private key $sk_w = (d_{i,1}, d_{i,2})_{\mu_i \in w}$ to the user and publish PAR.

Encrypt: On input the public parameters PP, a message $m \in \mathbb{G}_T$ and an identity $w' = (\mu'_1, \cdots, \mu'_n)$, the sender does:

1) Get the public parameter PAR of the receiver and compute $ID' = \mathsf{Rep}(b', PAR)$, where b' is a concatenation of each μ'_i $(1 \leq i \leq n)$.
2) Choose $r \in \mathbb{Z}_p^*$ uniformly at random.
3) Compute $C_1 = g^r$, $C_2 = (g^{H_1(ID')})^r$ and $C_3 = m \cdot e(g_1, g_2)^r$.
4) Send $C' = (w', C_1, C_2, C_3)$.

Decrypt: To decrypt the ciphertext C' encrypted under the attribute set w', a user with attribute set w satisfying $|w' \bigcap w| \geq d$ does:

1) Choose an arbitrary set $S \subseteq w' \bigcap w$ such that $|S| = d$.
2) Compute $m = C_3 \cdot \frac{e\left(C_2, \prod_{\mu_i \in S}(d_{i,2})^{\Delta_{\mu_i,S}(0)}\right)}{e\left(C_1, \prod_{\mu_i \in S}(d_{i,1})^{\Delta_{\mu_i,S}(0)}\right)}$.

The **Decrypt** algorithm works since $ID = ID'$ when $|w' \bigcap w| \geq d$ and

$$\begin{aligned}
& C_3 \cdot \frac{e\big(C_2, \prod_{\mu_i \in S}(d_{i,2})^{\Delta_{\mu_i,S}(0)}\big)}{e\big(C_1, \prod_{\mu_i \in S}(d_{i,1})^{\Delta_{\mu_i,S}(0)}\big)} \\
= \; & C_3 \cdot \frac{e\big((g^{H_1(ID')})^r, \prod_{\mu_i \in S}(g^{q(\mu_i)})^{\Delta_{\mu_i,S}(0)}\big)}{e\big(g^r, \prod_{\mu_i \in S}(g_1 \cdot g^{H_1(ID)})^{q(\mu_i)\cdot\Delta_{\mu_i,S}(0)}\big)} \\
= \; & C_3 \cdot \frac{e\big(g^{H_1(ID')\cdot r}, g^s\big)}{e\big(g^r, (g_1 \cdot g^{H_1(ID)})^s\big)} \\
= \; & m \cdot e(g_1, g_2)^r \cdot \frac{e\big(g^{H_1(ID)\cdot r}, g^s\big)}{e\big(g^s, (g_1 \cdot g^{H_1(ID)})^r\big)} \\
= \; & m \cdot e(g_1, g^s)^r / e\big(g^s, (g_1)^r\big) \\
= \; & m
\end{aligned}$$

Remark. Compared to the scheme in [8], there is a small (but important) modification in the above scheme. Namely, we use $H_1(ID)$ (resp. $H_1(ID')$) instead of $H_1(w, ID)$ (resp. $H_1(w', ID')$). We know that, for two random strings w and w', $H_1(w, ID) = H_1(w', ID)$ cannot be true in general. Therefore, the original **Decrypt** algorithm in [8] may fail. In our modified scheme, the **Decrypt** algorithm will work since $H_1(ID) = H_1(ID')$ when $|w' \bigcap w| \geq d$. In fact, $H_1(ID)$ plays the same role as $H_1(w, ID)$ in this scheme.

4 Our Attack

Yang et al. [8] proved that their scheme is IND-sID-CCA2 secure in the random oracle model. However, in this section, we show that their scheme is even not IND-sID-CPA secure. Assume that the target attribute set is $w' = (\mu'_1, \cdots, \mu'_n)$. A polynomial time adversary $\mathcal{A}$ attacks Yang at al.'s Bio-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, the adversary $\mathcal{A}$ makes a secret key extraction query on an attribute set w, where $|w' \bigcap w| < d$. The challenger $\mathcal{C}$ runs the **Extract** algorithm to obtain a private key sk_w for w and sends the result 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 **Encrypt**(m_b, w') 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) For each $\mu_i \in w$, let $d_{i,1} = (g_1 \cdot g^{H_1(ID)})^{q(\mu_i)}$ and $d_{i,2} = g^{q(\mu_i)}$. Then $sk_w = (d_{i,1}, d_{i,2})_{\mu_i \in w}$. Upon receiving the ciphertext $C'_b = (w', C_1, C_2, C_3) = (w', g^r, (g^{H_1(ID')})^r, m_b \cdot e(g_1, g_2)^r)$, $\mathcal{A}$ determines the bit b by performing the following steps:
    a. For each $\mu_i \in w$, compute $g_1^{q(\mu_i)} = d_{i,1}/d_{i,2}^{H_1(ID)}$.
    b. Set $d'_{i,1} = g_1^{q(\mu_i)} \cdot d_{i,2}^{H_1(ID')} = (g_1 \cdot g^{H_1(ID')})^{q(\mu_i)}$ and $d'_{i,2} = d_{i,2} = g^{q(\mu_i)}$ for each $\mu_i \in w$.
    c. Select an arbitrary set $S \subseteq w$ such that $|S| = d$.
    d. Output $m_b = C_3 \cdot \frac{e\left(C_2, \prod_{\mu_i \in S}(d'_{i,2})^{\Delta_{\mu_i,S}(0)}\right)}{e\left(C_1, \prod_{\mu_i \in S}(d'_{i,1})^{\Delta_{\mu_i,S}(0)}\right)}$.

We can verify its correctness as follows:

$$\begin{aligned}
& C_3 \cdot \frac{e\big(C_2, \prod_{\mu_i \in S}(d'_{i,2})^{\Delta_{\mu_i,S}(0)}\big)}{e\big(C_1, \prod_{\mu_i \in S}(d'_{i,1})^{\Delta_{\mu_i,S}(0)}\big)} \\
= \; & C_3 \cdot \frac{e\big((g^{H_1(ID')})^r, \prod_{\mu_i \in S}(g^{q(\mu_i)})^{\Delta_{\mu_i,S}(0)}\big)}{e\big(g^r, \prod_{\mu_i \in S}(g_1 \cdot g^{H_1(ID')})^{q(\mu_i)\cdot\Delta_{\mu_i,S}(0)}\big)} \\
= \; & C_3 \cdot \frac{e\big(g^{H_1(ID')\cdot r}, g^s\big)}{e\big(g^r, (g_1 \cdot g^{H_1(ID')})^s\big)} \\
= \; & m_b \cdot e(g_1, g_2)^r \cdot \frac{e\big(g^{H_1(ID')\cdot r}, g^s\big)}{e\big(g^s, (g_1 \cdot g^{H_1(ID')})^r\big)} \\
= \; & m_b \cdot e(g_1, g^s)^r / e\big(g^s, (g_1)^r\big) \\
= \; & m_b
\end{aligned}$$

It's clear that Yang et al.'s Bio-IBE scheme is broken. That is their scheme is not chosen-plaintext secure. In the above attack, a user with identity w is able to convert his secret key sk_w into a new one $sk'_w = (d'_{i,1}, d'_{i,2})_{\mu_i \in w}$, which can be used to decrypt ciphertexts encrypted under the identity w'. Notice that w and w' may be arbitrary identities. Consequently, in Yang et al.'s scheme, a valid user can decrypt any ciphertext encrypted under any identity using his secret key.

5 Conclusion

Recently, Yang et al. [8] proposed a constant-size Bio-IBE scheme and proved that it is adaptively chosen-ciphertext secure in the random oracle 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), the Fundamental Research Funds for the Central Universities (No. WK0110000027), and the Natural Science Foundation of Jiangsu Province of China (No. BK2011357).

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Advances in Cryptology-CRYPTO 2001*, pp. 213–229. Springer, 2001.

[2] A. Burnett, F. Byrne, T. Dowling, and A. Duffy, “A biometric identity based signature scheme,” *International Journal of Network Security*, vol. 5, no. 3, pp. 317–326, 2007.

[3] C. Cocks, “An identity based encryption scheme based on quadratic residues,” *Cryptography and Coding*, pp. 360–363, 2001.

[4] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” *Advances in Cryptology–EUROCRYPT 2005*, pp. 557–557, 2005.

[5] N.D. Sarier, “A new biometric identity based encryption scheme,” in *Proceedings of the 9th International Conference for Young Computer Scientists (ICYCS 2008)*, pp. 2061–2066. IEEE, 2008.

[6] N.D. Sarier, “A new biometric identity based encryption scheme secure against dos attacks,” *Security and Communication Networks*, vol. 4, no. 1, pp. 23–32, 2011.

[7] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology-CRYPTO’84*, pp. 47–53. Springer, 1985.

[8] Y. Yang, Y. Hu, L. Zhang, and C. Sun, “Cca2 secure biometric identity based encryption with constant-size ciphertext,” *Journal of Zhejiang University-Science C*, vol. 12, no. 10, pp. 819–827, 2011.

Miaomiao Tian is a Ph.D. student in School of Computer Science and Technology at University of Science and Technology of China. His research interests include cryptography and information security.

Wei Yang is a postdoctoral research fellow in School of Computer Science and Technology at University of Science and Technology of China. In 2007, he received his Ph.D. degree in computer science from University of Science and Technology of China and was awarded the Dean’s Prize of Chinese Academy of Sciences. His research interests include quantum information and cryptography.

Liusheng Huang is a professor in School of Computer Science and Technology at University of Science and Technology of China. His research interests include information security, wireless sensor network and distributed computing. He is author or coauthor of more than 100 research papers and 6 books.