INFORMATICA, 2012, Vol. 23, No. 2, 299–314

Cryptanalysis of a Fuzzy Identity Based Encryption Scheme in the Standard Model

Xu An WANG[1], Xiaoyuan YANG[1], Minqing ZHANG[1], Yong YU[2]

[1] *Key Laboratory of Information and Network Security*
Engineering University of Chinese Armed Police Force
Xi'an 710086, P.R. China
[2] *School of Computer Science and Engineering*
University of Electronic Science and Technology of China
Chengdu 610054, P.R. China
e-mail: wangxahq@yahoo.com.cn

Received: October 2010; accepted: December 2011

Abstract. Fuzzy identity based encryption (FIBE), proposed by Sahai and Waters, is a new kind of identity based encryption. It allows users with identity w can decrypt ciphertext for w' if and only if w is close enough to w'. Recently, Ren *et al.* proposed a new FIBE scheme and claimed it is fully CCA2 secure in the standard model with a tight reduction. However, in this paper we will show that their scheme is not correct. Furthermore, the key generation process of their scheme cannot resist the collusion attack, which is a basic security requirement for FIBE. At last, we propose a new fully secure FIBE scheme based on the Sahai–Waters FIBE scheme and prove its security by using the "dual system encryption" technique.

Keywords: cryptography, fuzzy identity based encryption, fully secure, CCA2-secure, attack.

1. Introduction

Shamir (1984) introduced the concept of identity based encryption (IBE), whose motivation is to ease the certificate management. A user's public key in an identity based system is some unique information about the identity of the user (e.g., email address). However, only in 2001 the first practical identity based encryption was realized by Boneh and Franklin using bilinear maps on elliptic curve. However, their scheme can only be proved secure in the random oracle model. In Eurocrypt'03, Canetti *et al.* proposed a weaker security notion, selective identity (selective-ID) security for IBE, relative to which they were able to build an inefficient but secure IBE scheme in the standard model (Canetti *et al.*, 2003). In Eurocrypt'04, Boneh and Boyen proposed two new efficient selective identity secure identity based encryption schemes without random oracles (BB_1 IBE and BB_2 IBE) (Boneh and Boyen, 2004a). In Crypto'04, they improved their scheme to full security (Boneh and Boyen, 2004b) but with a loose security reduction. In Eurocrypt'05, Waters improved their work by proposing a fully secure identity based encryption with tight security proof in the standard model (Waters' IBE; Waters, 2005). In Eurocrypt'06, Gentry gave another interesting efficient fully secure identity based encryption with tight security proof in the standard model but based on a strong assumption (Gentry's IBE; Gentry, 2006).

1.1. *Fuzzy Identity Based Encryption*

In Eurocrypt'05, Sahai and Waters introduced a new concept, fuzzy identity based encryption (FIBE), which aimed at error-tolerance property of IBE (Sahai and Waters, 2005). In a FIBE, a user with the secret key for the identity w is able to decrypt a ciphertext encrypted with the public key w' if and only if ID and ID' are within a certain distance of each other as judged by some metric. FIBE at least has two interesting applications, the first is an IBE system with biometric identities, the error-tolerance property of FIBE allows for a private key (derived from a measurement of a biometric) to decrypt a ciphertext encrypted with a slightly different measurement of the same biometric. Secondly FIBE can be used for "attribute-based encryption (ABE)", where both ciphertexts and secret keys are associated with sets of attributes. Decryption is enabled if and only if the cipertext and secret key attribute sets overlap by at least a fixed threshold value d. Goyal *et al.* (2006) proposed an ABE scheme that provides fine-grained sharing of encrypted data. Piretti *et al.* (2006) used FIBE to realize their secure information management architecture. Later Baek *et al.* constructed two new efficient FIBE schemes in the random oracle model (Baek *et al.*, 2007).

1.2. *Dual System Encryption*

In Crypto'09, Waters (2009) introduced a new methodology named "dual system encryption" for proving security of encryption systems. In this system, both ciphertexts and private keys can take on one of two indistinguishable forms, semi-functional one or normal one. A semi-functional private key will be able to decrypt all normally generated ciphertexts; however, a semi-functional private key cannot decrypt a semi-functional ciphertext. The security can be reduced to a sequence of games, where the challenge ciphertext and the private keys one by one were changed to be semi-functional. In the finally game, the challenge ciphertext and all private keys are semi-functional, at which point the adversary can only guess the challenge plaintext randomly. In TCC'10, Lewko and Waters 2010b) realized the dual system encryption in the composite order group and thus achieve fully secure IBE and HIBE scheme with simple structure. In Eucrypto'10, Lewko *et al.* (2010) construct the fully secure ABE also by using dual system encryption technique.

1.3. *Our Contribution*

Recently Ren *et al.* (2010) claimed to construct a fully CCA2 secure FIBE in the standard model with a tight reduction. However, we will show that their scheme is not correct at all. Furthermore, the key generation process of their scheme cannot resist the collusion attack, which is crucial for FIBE. As an improvement of Ren *et al.* 's FIBE result, we propose a new fully secure FIBE scheme based on the Sahai–Waters FIBE scheme and prove its security by using the "dual system encryption" technique.

1.4. *Organization*

The organization of this paper is as follows. Section 2 gives the definition and security model for FIBE. We review Ren *et al.*'s scheme and show their scheme is not correct and secure at all in Section 3. In Section 4, we propose our new FIBE scheme and prove its security. We conclude our paper in the last section.

2. Definition and Security Model for FIBE

2.1. *Definition*

A FIBE consists of the following algorithms.

1. Setup(1^k). Taking 1^k as the security parameter, the Private Key Generator (PKG) runs this algorithm to generate its master key mk and public parameters $params$ which contains an error tolerance parameter d. Note that $params$ is given to all interested parties while mk is kept secret.
2. Extract(mk, ID). Taking the master key mk and an identity ID as input, the PKG runs this algorithm to generate a private key associated with ID, denoted by d_{ID}.
3. Encrypt($params$, ID$'$, M). Taking the public parameters $params$, an identity ID$'$, and a plaintext M as input, a sender runs this algorithm to generate a ciphertext C'.
4. Decrypt($params$, d_{ID}, C'). Taking the public parameters $params$, a private key d_{ID} associated with the identity ID and a ciphertext C encrypted with an identity ID such that $|\mathsf{ID}' \cap \mathsf{ID}| > d$ as input, a receiver runs this algorithm to get a decryption, which is either a plaintext or a "Reject" message.

2.2. *Security Model*

(IND-FID-CCA2 and IND-FID-CPA Security.) The semantic security against an adaptive chosen ciphertext attack security for a fuzzy IBE system is defined by the following game between an adversary and a challenger.

Setup. The challenger runs algorithm Setup, and forwards parameters to the adversary.

Phase 1. Proceeding adaptively, the adversary issues queries $q_1, \ldots, q_m$, where q_i is one of the following:

- Key generation query $\langle \mathsf{ID}_i \rangle$ The challenger runs algorithm KeyGen on ID_i and forwards the resulting private key to the adversary.
- Decryption query $\langle \mathsf{ID}_i, c_i \rangle$ The challenger runs algorithm KeyGen on ID_i, decrypts c_i with the resulting private key, and sends the result to the adversary.

Challenge. The adversary sends $(\mathsf{ID}^*, m_0, m_1)$ to the challenger, where $|\mathsf{ID} \cap \mathsf{ID}^*| < d$, and ID denotes the identity that has appeared in key generation and decryption query in Phase 1. The challenger selects a random bit $k \in \{0, 1\}$, sets $c^* = \text{Encrypt}(params, \mathsf{ID}^*, m_k)$, and sends c^* to the adversary as its challenged ciphertext.

Phase 2. $\mathcal{A}$ executes the following queries:

- Key generation query $\langle \mathsf{ID} \rangle$, where $|\mathsf{ID} \cap \mathsf{ID}^*| < d$.
- Decryption query $\langle \mathsf{ID}, c \rangle$, where $c \neq c^*$.

These queries maybe be adaptive.

Guess. The adversary submits a guess $k' \in \{0, 1\}$.

We call an adversary $\mathcal{A}$ in the above game an IND-FID-CCA2 adversary. The advantage of $\mathcal{A}$ is defined as $|Pr[k = k'] - \frac{1}{2}|$.

DEFINITION 1. A fuzzy IBE system is (t, ϵ, q_k, q_d) IND-FID-CCA2 secure if all t-time IND-FID-CCA2 adversaries making at most q_k key generation queries and q_d decryption queries have advantage of at most ϵ in the above game.

We call an adversary $\mathcal{A}$ an IND-FID-CPA adversary if the adversary remain the same in the above game except it cannot execute decryption queries. The advantage of $\mathcal{A}$ is defined as $|Pr[k = k'] - \frac{1}{2}|$.

DEFINITION 2. A fuzzy IBE system is (t, ϵ, q_k) IND-FID-CPA secure if all t-time IND-FID-CCA2 adversaries making at most q_k key generation queries have advantage of at most ϵ in the above game.

Collusion Attack Security. Collusion attack for a fuzzy IBE system is defined by the following game between an adversary and a challenger.

Setup. The challenger runs algorithm Setup, and forwards parameters to the adversary.

Phase 1. Proceeding adaptively, the adversary issues queries $q_1, \ldots, q_m$, where q_i is one of the following:

- Key generation query $\langle \mathsf{ID}_i \rangle$ The challenger runs algorithm KeyGen on ID_i and forwards the resulting private key to the adversary.

Challenge. The adversary can output a valid private key of ID^* which is not equal any of ID_i $(i = 1 \ldots, m)$

We call the adversary successfully run the collusion attack on the scheme.

3. Cryptanalysis of Ren *et al.*'s FIBE Scheme

3.1. *Review of Ren et al.'s FIBE Scheme*

Assume an identity $\mathsf{ID} = (ID_1, ID_2, \ldots, ID_n)$, where n is the length of ID and $ID_i \in Z_p^*$ represents the minimal error tolerance and $n > d$. Now we wish to create a FIBE scheme in which a ciphertext created using identity ID' can be decrypted only by a private key associated with identity ID, where $|\mathsf{ID} \cap \mathsf{ID}'| > d$. We also define the Lagrange coefficient $\Delta_{i,S}$ for $i \in Z_p^*$ and a set S, of elements in Z_p^* : $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$.

Setup. 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, $h : (Z_p^*)^{\{0,1\}} \times \{1, 2, \dots, n\} \to Z_p^*$, $H : G_1^n \times G_2^l \to Z_p^*$ are collision-resistant hash functions, where $l \in Z_p^*$. The PKG randomly choose $\alpha \in Z_p^*$, $h_0, h_1, h_2 \in G_1$, and two random polynomials $f(x), q(x) \in Z_p^*[x]$ of degree 1 and $d - 1$ respectively, where $f(x) = ax + b$. If $h_0 = h_2^{-a}$ or $h_1 = h_2^{-b}$, randomly choose $f(x)$ again. The PKG computes $g_1 = g^{\alpha}, g_2 = g^{q(0)}, g_3 = g_1^{q(0)}$. The public parameters are $(g, g_1, g_2, g_3, h_0, h_1, h_2, d, h, H, f(x))$ and $\alpha, q(x)$ are the private keys of PKG.

KeyGen. To a user U with identity $\mathsf{ID} = (ID_1, ID_2, \dots, ID_n)$, the PKG randomly chooses $r_0 \in Z_p^*$ and computes

$$d_0 = r_0, d_i = \Big(h_0 h_1^{r_0} h_2^{f(r_0)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_i,i)+h(i)}} \quad (i = 1, 2, \dots, n),$$

so the private key of U is $d_{\mathsf{ID}} = (d_0, d_1, d_2, \dots, d_n)$.

Encrypt. To encrypt a message $m \in G_2$ with a key associated with identity $\mathsf{ID}' = (ID'_1, \dots, ID'_n)$, randomly choose $s \in Z_p^*$ and a polynomial $A(x) \in Z_p^*[x]$ of degree $d - 1$, compute:

$$u_i = (g_2^{h(ID'_i,i)} \cdot g^{h(i)})^{sA(i)} \ (i = 1, 2, \dots, n), \qquad v_1 = e(g_3, h_1)^{sA(0)},$$
$$v_2 = e(g_3, h_2)^{sA(0)}, \qquad w = m \cdot e(g_3, h_0)^{sA(0)+\gamma},$$
$$\beta = H\Big(u_1, \dots, u_n, v_1, v_2, w, m \cdot e(g_3, h_0\Big)^{sA(0)}),$$

where $\gamma = H(u_1, \dots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)})$. The ciphertext of message m is $c = (u_1, \dots, u_n, v_1, v_2, w, \beta)$.

Decrypt. Suppose that a ciphertext c is encrypted with a key associated with identity ID' and we have a private key for identity ID, where $|\mathsf{ID} \cap \mathsf{ID}'| > d$. Choose an arbitrary d-element subset $S = \{i | i \in \{1, \dots, n\}, ID_i \in \mathsf{ID} \cap \mathsf{ID}'\}$ and decrypt

$$\frac{\prod_{i \in S} e(u_i, d_i)^{\Delta_{i,S}(0)}}{v_1^{d_0} v_2^{f(d_0)}} = e(g_3, h_0)^{sA(0)},$$
$$\gamma = H\big(u_1, \dots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)}\big),$$
$$\frac{w}{e(g_3, h_0)^{\gamma}} = R, \beta' = H(u_1, \dots, u_n, v_1, v_2, w, R),$$

and verify whether $\beta' = \beta$. If yes, decrypt $\frac{R}{e(g_3,h_0)^{sA(0)}} = m$. Otherwise, return an error message.

3.2. *On the Correctness*

In Ren *et al.* (2010), the correctness of the new fuzzy IBE scheme is shown as follows where $ID_i \in \mathsf{ID} \cap \mathsf{ID}'$ if $i \in S$.

$$\begin{aligned} e(u_i, d_i) &= e\Big(\big(g_2^{h(ID'_i,i)} \cdot g^{h(i)}\big)^{sA(i)}, \big(h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\frac{\alpha \cdot q(i)}{q(0)h(ID_i,i)+h(i)}}\Big) \\ &= e\Big(g^{sA(i)(q(0)h(ID_i,i)+h(i))}, \big(h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\frac{\alpha \cdot q(i)}{q(0)h(ID_i,i)+h(i)}}\Big) \\ &= e\Big(g^{sA(i)}, \big(h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\alpha q(i)}\Big), \end{aligned}$$

$$\begin{aligned} &\prod_{i\in S} e(u_i, d_i)^{\delta_{i,S}(0)} \\ &\quad = \prod_{i\in S} e\Big(\big(g^{sA(i)}, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\alpha q(i)}\Big)^{\delta_{i,S}(0)} \\ &\quad = e\big(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\Sigma_{i\in S} A(i)q(i)\delta_{i,S}(0)} \\ &\quad = e\big(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{A(0)q(0)} \\ &\quad = e(g_3, h_0)^{sA(0)} e(g_3, h_1)^{sr_0A(0)} e(g_3, h_2)^{sf(r_0)A(0)}, \\ &\frac{\prod_{i\in S} e(u_i, d_i)^{\delta_{i,S}(0)}}{v_1^{d_0} v_2^{f(d_0)}} = e(g_3, h_0)^{sA(0)}, \\ &\gamma = H\big(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)}\big), \\ &\frac{w}{e(g_3, h_0)^{\gamma}} = m \cdot e(g_3, h_0)^{sA(0)} = R, \\ &\beta' = H(u_1, \ldots, u_n, v_1, v_2, w, R) = \beta, \qquad R/e(g_3, h_0)^{sA(0)} = m. \end{aligned}$$

But actually, the equation of

$$e\big(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\Sigma_{i\in S} A(i)q(i)\delta_{i,S}(0)} = e\big(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{A(0)q(0)}$$

cannot hold.

In the reconstruction of an interpolating polynomial, n point-values are required to reconstruct a polynomial with degree $n-1$ to satisfy these n point-values. The degree of $A(x)q(x)$ is the sum of the degrees of $A(x)$ and $q(x)$, which is $2d-2$. But $S = \{i \mid i \in \{1, \ldots, n\}, ID_i \in \mathsf{ID} \cap \mathsf{ID}'\}$ is a d-element subset, which is not $2d-1$, meaning the above equation cannot hold at all. Thus the Decrypt algorithm is not correct.

3.3. *Collusion Attack*

Ren *et al.* claimed that their FIBE scheme is IND-FID-CCA secure, However, in this section, we show that this is not true. Concretely, there exists a polynomial time adversary $\mathcal{A}$ who can act the collusion attack against the FIBE scheme. Adversary $\mathcal{A}$ works as follows:

1. In Setup phase, adversary $\mathcal{A}$ obtains the public parameters $params$ from the challenger.
2. In $\mathsf{Phase\ 1}$ and $\mathsf{Challenge}$ phase, adversary $\mathcal{A}$ chooses a target identity $\mathsf{ID}^* = (ID_1^*, \ldots, ID_n^*)$, denote

$$\begin{aligned}
\widehat{\mathsf{ID}}_1 &= (ID_1^*, ID_{21}, \ldots, ID_{n1}),\\
\widehat{\mathsf{ID}}_2 &= (ID_{12}, ID_2^*, \ldots, ID_{n2}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
\widehat{\mathsf{ID}}_n &= (ID_{1n}, ID_{2n}, \ldots, ID_n^*),
\end{aligned}$$

where $ID_{1i} \neq ID_1^*$ $(i = 2, 3, \ldots, n)$, $ID_{2i} \neq ID_2^*$ $(i = 1, 3, \ldots, n)$, …, $ID_{ni} \neq ID_n^*$ $(i = 1, 2, \ldots, n-1)$. Note here $\widehat{\mathsf{ID}}_1, \widehat{\mathsf{ID}}_2, \ldots, \widehat{\mathsf{ID}}_n$ all satisfies $|\mathsf{ID} \cap \mathsf{ID}^*| < d$.

   (a) First adversary $\mathcal{A}$ issues key generation queries on every $\widehat{\mathsf{ID}}_i$ $(i = 1, \ldots, n)$ two times, he will get the private keys as follows:

$$\begin{aligned}
d^0_{\widehat{\mathsf{ID}}_1} &= \Big\{ d^0_{01} = r^0_1, d^0_{11} = \Big(h_0 h_1^{r^0_1} h_2^{f(r^0_1)}\Big)^{\frac{\alpha q(1)}{q(0)h(ID^*_1,1)+h(1)}},\\
&\qquad d^0_{i1} = \Big(h_0 h_1^{r^0_1} h_2^{f(r^0_1)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_{i1},i)+h(i)}} \ (i = 2, 3, \ldots, n)\Big\},\\
d^1_{\widehat{\mathsf{ID}}_1} &= \Big\{ (d^1_{01} = r^1_1, d^1_{11} = \Big(h_0 h_1^{r^1_1} h_2^{f(r^1_1)}\Big)^{\frac{\alpha q(1)}{q(0)h(ID^*_1,1)+h(1)}},\\
&\qquad d^1_{i1} = \Big(h_0 h_1^{r^1_1} h_2^{f(r^1_1)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_{i1},i)+h(i)}} \ (i = 2, 3, \ldots, n)\Big\},\\
d^0_{\widehat{\mathsf{ID}}_2} &= \Big\{ d^0_{02} = r^0_2, d^0_{22} = \Big(h_0 h_1^{r^0_2} h_2^{f(r^0_2)}\Big)^{\frac{\alpha q(2)}{q(0)h(ID^*_2,2)+h(2)}},\\
&\qquad d^0_{i2} = \Big(h_0 h_1^{r^0_2} h_2^{f(r^0_2)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_{i2},i)+h(i)}} \ (i = 1, 3, \ldots, n)\Big\},\\
d^1_{\widehat{\mathsf{ID}}_2} &= \Big\{ d^1_{02} = r^1_2, d^1_{22} = \Big(h_0 h_1^{r^1_2} h_2^{f(r^1_2)}\Big)^{\frac{\alpha q(2)}{q(0)h(ID^*_2,2)+h(2)}},\\
&\qquad d^1_{i2} = \Big(h_0 h_1^{r^1_2} h_2^{f(r^1_2)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_{i2},i)+h(i)}} \ (i = 1, 3, \ldots, n)\Big\},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
d^0_{\widehat{\mathsf{ID}}_n} &= \Big\{ d^0_{0n} = r^0_n, d^0_{nn} = \Big(h_0 h_1^{r^0_n} h_2^{f(r^0_n)}\Big)^{\frac{\alpha q(n)}{q(0)h(ID^*_n,n)+h(n)}},\\
&\qquad d^0_{in} = \Big(h_0 h_1^{r^0_n} h_2^{f(r^0_n)}\Big)^{\frac{\alpha q(i)}{q(0)h(ID_{in},i)+h(i)}} \ (i = 1, 2, \ldots, n-1)\Big\},\\
d^1_{\widehat{\mathsf{ID}}_n} &= \Big\{ d^1_{0n} = r^1_n, d^1_{nn} = \Big(h_0 h_1^{r^1_n} h_2^{f(r^1_n)}\Big)^{\frac{\alpha q(n)}{q(0)h(ID^*_n,n)+h(n)}},\\
&\qquad d^1_{in} = \Big(h_0 h_1^{r^1_n} h_2^{f(r^1_n)}\Big)^{\frac{\alpha q(n)}{q(0)h(ID_{in},i)+h(n)}} \ (i = 1, 2, \ldots, n-1)\Big\},
\end{aligned}$$

where in d_{ij}^t, i denotes the place in the private key, j denotes the place in the identity list $(\widehat{\mathsf{ID}}_1, \widehat{\mathsf{ID}}_2, \dots, \widehat{\mathsf{ID}}_n)$, and t denotes the time the key generation query issued. $r_1^0, r_1^1, \dots, r_n^0, r_n^1$ are all randomly chosen from Z_p^*.

(b) Note $f(x) = ax + b$ is a public key, thus adversary $\mathcal{A}$ can compute

$$\begin{aligned}
d_{11}^0 &= \left(h_0 h_1^{r_1^0} h_2^{f(r_1^0)}\right)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}}, \\
&= \Big(\big(h_0 h_2^b\big)(h_1 h_2)^{a r_1^0}\Big)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}}, \\
d_{11}^1 &= \left(h_0 h_1^{r_1^1} h_2^{f(r_1^1)}\right)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}}, \\
&= \Big(\big(h_0 h_2^b\big)(h_1 h_2)^{a r_1^1}\Big)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}}.
\end{aligned}$$

Adversary $\mathcal{A}$ can then have

$$\begin{aligned}
A_1 &= \big((h_1 h_2)^a\big)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}} = \left(\frac{d_{11}^0}{d_{11}^1}\right)^{\frac{1}{r_1^0 - r_1^1}} \\
B_1 &= \big(h_0 h_2^b\big)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}} = \frac{d_{11}^0}{A_1^{r_1^0}}.
\end{aligned}$$

Similarly, adversary $\mathcal{A}$ can have

$$\begin{aligned}
A_2 &= \left(\frac{d_{22}^0}{d_{22}^1}\right)^{\frac{1}{r_2^0 - r_2^1}}, \qquad B_2 = \frac{d_{22}^0}{A_2^{r_2^0}}, \\
&\cdots\cdots\cdots \\
A_n &= \left(\frac{d_{nn}^0}{d_{nn}^1}\right)^{\frac{1}{r_n^0 - r_n^1}}, \qquad B_n = \frac{d_{nn}^0}{A_n^{r_n^0}}.
\end{aligned}$$

(c) Adversary $\mathcal{A}$ then randomly chooses $r \in Z_p^*$ and computes a valid private key for ID^*

$$\begin{aligned}
&\widetilde{d_0} = r, \widetilde{d_1} = B_1(A_1)^r = \left(h_0 h_1^r h_2^{f(r)}\right)^{\frac{\alpha q(1)}{q(0)h(ID_1^*,1)+h(1)}}, \\
&\widetilde{d_2} = B_2(A_2)^r = \left(h_0 h_1^r h_2^{f(r)}\right)^{\frac{\alpha q(2)}{q(0)h(ID_2^*,2)+h(2)}}, \dots\dots\dots, \\
&\widetilde{d_n} = B_n(A_n)^r = \left(h_0 h_1^r h_2^{f(r)}\right)^{\frac{\alpha q(n)}{q(0)h(ID_n^*,n)+h(n)}}.
\end{aligned}$$

We can verify it is a valid private key for ID^*.

Thus adversary $\mathcal{A}$ can successfully collusion attack this scheme.

4. New Fully Secure FIBE Scheme

4.1. *Construction*

1. Setup(d). The setup algorithm chooses a bilinear group G of order $N = p_1p_2p_3$(where p_1, p_2, and p_3 are distinct primes). We let G_{p_i} denote the subgroup of order p_i in G. It chooses $g \in G_{p_1}$. Define the universe, U of elements. For simplicity, we can take the first $|U|$ elements of Z_N^* to be the universe. Namely, the integers $1, \ldots, |U| \bmod N$. Choose $t_1, \ldots, t_{|u|}$ uniformly at random from Z_N. Choose y uniformly at random in Z_N. The published public parameters are:
$$T_1 = g^{t_1}, \ldots, T_{|U|} = g^{t_{|u|}}, \qquad Y = e(g, g)^y.$$
The master key is $t_1, \ldots, t_{|u|}, y$ and a generator of G_{p_3}.
2. KeyGeneration. To generate a private key for identity $w \subseteq U$ the following steps are taken. A $d - 1$ degree polynomial q is randomly chosen such that $q(0) = y$ and randomly $R_i \in G_{p_3}$ $(i = 1, \ldots, N)$ are chosen. The private key consists of components, $(D_i)_{i \in w}$, where $D_i = g^{\frac{q(i)}{t_i}} R_i$ for every $i \in w$.
3. Encryption. Encryption with the public key w' and message $M \in G_2$ proceeds as follows. First, a random value is chosen $s \in Z_p$ is chosen. The ciphertext is then published as:
$$E = \Big(w',\ E' = MY^s, \big\{E_i = T_i^s\big\}_{i \in w'}\Big).$$
Note that the identity, w', is included in the ciphertext.
4. Decryption. Suppose that a ciphertext, E, is encrypted with a key for identity w' and we have a private key for identity w, where $|w \cap w'| > d$. Choose an arbitrary d-element subset, S, of $w \cap w'$.
Then the ciphertext can be decrypted as
$$\begin{aligned}
&\frac{E'}{\prod_{i \in S} (e(D_i, E_i))^{\delta_{i,s}(0)}} \\
&\quad = \frac{E'}{\prod_{i \in S} (e(g^{\frac{q_i}{t_i}} R_i, g^{t_i s}))^{\delta_{i,s}(0)}} \\
&\quad = \frac{E'}{\prod_{i \in S} e(g, g)^{\delta_{i,s}(0) q_i s}} \\
&\quad = \frac{E'}{\prod_{i \in S} e(g, g)^{ys}} \\
&\quad = M.
\end{aligned}$$
The last equality is derived from using polynomial interpolation in the exponents. Since, the polynomial $sq(x)$ is of degree $d - 1$ it can be interpolated using d points.

4.2. *Assumptions*

In this section, we give our complex assumption. These assumptions have been used in Lewko and Waters (2010b), Lewko *et al.* (2010).

Assumption 1 (Subgroup Decision Problem). Given $(N = p_1p_2p_3, G, G_1, e)$ select randomly $g \in G_{p_1}$, $X_3 \in G_{p_3}$, $T_1 \in G_{p_1p_2}$, $T_2 \in G_{p_1}$ and set $D = (N, G, G_1, e, g, X_3)$. It is hard to distinguish T_1 from T_2. The advantage of an algorithm is defined as

$$\mathrm{Adv}_1 = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1].$$

DEFINITION 3. Assumption 1 holds if Adv_1 is negligible.

Assumption 2 Given $(N = p_1p_2p_3, G, G_1, e)$ choose randomly $g, X_1 \in G_{p_1}$, $X_2, Y_2 \in G_{p_2}$, $X_3, Y_3 \in G_{p_3}$, and set $D = (N, G, G_1, e, g, X_1X_2, X_3, Y_2Y_3)$. Then select $T_1 \in G$, $T_2 \in G_{p_1p_3}$ at random. It is hard to distinguish T_1 from T_2. The advantage of an algorithm is defined as

$$\mathrm{Adv}_2 = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1].$$

DEFINITION 4. Assumption 2 holds if Adv_2 is negligible.

Assumption 3 Given $(N = p_1p_2p_3, G, G_1, e)$, pick randomly $g \in G_{p_1}$, $X_2, Y_2, Z_2 \in G_{p_2}$, $X_3 \in G_{p_3}$, $\alpha, s \in Z_N$ and set $D = (N, G, G_1, e, g, g^{\alpha}X_2, X_3, g^sY_2, Z_2)$. Then compute $T_1 = e(g, g)^{\alpha s}$ and pick randomly $T_2 \in G_1$. It is hard to distinguish T_1 from T_2. The advantage of an algorithm is defined as

$$\mathrm{Adv}_3 = |Pr[A(D, T_1) = 1] - Pr[A(D, T_2) = 1].$$

DEFINITION 5. Assumption 3 holds if Adv_3 is negligible.

4.3. *Security Proof*

In this section, we will prove the security of the proposed scheme. We first define semi-functional keys and semi-functional ciphertexts. Let g_2 denote a generator of G_{p_2}.

Semi-functional keys. At first, a normal secret key $(\widehat{D_i})$ $(i \in w)$ is generated by using the KeyGeneration algorithm. Then some random elements γ_i $(i \in w)$ are chosen in Z_N. The semi-functional keys are set as follows:

$$D_i = \widehat{D_i}g_2^{\gamma_i}.$$

Semi-functional ciphertexts. At first, a normal ciphertext $(\widehat{w'}, \widehat{E'}, \widehat{E_i})$ is obtained using the Encrypt algorithm. Then random elements λ_i are chosen in Z_N. The semi-functional ciphertexts are set as follows:

$$w' = \widehat{w'}, \qquad E' = \widehat{E'}, \qquad E_i = \widehat{E_i}g_2^{\lambda_i}.$$

We organize our proof as a sequence of games. The first game defined will be the real fuzzy identity-based encryption game and the last one will be one in which the adversary has no advantage unconditionally. We will show that each game is indistinguishable from the next (under three complexity assumptions). We first define the games as:

Game$_{\mathrm{real}}$: This is a real FIBE security game. The next game, Game$_{\mathrm{restricated}}$, will be like the real security game except that the attacker cannot ask for keys for identities which are equal to the challenge identity modulo p_2. This is a stronger restriction than the real security game, where the identities must be unequal modulo N. We will retain this stronger restriction throughout the subsequent games. The reason for it will be explained in the proof. For $0 < i < q$, the Game$_i$ is defined as follows.

Game$_i$: Let Q denote the set of private keys which the adversary queries during the games. This game is a real FIBE security game with the two exceptions: (1) The challenge ciphertext will be a semi-functional ciphertext. (2) The first i keys will be semi-functional private keys. The rest of the keys in Q will be normal.

Note. In game$_0$, the challenge ciphertext is semi-functional. In game$_q$, the challenge ciphertexts and all keys are semi-functional.

Game$_{\mathrm{final}}$: This game is the same with game$_q$ except that the challenge ciphertext is a semi-functional encryption of random group element of G_1.

We will show that these games are indistinguishable in a set of lemmas. Let $\mathrm{Adv}_{\mathrm{game}}\mathcal{A}$ denote the advantage in the real game.

Lemma 1. *Suppose there exists an algorithm $\mathcal{A}$ such that*
$\mathrm{Game}_{\mathrm{Real}}\mathrm{Adv}_{\mathcal{A}} - \mathrm{Game}_{\mathrm{Restricated}}\mathrm{Adv}_{\mathcal{A}} = \epsilon$.
Then we can build an algorithm $\mathcal{B}$ with advantage $> \frac{\epsilon}{2}$ in breaking either Assumption 1 *or Assumption* 2*.*

Proof. Given g, X_3, $\mathcal{B}$ can simulate $\mathrm{Game}_{\mathrm{Real}}$ with $\mathcal{A}$. With probability ϵ, $\mathcal{A}$ produces identities ID and ID^* such that $\mathsf{ID} \neq \mathsf{ID}^*$ modulo N and p_2 divides $\mathsf{ID} - \mathsf{ID}^*$. $\mathcal{B}$ uses these identities to produce a nontrivial factor of N by computing $a = gcd(\mathsf{ID} - \mathsf{ID}^*, N)$. We set $b = \frac{N}{a}$. We note that p_2 divides a and $N = ab = p_1p_2p_3$. We consider two cases:

1. p_1 divides b.
2. $a = p_1p_2$ and $b = p_3$.

At least one of these cases must occur with probability $> \frac{\epsilon}{2}$. In case 1, $\mathcal{B}$ will break assumption 1. Given g, X_3, T, $\mathcal{B}$ can determine that p_1 divides b by verifying that g^b is the identity and will then test whether T^b is the identity. If it is, then $T \in G_{p_1}$. If it is not, $T \in G_{p_1p_2}$.

In case 2, $\mathcal{B}$ will break Assumption 2. Given g, X_1X_2, X_3, Y_2Y_3, B can determine that $a = p_1p_2$ by verifying that $(X_1X_2)^a$ is the identity and will then test whether $e((Y_2Y_3)^b, T)$ is the identity. If it is, then $T \in G_{p_1p_3}$. If it is not, then $T \in G$.

Lemma 2. *Suppose that there exists an algorithm $\mathcal{A}$ such that*
$\mathrm{Adv}_{\mathrm{game}_{\mathrm{Restricated}}}\mathcal{A} - \mathrm{Adv}_{\mathrm{game}_0}\mathcal{A} = \epsilon$.
Then we can build an algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 1*.*

Proof. Our algorithm $\mathcal{B}$ begins by receiving g, X_3, T where $g \in G_{p_1}$, $X_3 \in G_{p_3}$. It works as follows:

1. Setup. $\mathcal{B}$ chooses random elements $t_1, \ldots, t_{|U|}$, $y \in Z_N$ and sets $T_i = g^{t_i}$, $Y = e(g,g)^y$ for $1 < i < |U|$. It sends the public keys $PK = (T_1, \ldots, T_{|U|}$, $Y = e(g,g)^y)$ to $\mathcal{A}$.
2. Query phase 1. The adversary $\mathcal{A}$ issues a private key query for identity w. B answers as follows: A $d-1$ degree polynomial q is randomly chosen such that $q(0) = y$ and $t'_i (i \in w)$ are randomly chosen in Z_N. Then it sets
$$D_i = g^{\frac{q(i)}{t_i}} X_3^{t'_i}.$$
It is a valid simulation to $\mathcal{A}$.
3. Challenge. The adversary $\mathcal{A}$ outputs two challenge message M_0, M_1 and a challenge identity w^*. Then the ciphertext is formed as
$$w^*, \qquad E' = M_b e(T,g)^y, \qquad E_i = T^{t_i}\ (i \in w^*),$$
where $b \in \{0,1\}$.
4. Query phase 2. The adversary continues to issue queries q_j, where q_j is the following:
   - Extraction query (γ): as in phase 1 with the constraint that $|\gamma \cap w^*| < d$.
5. Guess. Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$.

If $T \in G_{p_1 p_2}$, then $(w^*, E', E_i\ (1 < i < |w^*|))$ is a semi-functional ciphertext. If $T \in G_{p_1}$, then $(w^*, E', E_i\ (1 < i < |w^*|))$ is a normal ciphertext. Hence $\mathcal{B}$ can use $\mathcal{A}$'s guess to break Assumption 1 with advantage ϵ.

Lemma 3. *Suppose there exists an algorithm $\mathcal{A}$ such that*
$\mathrm{Game}_{k-1}\mathrm{Adv}_{\mathcal{A}} - \mathrm{Game}_k\mathrm{Adv}_{\mathcal{A}} = \epsilon$.
Then we can build an algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 2.

Proof. $\mathcal{B}$ first receives $g, X_1X_2, X_3, Y_2Y_3, T$. It works as follows:

1. Setup. $\mathcal{B}$ chooses random elements $t_1, \ldots, t_{|U|}$, $y \in Z_N$ and sets $T_i = g^{t_i}$, $Y = e(g,g)^y$ for $1 < i < |U|$. It sends the public keys $PK = (T_1, \ldots, T_{|U|}, Y = e(g,g)^y)$ to $\mathcal{A}$.
2. Query phase 1.
   (a) The adversary $\mathcal{A}$ issues the ith private key query for identity w when $i < k$. $\mathcal{B}$ answers as follows: two $d-1$ degree polynomial q_1, q_2 is randomly chosen such that $q_1(0) = y$, $q_2(0) = 0$. Then it sets
$$D_i = g^{\frac{q_1(i)}{t_i}} (Y_2Y_3)^{\frac{q_2(i)}{t_i}}.$$

It is a semi-functional key to $\mathcal{A}$.

(b) The adversary $\mathcal{A}$ issues the ith private key query for identity w when $i > k$. $\mathcal{B}$ answers as follows: two $d-1$ degree polynomial q_1, q_2 is randomly chosen such that $q_1(0) = y$, $q_2(0) = 0$. Then it sets

$$D_i = g^{\frac{q_1(i)}{t_i}}(X_3)^{\frac{q_2(i)}{t_i}}.$$

It is a normal key to $\mathcal{A}$.

(c) The adversary $\mathcal{A}$ issues the ith private key query for identity w when $i = k$. $\mathcal{B}$ answers as follows: two $d-1$ degree polynomial q_1, q_2 is randomly chosen such that $q_1(0) = y$, $q_2(0) = 0$. Then it sets

$$D_i = g^{\frac{q_1(i)}{t_i}}(T)^{\frac{q_2(i)}{t_i}}.$$

3. Challenge. The adversary $\mathcal{A}$ outputs two challenge message M_0, M_1 and a challenge identity w^*. Then the ciphertext is formed as

$$w^*, \qquad E' = M_b e(X_1X_2, g)^y, \qquad E_i = (X_1X_2)^{t_i}\ (i \in w^*),$$

where $b \in \{0, 1\}$.

If $\mathcal{B}$ attempts to test itself whether key k is semi-functional by creating a semi-functional ciphertext for $w'(|S = \{w' \cap w\}| > d)$ and trying to decrypt, then decryption will work whether key k is semi-functional or not, because

$$\begin{aligned}
&\frac{E'}{\prod_{i\in S}(e(D_i, E_i))^{\delta_{i,s}(0)}} \\
&= \frac{E'}{\prod_{i\in S}(e(g^{\frac{q_1(i)}{t_i}}(T)^{\frac{q_2(i)}{t_i}}, (X_1X_2)^{t_i}))^{\delta_{i,s}(0)}} \\
&= \frac{E'}{\prod_{i\in S} e(g, g)^{\delta_{i,s}(0)q_1(i)s} e(g_2, g_2)^{\delta_{i,s}(0)q_2(i)s}} \\
&= \frac{E'}{\prod_{i\in S} e(g, g)^{ys} e(g_2, g_2)^0} \\
&= M.
\end{aligned}$$

In other words, the simulator $\mathcal{B}$ can only make a nominally semi-functional key k.

4. Query phase 2. The adversary continues to issue queries q_j, where q_j is the following:
   - Extraction query (γ): as in phase 1 with the constraint that $|\gamma \cap w^*| < d$.
5. Guess. Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins the game if $b' = b$.

If $T \in G_{p_1p_3}$, then $\mathcal{B}$ has properly simulated Game$_{k-1}$. If $T \in G$, then $\mathcal{B}$ has properly simulated Game$_k$. Hence $\mathcal{B}$ can use the output of $\mathcal{A}$ to break Assumption 2 with advantage ϵ.

Lemma 4. *Suppose there exists an algorithm $\mathcal{A}$ such that*
$\mathrm{Game}_{k-1}\mathrm{Adv}_{\mathcal{A}}-\mathrm{Game}_k\mathrm{Adv}_{\mathcal{A}} = \epsilon$.
Then we can build an algorithm $\mathcal{B}$ with advantage ϵ in breaking Assumption 3.

Proof. $\mathcal{B}$ first receives $g, g^\alpha X_2, X_3, g^s Y_2, Z_2, T$. It works as follows:

1. Setup. $\mathcal{B}$ chooses random elements $t_1, \ldots, t_{|U|}$, $y \in Z_N$ and sets $T_i = g^{t_i}$, $Y = e(g^\alpha X_2, g)$ for $1 < i < |U|$. It sends the public keys $PK = (T_1, \ldots, T_{|U|}, Y)$ to $\mathcal{A}$.
2. Query phase 1. The adversary $\mathcal{A}$ issues a private key query for identity w. B answers as follows: A $d-1$ degree polynomial q is randomly chosen such that $q(0) = y$ and t'_i $(i \in w)$ are randomly chosen in Z_N. Then it sets

   $$D_i = g^{\frac{q(i)}{t_i}} X_3^{t'_i}.$$

   It is a valid simulation to $\mathcal{A}$.
3. Challenge. The adversary $\mathcal{A}$ outputs two challenge message M_0, M_1 and a challenge identity w^*. Then the ciphertext is formed as

   $$w^*, \qquad E' = M_b T, \qquad E_i = (g^s Y_2)^{t_i} \ (i \in w^*),$$

   where $b \in \{0,1\}$.
4. Query phase 2. The adversary continues to issue queries q_j, where q_j is the following:
   - Extraction query (γ): as in phase 1 with the constraint that $|\gamma \cap w^*| < d$.
5. Guess. Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0,1\}$ and wins the game if $b' = b$.

If $T = e(g,g)^{\alpha s}$, then $(w^*, E', E_i \ (1 < i < |w^*|))$ is a semi-functional ciphertext. then this is a properly distributed semi-functional ciphertext with message M_b. If T is a random element of G_T, then this is a semi-functional ciphertext with a random message. Hence $\mathcal{B}$ can use $\mathcal{A}$'s guess to break Assumption 3 with advantage ϵ.

Theorem 1. *If Assumptions* 1, 2, *and* 3 *hold, then our FIBE system is fully IND-FID-CPA secure.*

Proof. If Assumptions 1, 2, and 3 hold, then we have shown by the previous lemmas that the real security game is indistinguishable from $\mathrm{Game}_{\mathrm{Final}}$, in which the value of b is information theoretically hidden from the attacker. Hence the attacker can attain no advantage in breaking the FIBE system.

5. Conclusion

In this paper, we analyzed Ren *et al.*'s (2010) FIBE scheme. We first show their scheme is not correct and then we give a resist collusion attack for the scheme's key generation process. At last, we propose a new fully secure FIBE scheme by using the "dual system encryption" technique (Waters, 2009) and prove its security.

Acknowledgments. The authors would like to express their gratitude thanks to the anonymous reviewer for pointing out the incorrectness of Ren *et al.*'s FIBE scheme, they also thanks Dr. Jian Weng for valuable comments. This work is supported by the National Natural Science Foundation of China under contract no. 61103230, 61003232, 61103231, Natural Science Foundation of Shaanxi Province under contract no. 2010JM8034, 2011JM8012.

References

Baek, J., Susilo, W., Zhou, J. (2007). New constructions of fuzzy identity-based encryption. In: *Proceedings of ACM Symposium on Information, Computer and Communication Security*, pp. 368–370.

Boneh, D., Boyen, X. (2004a). Efficient selective-id secure identity based encryption without random oracles. In: *Proceedings of EUROCRYPT 2004, Lecture Notes in Computer Science*, pp. 223–238.

Boneh, D., Boyen, X. (2004b). Secure identity based encryption without random oracles. In: *Proceedings of CRYPTO 2004, Lecture Notes in Computer Science*, pp. 443–459.

Boneh, D., Franklin, M. (2001). Identity based encryption from the Weil pairing. In: *Proceedings of CRYPTO 2001, Lecture Notes in Computer Science*, pp. 213–229.

Canetti, R., Halevi, S., Katz, J. (2003). A forward-secure public-key encryption scheme. In: *Proceedings of EUROCRYPT 2003, Lecture Notes in Computer Science*, pp. 255–271.

Gentry, C. (2006). Practical identity-based encryption without random oracles. In: *Proceedings of EUROCRYPT 2006, Lecture Notes in Computer Science*, pp. 445–464.

Goyal, V., Pandey, O., Sahai, A., Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In: *Proceedings of ACM Symposium on Information, Computer and Communication Security*, pp. 89–98.

Lewko, A., Waters, B. (2010). New techniques for dual system encryption and fully secure hibe with short ciphertexts. In: *Proceedings of TCC 2010, Lecture Notes in Computer Science*, pp. 455–479.

Lewko, A., Okamoto, T., Sahai, A., Takashima, K., Waters, B. (2010). Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In: *Proceedings of EUROCRYPT 2010, Lecture Notes in Computer Science*, pp. 62–91.

Pirretti, M., Traynor, P., McDaniel, P., Waters, B. (2006). Secure attribute-based systems. In: *Proceedings of ACM Symposium on Information, Computer and Communication Security*, pp. 99–112.

Ren, Y., Gu, D., Wang, S., Zhang, X. (2010). New fuzzy identity-based encryption in the standard model. *Informatica*, 21(3), 393–407.

Sahai, A., Waters, B. (2005). Fuzzy identity-based encryption. In: *Proceedings of EUROCRYPT2005, Lecture Notes in Computer Science*, pp. 457–473.

Shamir, A. (1984). Identity-based cryptosystems and signature Schemes. In: *Proceedings of CRYPTO 1984, Lecture Notes in Computer Science*, pp. 47–53.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In: *Proceedings of EUROCRYPT 2005, Lecture Notes in Computer Science*, pp. 114–127.

Waters, B. (2009). Dual system encryption: realizing fully secure ibe and hibe under simple assumptions. In: *Proceedings of CRYPTO 2009, Lecture Notes in Computer Science*, pp. 619–636.

X. Wang was born in 1981. He obtained his MS and BS degrees from the Engineering University of Chinese Armed Police Force. Now he is a senior lecturer in the same college, his main research fields are cryptography and information security.

X. Yang was born in 1959. He obtained his MS and BS degrees from the Xidian University. Now he is a professor in the Engineering University of Chinese Armed Police Force. His main research fields include cryptography, information hiding and security.

M. Zhang was born in 1969. She obtained her MS degree from the the Northwestern Polytechnical University, and her BS degree from Engineering University of Chinese Armed Police Force. Now she is a professor in the Engineering University of Chinese Armed Police Force. Her main research fields are information security and database management.

Y. Yu was born in 1981. He obtained his Phd degree from the Xidian University in 2008. Now he is an associate professor in the University of Electronic Science and Technology of China. His main research fields include cryptography and information security.

Standartinio modelio tapatumu grįstas neraiškiosios šifravimo schemos analizė

Xu An WANG, Xiaoyuan YANG, Minqing ZHANG, Yong YU

Tapatumu grįstas neraiškusis šifravimas (FIBE), kurį pasiūlė Sahai ir Waters, yra naujas tapatumu grįstas šifravimo metodas. Jis įgalina vartotoją, kurio tapatybė w, dešifruoti tekstą užšifruotą viešuoju raktu w', jei ir tik jei vartotojų identifikatoriai ID ir ID$'$ mažai skiriasi. Neseniai Ren ir kt. pasiūlė naują FIBE schemą ir tvirtino, kad ji yra visiškai saugi. Šiame straipsnyje parodyta, kad jų schema nėra gera, o jų schemos rakto generavimo procesas nėra atsparus konfliktinėms atakoms. Pasiūlyta nauja visiškai saugi FIBE schema besiremianti Sahai–Waters FIBE schema, o jos saugumas įrodytas naudojant „dvigubo šifravimo“ metodą.