INFORMATICA, 2010, Vol. 21, No. 3, 393–407

New Fuzzy Identity-Based Encryption in the Standard Model

Yanli REN[1,2], Dawu GU[1], Shuozhong WANG[2], Xinpeng ZHANG[2]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University*
Shanghai 200240, China
[2]*School of Communications and Information Engineering, Shanghai University*
Shanghai 200072, China
e-mail: renyanli1982123@yahoo.com.cn, dwgu@sjtu.edu.cn

Received: May 2009; accepted: November 2009

Abstract. In a fuzzy identity-based encryption (IBE) scheme, a user with the secret key for an identity ID is able to decrypt a ciphertext encrypted with another identity ID' if and only if ID and ID' are within a certain distance of each other as judged by some metric. Fuzzy IBE also allows to encrypt a document to all users that have a certain set of attributes. In 2005, Sahai and Waters first proposed the notion of fuzzy IBE and proved the security of their scheme under the selective-ID model. Currently, there is no fuzzy IBE scheme available that is fully CCA2 secure in the standard model. In this paper, we propose a new fuzzy IBE scheme which achieves IND-FID-CCA2 security in the standard model with a tight reduction. Moreover, the size of public parameters is independent of the number of attributes associated with an identity.

Keywords: cryptography, fuzzy identity-based encryption, IND-FID-CCA2 security, standard model.

1. Introduction

An identity-based (ID-based) cryptosystem (Shamir, 1984) is a public key cryptosystem where the public key can be represented as an arbitrary string. The user's private key is generated by a trusted authority, called a private key generator (PKG), which applies its master key to issue private keys to users based on their identities. For an identity-based encryption (IBE) scheme, a sender can securely encrypt a message to a receiver using an unambiguous identifier, such as an email address, as the public key. ID-based cryptosystems can simplify key management procedure compared to CA-based systems, so it can be an alternative way to CA-based public key systems in some occasions, especially when efficient key management and moderate security are required.

Shamir proposed the notion of IBE in 1984, then Boneh and Franklin (2003) proposed the first practical IBE scheme. Their scheme was based on bilinear maps, but it is only provably secure in the random oracle model. It has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure (Boneh and Franklin, 2004a; Canetti *et al.*, 1998). Canetti *et al.* (2003) suggested a weaker security notion for IBE, known as selective identity (selective-ID) security, relative to which they were able to build an inefficient but secure IBE scheme in the standard model (without random oracles). Boneh and Boyen (2004) presented two very efficient IBE systems ("BB1" and "BB2") with selective-ID security proofs, also in the standard model. The same authors (Boneh and Franklin, 2004b) then proposed an IBE scheme which achieves adaptive identity (adaptive-ID) security in the standard model, but the construction was impractical. Waters (2005) then proposed a much more simple extension to "BB1" also with an adaptive-ID security proof in the standard model, and its efficiency was further improved in two independent papers (Chatterjee and Sarkar, 2005; and Naccache, 2005). However, most of the IBE systems suffer from long parameters and lossy reductions. Several papers (Boneh *et al.*, 2005b; Boneh and Franklin, 2004b; Waters, 2005) have encouraged work on the problem of tight security and Waters (2005) posed the problem regarding compact public parameters. So Gentry (2006) proposed an anonymous IBE scheme that is fully secure in the standard model with short public parameters and a tight security reduction. His scheme is simple and efficient, and the proof technique differs substantially from the previous work.

The concept of fuzzy identity-based encryption (IBE) introduced by Sahai and Waters (2005) provides an error-tolerance property for IBE. Namely, in a fuzzy IBE scheme, a user with a private key for an identity ID is able to decrypt a ciphertext encrypted with an identity ID' if and only if ID and ID' are within a certain distance of each other as judged by some metric. Moreover, fuzzy IBE can be used for an application that we call "attribute-based encryption". In this application, a party will wish to encrypt a document to all users that have a certain set of attributes. For example, in a computer science department, the chairperson might want to encrypt a document to all of its systems faculty on a hiring committee. In this case it would encrypt the document to the identity "hiring-committee", "faculty", "systems". Any user who has an identity that contains all of these attributes could decrypt the document. The advantage of using fuzzy IBE schemes is that the document can be stored on a simple untrusted storage server instead of relying on trusted server to perform authentication checks before delivering a document.

In 2005, Sahai and Waters first proposed the notion of fuzzy IBE and viewed an identity as a set of descriptive attributes. Their scheme allows a private key for an identity ID to decrypt a ciphertext encrypted with an identity ID', if and only if the identity ID and ID' are close to each other as measured by the "set overlap" distance metric. They proved the security of their scheme under the selective-ID model without random oracles and claimed that their scheme was secure in the full model with an exponential factor in the reduction. Moreover, their scheme can be extended to the chosen-ciphertext model by applying the technique of using simulation-sound NIZK proofs (Sahai, 1999). Since Sahai and Water's work, fuzzy IBE has been discussed in the context of the attribute-based encryption (ABE). Goyal *et al.* (2006) proposed an ABE scheme that provides fine-grained sharing of encrypted data. Piretti *et al.* (2006) used Sahai and Waters' "large universe" construction of fuzzy IBE, which we simply call "Sahai–Waters construction", to realize their secure information management architecture. They also observed that if the random oracle (Bellare and Rogaway, 1993) is employed, computational overhead of the Sahai–Waters construction can be greatly reduced. Recently, Baek *et al.* (2007) presented new constructions of fuzzy IBE, which were more efficient than the Sahai–Waters' construction because of employing the random oracles. They also pointed out that the random oracle not only reduces computational overhead but also provides a very short public parameters whose size is independent of the number of attributes associated with an identity or the number of attributes in the defined universe, which is crucial in the storage constrained applications. However, as we claimed above, when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure.

1.1. *Our Contributions*

In the previous work, the fuzzy IBE scheme was only secure against selective-ID attacks in the random oracle model or the standard model. Though the schemes that are selective-ID secure are also fully secure as long as one hashes the identity prior to using it, the reduction is not tight. Currently, there is no fuzzy IBE available that is fully CCA2 secure in the standard model with a tight reduction. In this paper, we propose a new fuzzy IBE scheme that is fully secure in the standard model. It achieves IND-FID-CCA2 security based on the q-TBDHE assumption. Moreover, we provide the public parameters whose size is independent of the number of attributes associated with an identity. Compared to the previous fuzzy IBE schemes, our scheme has short parameters and a tight reduction simultaneously.

1.2. *Paper Outline*

The outline of the rest of this paper is organized as follows. Section 2 gives some definitions about our scheme. Then Section 3 presents our fuzzy IBE scheme in the standard model and its correctness, security and efficiency analysis are given in Section 4. Finally, we conclude the paper in Section 5.

2. Definitions

Below, we review the definition of a symmetric bilinear map and discuss the complexity assumption on which our system is based. We also review the syntax and security model for a fuzzy IBE system.

2.1. *Symmetric Bilinear Map*

Let p be a large prime number, G_1, G_2 are two groups of order p, and g is a generator of G_1. e: $G_1 \times G_1 \rightarrow G_2$ is a symmetric bilinear map, which satisfies the following properties (Boneh and Franklin, 2003, 2004a; Waters, 2005):

(1) Bilinearity: For all $u, v \in G_1$ and $a_0, b_0 \in \mathrm{Z}_p^*, e(u^{a_0}, v^{b_0}) = e(u, v)^{a_0 b_0}$.

(2) Non-degeneracy: $e(g, g) \neq 1$.

(3) Computability: $\forall u, v \in G_1$, there exists an efficient algorithm to compute $e(u, v)$.

Note that $e(\cdot)$ is symmetric since $e(g^{a_0}, g^{b_0}) = e(g,g)^{a_0 b_0} = e(g^{b_0}, g^{a_0})$. A bilinear map satisfying the three properties above is said to be a symmetric bilinear map. As shown in Boneh and Franklin (2003), such bilinear maps over cyclic groups can be obtained from the Weil or Tate pairing over supersingular elliptic curves or abelian varieties, where bilinear pairings offer an effective approach to reduce the computational cost of ID-based cryptographic schemes (Gao *et al.*, 2009; Sun *et al.*, 2010).

2.2. *Complexity Assumption*

The security of our scheme is based on a complexity assumption that we call the decisional truncated bilinear Diffie–Hellman exponent (TBDHE) assumption. It is also called wBDHI* assumption in Boneh *et al.* (2005a).

An algorithm A that outputs $k \in \{0,1\}$ has advantage of ε in solving the decision q-TBDHE if

$$\Big|\Pr\big[A(g', g, g^{\alpha}, \ldots, g^{\alpha^q}, e(g', g)^{\alpha^{q+1}}) = 0\big] \\ -\Pr\big[A(g', g, g^{\alpha}, \ldots, g^{\alpha^q}, Z) = 0\big]\Big| \geqslant \varepsilon,$$

where the probability is over the random choice of generators $g, g' \in G_1,\ \alpha \in \mathrm{Z}_p^*$, $Z \in G_2$, and the random bits consumed by A. We refer to the distribution on the left as $\mathrm{P}_{\mathrm{TBDHE}}$ and the distribution on the right as $\mathrm{R}_{\mathrm{TBDHE}}$.

We say that the decision (t, ε, q)-TBDHE assumption holds in G_1, G_2 if no t-time algorithm has advantage of at least ε in solving the decision q-TBDHE problem in G_1, G_2.

2.3. *Syntax*

The generic fuzzy IBE scheme (Sahai and Waters, 2005) consists of the following algorithms.

Setup. Taking a security parameter as input, the PKG runs this algorithm to generate its master key mk and public parameters $params$ which contain an error tolerance parameter d. Note that $params$ is given to all interested parties while mk is kept secret.

KeyGen(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}.

Encrypt$(params, \mathsf{ID}', m)$. Taking the public parameters $params$, an identity ID', and a plaintext m as input, a sender runs this algorithm to generate a ciphertext c'.

Decrypt$(params, d_{\mathsf{ID}}, c')$. Taking the public parameters $params$, a private key d_{ID} associated with an identity ID and a ciphertext c' encrypted with an identity ID' such that $|\mathsf{ID}' \cap \mathsf{ID}| \geqslant d$ as input, a receiver runs this algorithm to get a decryption, which is either a plaintext or an error message.

2.4. *Security Model*

IND-FID-CCA2 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 $c^* = \mathit{Encrypt}(\mathit{params}, \mathsf{ID}^*, m_k)$, and sends c^* to the adversary as its challenged ciphertext.

Phase 2. A executes the following queries:

(1) Key generation query $\langle \mathsf{ID} \rangle$, where $|\mathsf{ID} \cap \mathsf{ID}^*| < d$.

(2) Decryption query $\langle \mathsf{ID}, c \rangle$, where $c \neq c^*$.

These queries may be adaptive.

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

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

DEFINITION. A fuzzy IBE system is $(t, \varepsilon, q_k, q_d)$ 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.

3. New Fuzzy IBE Scheme

Assume an identity $\mathsf{ID} = (\mathsf{ID}_1, \mathsf{ID}_2, \ldots, \mathsf{ID}_n)$, where n is the length of ID and $\mathsf{ID}_i \in \mathrm{Z}_p^*$, d represents the minimal error tolerance and $n \geqslant d$. Now we wish to create a fuzzy IBE scheme in which a ciphertext created using identity ID' can be decrypted only by a private key associated with identity ID , where $|\mathsf{ID} \cap \mathsf{ID}'| \geqslant d$. We also define the Lagrange coefficient $\triangle_{i,S}$ for $i \in \mathrm{Z}_p^*$ and a set S, of elements in Z_p^*: $\triangle_{i,S}\ (x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$.

3.1. *Setup*

Let G_1, G_2, g, e be defined as Section 2.1. h: $(\mathrm{Z}_p^*)^{\{0,1\}} \times \{1, 2, \ldots, n\} \longrightarrow \mathrm{Z}_p^*$, H: $G_1^n \times G_2^l \longrightarrow \mathrm{Z}_p^*$ are collision-resistant hash functions, where $l \in \mathrm{Z}_p^*$. The PKG randomly chooses $\alpha \in \mathrm{Z}_p^*$, $h_0, h_1, h_2 \in G_1$, and two random polynomials $\mathrm{f}(x), \mathrm{q}(x) \in \mathrm{Z}_p^*[x]$ of degree 1 and $d-1$ respectively, where $\mathrm{f}(x) = ax+b$. If $h_0 = h_2^{-a}$ or $h_1 = h_2^{-b}$, randomly choose $\mathrm{f}(x)$ again. The PKG computes $g_1 = g^{\alpha},\ g_2 = g^{q(0)},\ g_3 = g_1^{q(0)}$. The public parameters are $(g, g_1, g_2, g_3, h_0, h_1, h_2, d, \mathrm{h}, \mathrm{H}, \mathrm{f}(x))$ and $\alpha, \mathrm{q}(x)$ are the private keys of PKG.

3.2. *KeyGen*

To a user U with identity $\mathsf{ID} = (\mathsf{ID_1}, \mathsf{ID_2}, \ldots, \mathsf{ID_n})$, the PKG randomly chooses $r_0 \in \mathrm{Z}_p^*$ and computes

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

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

3.3. *Encrypt*

To encrypt a message $m \in G_2$ with a key associated with identity ID', randomly choose $s \in \mathrm{Z}_p^*$ and a polynomial $\mathrm{A}(x) \in \mathrm{Z}_p^*[x]$ of degree $d-1$, compute:

$$\begin{aligned} &u_i = \left(g_2^{h(\mathsf{ID}'_i, i)} \cdot g^{h(i)}\right)^{sA(i)} \quad (i = 1, 2, \ldots, n), \qquad v_1 = e(g_3, h_1)^{sA(0)}, \\ &v_2 = e(g_3, h_2)^{sA(0)}, \qquad w = m \cdot e(g_3, h_0)^{sA(0)+\gamma}, \\ &\beta = \mathrm{H}\left(u_1, \ldots, u_n, v_1, v_2, w, m \cdot e(g_3, h_0)^{sA(0)}\right), \end{aligned}$$

where $\gamma = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)})$.

The ciphertext of message m is $c = (u_1, \ldots, u_n, v_1, v_2, w, \beta)$.

3.4. *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 $|\mathsf{ID} \cap \mathsf{ID}'| \geqslant d$. Choose an arbitrary d-element subset $S = \{i | i \in \{1, \ldots, n\}, \mathsf{ID}_i \in \mathsf{ID} \cap \mathsf{ID}'\}$ and decrypt

$$\begin{aligned} &\frac{\prod_{i \in S} e(u_i, d_i)^{\triangle_{i,S}(0)}}{v_1^{d_0} v_2^{f(d_0)}} = e(g_3, h_0)^{sA(0)}, \\ &\gamma = \mathrm{H}\left(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)}\right), \\ &w / e(g_3, h_0)^{\gamma} = R, \qquad \beta' = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, w, R), \end{aligned}$$

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

3.5. *Correctness*

The correctness of the new fuzzy IBE scheme is shown as follows. As described in Section 3.4, $\mathsf{ID}_i \in \mathsf{ID} \cap \mathsf{ID}'$ if $i \in S$. Therefore,

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

$$\begin{aligned}
\prod_{i \in S} e(u_i, d_i)^{\triangle_{i,S}(0)} &= \prod_{i \in S} e\big(g^{sA(i)}, \big(h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\alpha \cdot q(i)}\big)^{\triangle_{i,S}(0)} \\
&= e\big(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)}\big)^{\sum_{i \in S} A(i) q(i) \triangle_{i,S}(0)} \\
&= e(g_1^s, h_0 h_1^{r_0} h_2^{f(r_0)})^{A(0)q(0)} \\
&= e(g_3, h_0)^{sA(0)} e(g_3, h_1)^{sr_0 A(0)} e(g_3, h_2)^{sf(r_0)A(0)},
\end{aligned}$$

$$\frac{\prod_{i \in S} e(u_i, d_i)^{\triangle_{i,S}(0)}}{v_1^{d_0} v_2^{f(d_0)}} = e(g_3, h_0)^{sA(0)},$$

$$\gamma = \mathrm{H}\big(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{sA(0)}\big),$$

$$w / e(g_3, h_0)^{\gamma} = m \cdot e(g_3, h_0)^{sA(0)} = R,$$

$$\beta' = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, w, R) = \beta, \quad R / e(g_3, h_0)^{sA(0)} = m.$$

4. Analysis of the New Fuzzy IBE Scheme

In this section, we analyze the security of the new fuzzy IBE scheme and compare its efficiency with that of Baek *et al.* (2007) and Sahai and Waters (2005).

4.1. *Security*

We now prove that the new fuzzy IBE scheme achieves IND-FID-CCA2 security under the q-TBDHE assumption in the standard model.

Theorem 1. *Assume that the* (t', ε', q)*-TBDHE assumption holds in* G_1, G_2*, and* h, H *are collision-resistant hash functions, then our fuzzy IBE scheme is* $(t, \varepsilon, q_k, q_d)$ *IND-FID-CCA2 secure for* $t = t' - O(t_{exp} \cdot qn) - O(t_{pair} \cdot qd)$, $\varepsilon = \varepsilon' + 1/(p-1)$, $q_k + q_d \leqslant q - 1$, *where* t_{exp}, t_{pair} *are the average time required to exponentiate and pairing in* G_1, G_2 *respectively.*

Proof. Assume A is an IND-FID-CCA2 adversary described as Section 2.4, then we construct a challenger B that solves the q-TBDHE problem as follows. At first, B is given a vector $(g', g, g^{\alpha}, \ldots, g^{\alpha^q}, Z) \in G_1^{q+2} \times G_2$ to decide whether $Z = e(g', g)^{\alpha^{q+1}}$.

Setup. B randomly chooses $\mathrm{f}_0(x), \mathrm{f}_1(x), \mathrm{f}_2(x) \in \mathrm{Z}_p^*[x]$ of degree q, where $\mathrm{f}_0(x) = \sum_{i=0}^{q} a_i x^i$, $\mathrm{f}_1(x) = \sum_{i=0}^{q} b_i x^i$, $\mathrm{f}_2(x) = \sum_{i=0}^{q} c_i x^i$. Then he randomly chooses $\mathrm{q}(x) \in \mathrm{Z}_p^*[x]$ of degree $d-1$. Let

$$g_1 = g^{\alpha}, \qquad g_2 = g^{q(0)}, \qquad g_3 = g_1^{q(0)}, \qquad h_0 = g^{f_0(\alpha)},$$
$$h_1 = g^{f_1(\alpha)}, \qquad h_2 = g^{f_2(\alpha)}, \qquad \mathrm{f}(x) = -\frac{b_q}{c_q}x - \frac{a_q}{c_q}.$$

If $h_0 = h_2^{a_q/c_q}$ or $h_1 = h_2^{b_q/c_q}$, randomly choose $\mathrm{f}_0(x), \mathrm{f}_1(x), \mathrm{f}_2(x)$ again. Then B sends the parameters $(g, g_1, g_2, g_3, h_0, h_1, h_2, d, \mathrm{f}(x))$ to the adversary A. Observe that from the viewpoint of the adversary, the distribution of these public parameters is identical to the real construction since $\mathrm{f}_0(x), \mathrm{f}_1(x), \mathrm{f}_2(x), \mathrm{q}(x)$ are randomly chosen.

Phase 1. A adaptively issues the queries as follows.

Key generation query. A sends identity $\mathsf{ID} = (\mathsf{ID}_1, \mathsf{ID}_2, \dots, \mathsf{ID}_n)$ to B. B randomly chooses $r_0 \in \mathrm{Z}_p^*$ and computes

$$d_0 = r_0, d_i = \bigl(g^{\sum_{i=0}^{q-1}(a_i + r_0 b_i + f(r_0)c_i)\alpha^{i+1}}\bigr)^{\frac{q(i)}{q(0)h(\mathsf{ID}_i, i) + h(i)}} \quad (i = 1, 2, \dots, n),$$

so $d_{\mathsf{ID}} = (d_0, \dots, d_n)$. It is a valid private key, because

$$\begin{aligned}
\mathrm{f}(r_0) = -\frac{b_q}{c_q}r_0 - \frac{a_q}{c_q}, &\quad a_q + r_0 b_q + \mathrm{f}(r_0)c_q = 0,\\
g^{\sum_{i=0}^{q-1}(a_i + r_0 b_i + f(r_0)c_i)\alpha^{i+1}} &= g^{\sum_{i=0}^{q}(a_i + r_0 b_i + f(r_0)c_i)\alpha^{i+1}}\\
&= \bigl(g^{f_0(\alpha)} \cdot g^{r_0 f_1(\alpha)} \cdot g^{f(r_0)f_2(\alpha)}\bigr)^{\alpha}\\
&= \bigl(h_0 h_1^{d_0} h_2^{f(d_0)}\bigr)^{\alpha},\\
d_i = \bigl(h_0 h_1^{d_0} h_2^{f(d_0)}\bigr)^{\frac{\alpha \cdot q(i)}{q(0)h(\mathsf{ID}_i, i) + h(i)}} &\quad (i = 1, 2, \dots, n).
\end{aligned}$$

Since $\mathrm{f}_0(x), \mathrm{f}_1(x), \mathrm{f}_2(x), \mathrm{q}(x)$ are uniformly random polynomials, then h_0, h_1, h_2, r_0 are uniformly random and independent from A's view, and so the private keys issued by B are appropriately distributed.

Decryption query. A sends (ID, c) to B. B first executes the key generation query to identity ID as above, then decrypts and verifies c with the private key of ID according to the decryption process. If c can pass the verification, B sends A the plaintext; otherwise, B returns an error message.

Challenge. A sends $(\mathsf{ID}^*, m_0, m_1)$ to B, where $|\mathsf{ID} \cap \mathsf{ID}^*| < d$, and ID denotes the identity that has appeared in key generation and decryption query in Phase 1.

B randomly chooses $m_k, k \in \{0, 1\}$, a polynomial $\mathsf{A}^*(x)$ of degree $d-1$, and computes

$$u_i^* = (g')^{A^*(i)(q(0)h(\mathsf{ID}_i^*, i) + h(i))} \quad (i = 1, \dots, n),$$
$$v_1^* = Z^{b_q A^*(0)q(0)} \cdot e\bigl(g', g^{\sum_{i=0}^{q-1} b_i \alpha^{i+1}}\bigr)^{A^*(0)q(0)},$$

$$
\begin{aligned}
v_2^* &= Z^{c_q A^*(0)q(0)} \cdot e\big(g', g^{\sum_{i=0}^{q-1} c_i \alpha^{i+1}}\big)^{A^*(0)q(0)},\\
w^* &= m_k \cdot Z^{a_q A^*(0)q(0)} e\big(g', g^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}}\big)^{A^*(0)q(0)} e(g_3, h_0)^{\gamma^*},\\
\beta^* &= \mathrm{H}\big(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, w^*, w^*/e(g_3, h_0)^{\gamma^*}\big),
\end{aligned}
$$

where $\gamma^* = \mathrm{H}(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, Z^{a_q A^*(0)q(0)} \cdot e(g', g^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}})^{A^*(0)q(0)})$.

Then B sends c^* to A, where $c^* = (u_1^*, \ldots, u_n^*, v_1^*, v_2^*, w^*, \beta^*)$.

Let $s^* = \log_g g'$. If $Z = e(g', g)^{\alpha^{q+1}}$,

$$
\begin{aligned}
u_i^* &= g^{s^* A^*(i)(q(0)h(\mathsf{ID}_i^*, i) + h(i))} = \big(g_2^{h(\mathsf{ID}_i^*, i)} g^{h(i)}\big)^{s^* A^*(i)},\\
v_1^* &= e\big(g', g^{\sum_{i=0}^{q} b_i \alpha^{i+1}}\big)^{A^*(0)q(0)} = e(g_3, h_1)^{s^* A^*(0)},\\
v_2^* &= e\big(g', g^{\sum_{i=0}^{q} c_i \alpha^{i+1}}\big)^{A^*(0)q(0)} = e(g_3, h_2)^{s^* A^*(0)},\\
w^* &= m_k \cdot e\big(g', g^{\sum_{i=0}^{q} a_i \alpha^{i+1}}\big)^{A^*(0)q(0)} e(g_3, h_0)^{\gamma^*} = m_k \cdot e(g_3, h_0)^{s^* A^*(0) + \gamma^*},\\
\beta^* &= \mathrm{H}\big(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, w^*, m_k \cdot e(g_3, h_0)^{s^* A^*(0)}\big),
\end{aligned}
$$

where $\gamma^* = \mathrm{H}(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, e(g_3, h_0)^{s^* A^*(0)})$.

Therefore, c^* is a valid ciphertext for m_k under the randomness of s^*. Since $\log_g g'$ is uniformly random, s^* is uniformly random, and so c^* is a valid, appropriately-distributed challenge to A.

Phase 2. A executes the following queries:

(1) Key generation query $\langle \mathsf{ID} \rangle$, where $|\mathsf{ID} \cap \mathsf{ID}^*| < d$.

(2) Decryption query $\langle \mathsf{ID}, c \rangle$, where $c \neq c^*$.

Guess. A submits a guess $k' \in \{0, 1\}$. If $k' = k$, B outputs 0 (indicating that $Z = e(g', g)^{\alpha^{q+1}}$); otherwise, he outputs 1.

4.2. *Probability Analysis*

Lemma 1. *When Z is sampled according to P_{TBDHE}, the joint distribution of A's view and the bit k is indistinguishable from that in the actual construction, except probability* $1/(p-1)$.

Proof. When B's input is sampled from $\mathrm{P}_{\mathrm{TBDHE}}$, B's simulation appears perfect to A if A makes only key generation queries. B's simulation still appears perfect if A makes decryption queries only on identities for which it queries the private key, since B's responses do not give A any additional information. Furthermore, querying well-formed ciphertexts to the decryption oracle does not help A distinguish between the simulation and the actual construction, since, by the correctness of algorithm *Decrypt*, well-formed ciphertexts will be accepted in either case. Finally, querying a non-well-formed ciphertext for ID does not help A distinguish, since this cihertext will fail the "decrypt" check under every valid private key for ID. Thus, the lemma follows from the following claims.

Claim 1. Assuming the adversary does not find a collision in h, H, then the decryption oracle, in the simulation and in the actual construction, rejects all invalid ciphertexts under identities not queried by A.

Proof. Let $\log(\cdot)$, $\log'(\cdot)$ denote the logarithms to the base $g, e(g,g)$ respectively, and an invalid ciphertext $c = (u_1, \ldots, u_n, v_1, v_2, w, \beta)$ associated with an identity ID for

$$\begin{aligned}
&u_i = \big(g_2^{h(\mathsf{ID}_i,i)} g^{h(i)}\big)^{s_i A(i)} \quad (i = 1, 2, \ldots, n),\\
&v_1 = e(g_3, h_1)^{s_{v_1} A(0)}, \qquad v_2 = e(g_3, h_2)^{s_{v_2} A(0)},\\
&w = m \cdot e(g_3, h_0)^{s_w A(0)+\gamma}, \beta,
\end{aligned}$$

where $\gamma = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{s_w A(0)})$, and $s_i \neq s_{v_1}, s_{v_2}$ or s_w. Therefore,

$$\begin{aligned}
&\log u_i = s_i A(i)(\mathrm{q}(0)\mathrm{h}(\mathsf{ID}_i, i) + \mathrm{h}(i)) \quad (i = 1, 2, \ldots, n),\\
&\log' v_1 = s_{v_1} A(0)(\mathrm{q}(0)\alpha + \log h_1), \qquad \log' v_2 = s_{v_2} A(0)(\mathrm{q}(0)\alpha + \log h_2),\\
&\log'(w/m) = (s_w A(0) + \gamma)(\mathrm{q}(0)\alpha + \log h_0).
\end{aligned}$$

According to the *Decrypt* algorithm, a ciphertext c can be accepted if

$$\begin{aligned}
&\frac{\prod_{i \in S} e(u_i, d_i)^{\triangle_{i,S}(0)}}{v_1^{d_0} \cdot v_2^{f(d_0)}} = e(g_3, h_0)^{s_w A(0)}, \qquad w/e(g_3, h_0)^{\gamma} = R,\\
&R/e(g_3, h_0)^{s_w A(0)} = m, \qquad \beta = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, w, R),
\end{aligned} \tag{1}$$

where $d = (d_0, \ldots, d_n)$ is a private key of ID', $|\mathsf{ID} \cap \mathsf{ID}'| \geqslant d$.

According to (1),

$$\frac{\prod_{i \in S} e(u_i, d_i)^{\triangle_{i,S}(0)}}{v_1^{d_0} \cdot v_2^{f(d_0)}} = \frac{e(g^{s_i}, (h_0 h_1^{r_0} h_2^{f(r_0)})^{\alpha})^{A(0)q(0)}}{v_1^{r_0} \cdot v_2^{f(r_0)}} = e(g_3, h_0)^{s_w A(0)}. \tag{2}$$

Because A has not queried the decryption key associated with ID', and $\mathrm{f}(r_0) = -\frac{b_q}{c_q} r_0 - \frac{a_q}{c_q}$, according to (2),

$$e(g_3, h_0)^{s_w A(0)} v_2^{-\frac{a_q}{c_q}} \big(v_1 v_2^{-\frac{b_q}{c_q}}\big)^{r_0} = e\big(g^{s_i A(0) q(0)}, \ \big(h_0 h_2^{-\frac{a_q}{c_q}}\big)^{\alpha} \big(h_1 h_2^{-\frac{b_q}{c_q}}\big)^{\alpha r_0}\big)$$

Since r_0 is randomly chosen from Z_p^*, we know that

$$\begin{aligned}
&e(g_3, h_0)^{s_w A(0)} v_2^{-\frac{a_q}{c_q}} = e\big(g^{s_i A(0) q(0)}, \big(h_0 h_2^{-\frac{a_q}{c_q}}\big)^{\alpha}\big),\\
&v_1 v_2^{-\frac{b_q}{c_q}} = e\big(g^{s_i A(0) q(0)}, \ \big(h_1 h_2^{-\frac{b_q}{c_q}}\big)^{\alpha}\big).
\end{aligned} \tag{3}$$

From (3),

$$(s_w - s_i) \log h_0 - \frac{a_q}{c_q} \log h_2 (s_{v_2} - s_i) = 0,$$

$$(s_{v_1} - s_i)\log h_1 - \frac{b_q}{c_q}\log h_2(s_{v_2} - s_i) = 0. \tag{4}$$

Since $\log h_0 = \mathrm{f}_0(\alpha),\ \log h_1 = \mathrm{f}_1(\alpha),\ \log h_2 = \mathrm{f}_2(\alpha), \mathrm{f}_0(x),\ \mathrm{f}_1(x),\ \mathrm{f}_2(x)$ are randomly chosen, $\log h_0,\ \log h_1,\ \log h_2$ are uniformly random. Because $h_0 \neq h_2^{\frac{a_q}{c_q}},\ h_1 \neq h_2^{\frac{b_q}{c_q}}$, we know $s_i = s_{v_1} = s_{v_2} = s_w$ from (4).

Therefore, a ciphertext can be accepted only if it is valid. The decryption oracle, in the simulation and in the actual construction, rejects all invalid ciphertexts under identities not queried by A.

Claim 2. If the decryption oracle rejects all invalid ciphertexts, then A has advantage of $1/(p-1)$ in guessing the bit k.

When Z is sampled from $\mathrm{P}_{\mathrm{TBDHE}}$, a challenged ciphertext c^* is a valid ciphertext for the randomness of s^*.

First, we show the adversary cannot obtain a valid ciphertext $c = (u_1, \ldots, u_n, v_1, v_2, w, \beta)$ for m_k associated with ID from c^*, where

$$\begin{aligned} &u_i = \left(g_2^{h(\mathsf{ID}_i,i)} g^{h(i)}\right)^{s'A'(i)} \quad (i = 1, 2, \ldots, n),\\ &v_1 = e(g_3, h_1)^{s'A'(0)}, \qquad v_2 = e(g_3, h_2)^{s'A'(0)},\\ &w = m \cdot e(g_3, h_0)^{s'A'(0)+\gamma},\ \beta, \end{aligned}$$

where $\gamma = \mathrm{H}(u_1, \ldots, u_n, v_1, v_2, e(g_3, h_0)^{s'A'(0)})$.

There are three cases to consider:

(1) $(s', A'(x)) = (s^*, A^*(x)), \mathsf{ID} = \mathsf{ID}^*$: $c = c^*$, the ciphertext will certainly be rejected.

(2) $(s', A'(x)) = (s^*, A^*(x)), \mathsf{ID} \neq \mathsf{ID}^*$: $(v_1, v_2) = (v_1^*, v_2^*)$.

$$\begin{aligned} &u_i = u_i^* \cdot (g_2^{s^*A^*(i)})^{h(\mathsf{ID}_i,i)-h(\mathsf{ID}_i^*,i)}, \quad \gamma \neq \gamma^*,\\ &w = w^* \cdot e(g_3, h_0)^{\gamma - \gamma^*}. \end{aligned}$$

Since $s^* = \log_g g'$, and $A^*(x)$ is uniformly random, γ, γ^* are uniformly random, the adversary cannot compute a valid tuple $(\{u_i\}, w)$ from c^*.

(3) $(s', A'(x)) \neq (s^*, A^*(x))$:

$$\begin{aligned} &(u_i, v_1, v_2, \gamma) \neq (u_i^*, v_1^*, v_2^*, \gamma^*),\\ &w = w^* \cdot e(g_3, h_0)^{s'A'(0)+\gamma-s^*A^*(0)-\gamma^*}. \end{aligned}$$

Because s^* and $A^*(x)$ are uniformly random, γ, γ^* are uniformly random, the adversary cannot compute a valid w from c^*.

Therefore, the adversary cannot obtain a valid ciphertext c for m_k associated with ID from c^*. Finally, we know

$$R^* = m_k \cdot e(g_3, h_0)^{s^*A^*(0)}, \qquad w^* = m_k \cdot e(g_3, h_0)^{s^*A^*(0)+\gamma^*},$$

where $\gamma^* = \mathrm{H}(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, e(g_3, h_0)^{s^* A^*(0)})$.

Since s^* and $A^*(x)$ are uniformly random, γ^* is uniformly random, and $s^* A^*(0) + \gamma^* = 0$ with probability $1/(p-1)$, $R^*/m_k, w^*/m_k$ are uniformly random for the adversary except probability $1/(p-1)$. So A can guess $k' = k$ with probability $\frac{1}{2} + \frac{1}{p-1}$.

Lemma 2. *When Z is sampled according to R_{TBDHE}, the joint distribution of A's view and the bit k is indistinguishable from that in the actual construction.*

Proof. The lemma follows from Claim 1 and the following claim.

Claim 3. If the decryption oracle rejects all invalid ciphertexts, then A has no advantage in guessing the bit k.

When Z is sampled from $\mathrm{R}_{\mathrm{TBDHE}}$, we know that $s_{v_1}, s_{v_2} \neq s^*$. As Claim 2, the adversary cannot obtain a valid ciphertext c for m_k associated with an identity ID from c^*. We know

$$R^* = m_k \cdot Z^{a_q A^*(0) q(0)} e(g', g^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}})^{A^*(0)q(0)}, \quad w^* = R^* \cdot e(g_3, h_0)^{\gamma^*},$$

where $\gamma^* = \mathrm{H}(u_1^*, \ldots, u_n^*, v_1^*, v_2^*, Z^{a_q A^*(0)q(0)} e(g', g^{\sum_{i=0}^{q-1} a_i \alpha^{i+1}})^{A^*(0)q(0)})$.

Since s^*, $\mathsf{A}(x)$, Z are uniformly random, γ^* is uniformly random, and R^*/m_k, w^*/m_k are random for the adversary. So A can only guess $k' = k$ with probability $1/2$ and has no advantage in guessing the bit k.

Time Complexity. In the simulation, B's overhead is dominated by computing private keys and decrypting the ciphertexts in response to A's queries. Each key generation computation requires $O(n)$ exponentiations in G_1, and each decryption computation requires $O(n)$ exponentiations and $O(d)$ pairings in G_1, G_2. Since A makes at most $q-1$ queries, $t' = t + O(t_{exp} \cdot qn) + O(t_{pair} \cdot qd)$.

In the reduction, B's success probability and time complexity are the same as that of A's, except for additive factors depending on p and q respectively. So our fuzzy IBE system has a tight security reduction in the standard model. This completes the proof for Theorem 1.

4.3. *Efficiency*

In Table 1, we compare the efficiency of the known fuzzy IBE schemes.

In this table, n is the length of an identity, d represents the minimal error tolerance and "sID, full" denote "selective-ID" and "adaptive-ID" model respectively.

We conclude that our fuzzy IBE scheme has short parameters and an “adaptive-ID” security reduction in the standard model simultaneously from the table.

Table 1

Comparison among fuzzy IBE schemes

Scheme	Random oracles	Security model	Public key size	Private key size	Ciphertext size	Pairing operation
BSZ (Baek *et al.*, 2007)	yes	sID	O(1)	O(n)	O(n)	O(d)
SW (Sahai and Waters, 2005)	no	sID	O(n)	O(n)	O(n)	O(d)
Ours	no	full	O(1)	O(n)	O(n)	O(d)

5. Conclusion

Fuzzy identity-based encryption provides an error-tolerance property for IBE and can encrypt a document to all users that have a certain set of attributes. Currently, there is no fuzzy IBE scheme available that is fully CCA2 secure in the standard model. In this paper, we propose a new fuzzy IBE scheme which achieves IND-FID-CCA2 security based on the q-TBDHE assumption in the standard model. Moreover, our scheme has short public parameters and a tight reduction with an additive factor.

Acknowledgements. We would like to thank Junfeng Li and anonymous referees for their helpful comments and suggestions. The work described in this paper was supported by 863 Hi-tech Research and Development Program of China (2006AA01Z405, 2007AA01Z477), the Natural Science Foundation of China (60872116, 60832010, and 60773079), and also funded by Research Fund for the Doctoral Program of Higher Education of China (200802480019).

References

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

Bellare M., and P. Rogaway (1993). Random oracles are practical: a paradigm for designing efficient protocols. In: *Proceedings of ACM Symposium on Information, Computer and Communication Security*, pp. 62–73.

Boneh D., and M. Franklin (2003). Identity-based encryption from the weil pairing. *SIAM Journal of Computing*, 32(3), 586–615.

Boneh D., and X. Boyen (2004a). Efficient selective-ID secure identity-based encryption without random oracles. In: *Proceedings of EUROCRYPT'04*, pp. 223–238.

Boneh D., and X. Boyen (2004b). Secure identity-based encryption without random oracles. In: *Proceedings of CRYPTO'04*, pp. 443–459.

Boneh D., X. Boyen, and E.J. Goh (2005a). Hierarchical identity-based encryption with constant size ciphertext. In: *Proceedings of EUROCRYPT'05*, pp. 440–456.

Boneh, D., C. Gentry and B. Waters (2005b). Collusion-resistant broadcast encryption with short ciphertexts and private keys. In: *Proceedings of CRYPTO'05*, pp. 258–275.

Canetti R., O. Goldreich and S. Halevi (1998). The random oracle methodology, revisited (preliminary version). In: *Proceedings of ACM Symposium on Theory of Computing*, pp. 209–218.

Canetti R., S. Halevi and J. Katz (2003). A forward-secure public-key encryption scheme. In: *Proceedings of EUROCRYPT'03*, pp. 255–271.

Chatterjee S., and P. Sarkar (2005). Trading time for space: towards an efficient IBE scheme with short(er) public parameters in the standard model. In: *Proceedings of 10th International Conference on Information Security and Cryptology*, pp. 424–440.

Gao W., G. Wang, X. Wang, and Z. Yang (2009). One-round id-based threshold signature scheme from bilinear pairings. *Informatica*, 20(4), 461–476.

Gentry, C. (2006). Practical identity-based encryption without random oracles. In: *Proceedings of EUROCRYPT'06*, pp. 445–464.

Goyal, V., O. Pandey, A. Sahai and B. Waters (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.

Naccache D. (2005). Secure and practical identity-based encryption. *Cryptology ePrint Archive*, Report 2005/369. http://eprint.iacr.org/.

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

Sahai, A. (1999). Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: *Proceedings of 40 IEEE Symposium on Foundations of Computer Science*, pp. 543–553.

Sahai, A., and B. Waters (2005). Fuzzy identity-based encryption. In: *Proceedings of EUROCRYPT'05*, pp. 457–473.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. In: *Proceedings of CRYPTO'84*, pp. 47–53.

Sun X., J. Li, H. Yin, and G. Chen (2010). Delegatability of an identity based strong designated verifier signature scheme. *Informatica*, 21(1), 117–122.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In: *Proceedings of EUROCRYPT'05*, pp. 114–127.

Y. Ren is a post doctorate in School of Communication and Information Engineering at Shanghai University. She was awarded a MS degree in applied mathematics in 2005 from Shaanxi Normal University, and a PhD degree in computer science and technology in 2009 from Shanghai Jiao Tong University. Her research interests include applied cryptography, secure computing, and network security.

D. Gu is currently a full professor at Shanghai Jiao Tong University in Computer Science and Engineering Department. He was awarded a BS degree in applied mathematics in 1992, and a PhD degree in cryptography in 1998, both from Xidian University. He is a senior member of China Computer Federation and a winner of New Century Excellent Talent Program made by Ministry of Education of China. His research interests include applied cryptography, secure computing, network and system security, etc. He has got over 90 scientific papers in academic journals and conferences.

S. Wang received BS degree in 1966 from Peking University, P.R. China, and PhD degree in 1982 from University of Birmingham, England. He was with Institute of Acoustics, Chinese Academy of Sciences, from 1983 to 1985 as a research fellow. He joined Shanghai University of Technology in October 1985 as an associate professor. He is now a professor of the School of Communication and Information Engineering, Shanghai University. Professor Wang was a visiting associate scientist at Department of Electrical Engineering and Computer Science, University of Michigan, USA, from March 1993 to August 1994. His research interests include acoustics, image processing, audio processing, and information security.

X. Zhang received the BS degree in computational mathematics from Jilin University, China, in 1995, and the ME and PhD degrees in communication and information system from Shanghai University, China, in 2001 and 2004, respectively. Since 2004, he has been with the faculty of the School of Communication and Information Engineering, Shanghai University, where he is currently a professor. His research interests include multimedia security, image processing and digital forensics.

Naujas standartinio modelio neraiškusis tapatybe pagrįstas šifravimas

Yanli REN, Dawu GU, Shuozhong WANG, Xinpeng ZHANG

2005 m. Sahai ir Waters pasiūlė neraiškiąją tapatumu pagrįstą šifravimo schemą (IBE) ir įrodė, kad ši schema yra saugi. Neraiškiąją IBE schema galima užšifruoti dokumentą visiems vartotojams, kurie turi tam tikrus požymius. Straipsnyje pasiūlyta nauja neraiškioji IBE schema, kuri pasiekia IND-FID-CCA2 saugą standartiniame supaprastintame modelyje, o viešųjų parametrų skaičius nepriklauso nuo požymių susijusių su tapatybe skaičiaus.