# Full Security: Fuzzy Identity Based Encryption

Liming Fang [1*], Jiandong Wang [2], Yongjun Ren [3], Jinyue Xia [4], Shizhu Bian [5]

(1, 2, 3, 4, 5. College of Information Science and Technology,
Nanjing University of Aeronautics and Astronautics, Nanjing 210016, P.R.China)

* corresponding author

1. E-mail: fangliming@nuaa.edu.cn

**Abstract.** At EUROCRYPT 2005, Sahai and Waters presented the Fuzzy Identity Based Encryption (Fuzzy-IBE) which could be used for biometrics and attribute-based encryption in the selective-identity model. When a secure Fuzzy-IBE scheme in the selective-identity model is transformed to full identity model it exist an exponential loss of security. In this paper, we use the CPA secure Gentry's IBE (exponent inversion IBE) to construct the first Fuzzy IBE that is fully secure without random oracles. In addition, the same technique used to the modification of CCA secure Gentry's IBE which introduced by Kiltz and Vahlis to get the CCA secure Fuzzy IBE in the full-identity model.

**Keywords:** full-identity security, fuzzy identity based encryption, without random oracles.

## 1 Introduction

In an Identity Based Encryption (IBE) system any string like an e-mail address or other identifier can function as a public key. The ability that uses identities as public keys largely reduces the need for public key certificates and for certificate authorities to distribute public key certificates. This can simplify public key and certificate management in a public key infrastructure (PKI). Shamir [23] proposed the concept of IBE in 1984, and the first IBE systems were demonstrated by Boneh and Franklin [5] and Cocks [12], which could be proven secure in the random oracle model. Ever since then, a rapid development of IBE has taken place, and a series of papers [3][4][6][7][9][15][20][24] have reported progress in achieving stronger notions of security in the standard model. In 2007, Boneh et al. [2] presented a space-efficient Identity Based Encryption without pairings.

However, a unique string identifier does not necessarily exist for each person. Instead, people are more often identified by their attributes. To fulfill this task, the concept of Fuzzy-IBE recently introduced by Sahai and Waters [22] in 2005 is to provide an error-tolerance property for IBE which could be used for encryption using biometrics and attribute based encryption (ABE). Namely, in Fuzzy-IBE, a user with the secret key for the identity $\omega$ can decrypt a ciphertext encrypted with the public key $\omega'$ if $\omega$ and $\omega'$ are within a certain distance of each other. Since Sahai and Waters' first work, Fuzzy-IBE has been discussed in the context of the ABE. Instead of allowing decryption conditionally on the satisfaction of a single threshold gate (whose inputs are the matching attributes in the ciphertext and the key), Goyal et al. [16] proposed an ABE scheme that provides fine-grained sharing of encrypted data. In this model, when a user requests a private key, the authority determines what combinations of attributes must be present in order for this user to decrypt and gives the user the corresponding private key. In 2006, Piretti et al. [21] used Sahai and Waters' "large universe" construction of Fuzzy-IBE to realize their secure information management architecture. In 2007, Baek et al. [1] presented two new Fuzzy-IBE schemes in the random oracle model in which their public parameter's size is independent of the number of attributes in each identity. Recently, Chase [10] presented a scheme which allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. Boyen[6] showed the exponent inversion IBE with parallel

semantic security against selective-ID chosen-plaintext attacks, that has an appropriate linear structure, can extension to the Fuzzy IBE. But the ambiguity of Gentry's IBE as an exponent inversion candidate presents an intriguing open problem.

Recently, Fang [13] used hybrid encryption [17][18][19] with Fuzzy Identity-Based Encryption (Fuzzy-IBE) schemes and presented the first and efficient fuzzy identity-based key encapsulation mechanism (Fuzzy-IB-KEM) schemes which are CCA-secure without random oracle in the selective-identity model.

**1.1 Related Work**

To the best of our knowledge, all of the results reported in [1][10][13][16][21][22] are in the selective-ID model (Note that the selective-ID attack [3] refers to the attack in which an attacker commits ahead of time an identity that it intends to attack). It is easy to show that any selective-ID secure Fuzzy IBE is readily converted into a full-identity secure Fuzzy IBE by artificially restricting the space of identities, but the proof uses an inefficient security reduction [4]. Suppose all identities are composed of $n$ attributes and we have a universe of attributes, $u$. Sahai and Waters' scheme is secure in the full-identity model with a factor of $\binom{|u|}{n}$ in the reduction. As mentioned in [22]: "Therefore, we conjecture that a scheme that has a non-exponential loss of security in the full-identity model will require significantly different methods than those seen in prior work".

In IBE schemes, there are two major techniques to achieve IBE in the full model with non-exponential reductions. One is used in commutative blinding IBE which introduced by Boneh and Boyen [4] and later Waters [24] to devise IBE systems fully secure without random oracles, the methods achieve fully secure by essentially removing the relationships between nearby identities. Unfortunately, it is essential that there exists a relationship between nearby identities in Fuzzy-IBE. Another is introduced by Gentry [15] to get practical IBE in full-identity model, we observed that this technique can be extend to achieve a fully secure Fuzzy IBE scheme. Boyen [6] also showed exponent inversion IBE can extension to the Fuzzy IBE, they use different setup algorithm for each identity to achieve parallel IBE security, the result is the public key is different for each identity except generators. Being different as [6], our scheme have the same part of public key for each identity, so is more efficient.

**1.2 Our contributions**

In this paper, we use the CPA secure Gentry's IBE (exponent inversion IBE) to construct a Fuzzy IBE that is fully secure without random oracles and present a CPA secure scheme which gives comparable generalization performance as that of Sahai and Waters' "large universe" construction and a tightness reduction. We give a standard-model security proof reducing the intractability of decisional augmented bilinear Diffie-Hellman exponent ( $q-ABDHE$ ) problem to breaking the CPA security of our scheme in full-identity model. We remark that the proof technique is significantly different from the one used for Gentry's IBE scheme.

In addition, the same technique is used to the modification of CCA secure Gentry's IBE [15] which introduced by Kiltz and Vahlis [20] to get the CCA secure Fuzzy IBE in the full-identity model.

**1.3 Organization**

The rest of the paper is organized as follows. In Section 2, we formally define the Fuzzy Identity-Based Encryption scheme and the symmetric encryption scheme. Then, the intractability assumptions are described in Section 3, and a description of our CPA secure Fuzzy IBE follows in Section 4. In Section

5, we present a CCA secure Fuzzy IBE. We compare our schemes with known Fuzzy IBE schemes without random oracles from the literature in Section 6. Finally, we conclude in Section 7.

## 2 Preliminaries

We begin by presenting our definition of security, and then we follow with a brief review of symmetric encryption.

### 2.1 Notation

If $x$ is a string, then $|x|$ denotes its length, while if $S$ is a set then $|S|$ denotes its size. If $k \in N$ then $1^k$ denotes the string of $k$ ones. If $S$ is a set then $s \leftarrow_R S$ denotes the operation of picking an element $s$ of $S$ uniformly at random. Unless indicated specifically, algorithms are randomized and polynomial time. By $z \leftarrow_R A^{O_1, O_2 \cdots}(x, y, \cdots)$ we denote the operation of running algorithm $A$ with inputs $x, y, \cdots$ and access to oracles $O_1, O_2, \cdots$, and letting $z$ be the output. An adversary is an algorithm or a tuple of algorithms.

### 2.2 Security Model for Fuzzy Identity-Based Encryption

A Fuzzy-IBE system consists of four algorithms [22].

**Setup: Setup** establishes the PKG's parameter *pk* (public key) and *mk* (master key).

**KeyGen: KeyGen** applies the master key to an identity to generate the private key for that identity.

**Enc: Enc** uses the public key to encrypt a message to a given identity.

**Dec: Dec** decrypts a ciphertext for an identity by using a private key of that identity to get back the message.

Similar to the Fuzzy-sID-CPA game [22], a Fuzzy-full-identity-CCA game is captured by defining the following advantage function for an adversary $A = (A_1, A_2)$:

$$Adv^{CCA}_{FIBE,A}(k) \equiv \left| \Pr[Exp^{CCA}_{FIBE,A}(k) = 1] - 1/2 \right|$$

Where $Exp^{CCA}_{FIBE}(k)$ is defined by the following experiment. Identities will be element subsets of some universe $u$.

$Experiment \quad Exp^{CCA}_{FIBE}(k)$

$(pk, mk) \leftarrow_R setup(u, d, 1^k)$

$(\alpha^*, m_0, m_1, St_1) \leftarrow_R A_1^{keygen(\cdot), Dec(\cdot,\cdot)}(pk)$

$b \leftarrow_R \{0,1\}; E^* \leftarrow_R Enc(pk, \alpha^*, m_b)$

$b' \leftarrow_R A_2^{keygen(\cdot), Dec(\cdot,\cdot)}(E^*, St_1)$

If $b = b'$ Return 1 else return 0

The oracle **KeyGen($\gamma_i$)** where $|\gamma_i \cap \alpha^*| < d$ : The challenger runs KeyGen on $\gamma_i$ and forwards the resulting private key to the adversary.

The oracle **Dec($\gamma_i, E_i$)**: $A_2$ can not request a Dec query $< \gamma_i, E_i >$ where $|\gamma_i \cap \alpha^*| \geq d$ and $E_i = E^*$. Otherwise, the challenger runs KeyGen on $\gamma_i$, decrypts $E_i$ using the private key, and sends the result to the adversary.

**Definition 2.1** A Fuzzy-IBE system is $(t, q_{ID}, q_C, \varepsilon)$ Fuzzy full-identity CCA secure if all $t$-time Fuzzy-full-identity-CCA adversaries making at most $q_{ID}$ Key generation queries and at most $q_C$ chosen ciphertext queries have advantage at most $\varepsilon$ in winning the above game.

**Definition 2.2** A Fuzzy-IBE system is $(t, q_{ID}, 0, \varepsilon)$ Fuzzy-full-identity-CPA secure if all $t$-time Fuzzy-full-identity-CCA adversaries making at most $q_{ID}$ Key generation queries and no chosen ciphertext queries have advantage at most $\varepsilon$ in winning the above game.

Note that in contrast to the definition of Fuzzy slectiver-identity CPA game [22], we consider a full identity model instead of the selective-identity model, this is mean the adversary should not declare the challenge identity firstly in the full-identity model.

**2.3 Symmetric Encryption**

A symmetric encryption scheme [20] $SE = (E, D)$ is specified by its encryption algorithm $E$ (encrypting $m \in MsgSp(k)$ with key $K \in \kappa(k)$ ) and decryption algorithm $D$ (returning $m \in MsgSp(k)$ or reject). Here we restrict ourselves to deterministic algorithms $E$ and $D$.

The most common notion of security for symmetric encryption is formalized as following:

CIPHERTEXT INDISTINGUISHABILITY. Let $SE = (E, D)$ be a symmetric encryption scheme, and let $A = (A_1, A_2)$ be an adversary. We define the following experiment:

$Experiment\ Exp^{IND}_{SE,A}(k)$

$K \leftarrow_R \kappa(k)$

$(m_0, m_1, St) \leftarrow_R A_1(1^k)$

$b \leftarrow_R \{0,1\}; c^* \leftarrow_R E_K(m_b)$

$b' \leftarrow_R A_2(1^k, St, c^*)$

If $b = b'$ Return 1 else return 0

The advantage of ***A*** in breaking the ciphertext indistinguishability security of SE is:

$$Adv^{IND}_{SE,A}(k) = \left| \Pr[Exp^{IND}_{SE,A}(k) = 1] - 1/2 \right|$$

**Definition 2.3** The symmetric encryption scheme $SE$ has indistinguishable ciphertexts if for every adversary $A$ the advantage $Adv^{IND}_{SE,A}(\cdot)$ is negligible.

*CIPHERTEXT AUTHENTICITY.* In this work we are only interested in one-time authenticated schemes. These schemes are that no efficient adversary can produce a new valid ciphertext after seeing the encryption of a single message.

Let $SE = (E, D)$ be a symmetric encryption scheme, and let $A = (A_1, A_2)$ be an algorithm. We define the following experiment:

$Experiment\ Adv^{CT-IND}_{SE,A}(k)$

$K \leftarrow_R \kappa(k)$

$(m, St) \leftarrow_R A_1(1^k)$

$c \leftarrow E_K(m)$

$c' \leftarrow_R A_2(1^k, St, c)$

If $c' \neq c$ and $D_k(C') \neq \perp$ return 1 else return 0

The advantage of ***A*** in breaking the ciphertext integrity of $SE$ is:

$$Adv^{CT-IND}_{SE,A}(k) = \Pr[Exp^{CT-IND}_{SE,A}(k) = 1]$$

**Definition 2.4** The symmetric encryption scheme $SE$ has ciphertext integrity, if for every adversary ***A***, the advantage $Adv^{CT-IND}_{SE,A}(\cdot)$ is negligible.

*AUTHENTICATED ENCRYPTION.* A symmetric encryption scheme which is secure according to both

Definition 2.3 and Definition 2.4 is secure in the sense of one time authenticated encryption (of AE-OT).

*CONSTRUCTIONS.* In our IBE constructions we will require an abstract notion of algebraic symmetric encryption where the key-space $\kappa$ consists of a cyclic group $G_2$. How to build such symmetric encryption schemes satisfying all required functionality and security is well known (following the encrypt-then-mac approach) from the following basic primitives:

A (computationally secure) one-time symmetric encryption scheme with binary $\kappa$-bit keys (such as AES or padding with a PRNG)

A (computationally secure) MAC (existentially unforgeable) with $\kappa$-bit keys

A (computationally secure) key-derivation function that maps elements from $G_2$ into $2\kappa$-bit strings (such as SHA-1).

We refer the reader to previous literature [17][20] for more details.

## 3 Intractability assumptions

### 3.1 Bilinear Maps

We briefly review the facts about groups with efficiently computable bilinear maps. We refer the reader to previous literature [5] for more details. Let $G_1, G_2$ be groups of prime order $p$, and let $g$ be a generator of $G_1$. We say $G_1$ has an admissible bilinear map, $e: G_1 \times G_1 \to G_2$, into $G_2$, if the following two conditions hold.

The map is bilinear; for all $a, b$ we have $e(g^a, g^b) = e(g, g)^{ab}$.

The map is non-degenerate; we must have $e(g, g) \neq 1$.

### 3.2 The Truncated $q-ABDHE$ Assumption

Let $e: G_1 \times G_1 \to G_2$ is a bilinear map, we define the advantage function $Adv_{G_1,B}^{q-abdhe}(k)$ of an adversary ***B*** as

$$\left|\Pr[B(g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, e(g,g)^{zx^{q+1}}) = 1] - \Pr[B(g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, e(g,g)^r) = 1]\right|$$

where $x, y, z, r \leftarrow_R \mathbb{Z}_p$. We say that the truncated $q-ABDHE$ assumption relative to generator $G_1$ holds if $Adv_{G_1,B}^{q-abdhe}(k)$ is negligible for all ***B***.

## 4 CPA Secure Fuzzy IBE

In this section we present our CPA secure Fuzzy IBE scheme from the $q-ABDHE$ assumption. It is based on the exponent inversion IBE scheme [3] in its full-identity secure variant of Gentry [15].

An important security requirement for a fuzzy IBE scheme which used for biometric applications and attribute-based encryption is the security against collusion attack, which implies that no group of users should be able to combine their keys in such a way that they can decrypt a ciphertext that none of them alone could [22]. In Sahai and Waters' scheme [22], each user's keys are generated using different random sharing of a secret, so keys generated for different users cannot be combined. We use the same technique to the Gentry's CPA secure IBE, let $u \leftarrow g^x; v_1 \leftarrow e(g,g)^{y_1}$ be the public key in Gentry's scheme, $x$ is the master key; the private key for identity $id_i$ is $(s_{id_i}, d_{id_i} = g^{\frac{y_1 - s_{id_i}}{x - id_i}})$; the ciphertext for identity $id_i$ is $C_1 \leftarrow (ug^{-id_i})^r, C_2 \leftarrow g_T^r; C_3 \leftarrow (v_1)^r \cdot m$. To prevent collusion in Fuzzy IBE, a private key for a user we will associate a random $d-1$ degree polynomial, $q_1(x)$, with each user with

the restriction that each polynomial have the same valuation at point $0$, that is $q_1(0) = y_1$. The result is a user is able to perform decryption as long as he is able to match at least $d$ components of the ciphertext with their private key components. This may cause a new problem for a fuzzy identity $\omega = \{id_1, \cdots, id_I\}$, when using the same randomness $r$ to encrypt the attribute part of fuzzy identity $\omega$ : $C_{1,id_i} = (ug^{-id_i})^r; id_i \in \omega$ , the adversary can easily from two attribute part of ciphertext $C_{1,id_1} = (ug^{-id_1})^r$ $C_{1,id_2} = (ug^{-id_2})^r$ to construct a new attribute part of ciphertext $C_{1,id_3} = (ug^{-id_3})^r$ by $C_{1,id_3} = C_{1,id_1}(C_{1,id_1} / C_{1,id_2})^{(id_1 - id_3)/(id_2 - id_1)}$. To solving this problem we use the different $u_{id_i}$ for each attribute $id_i$. A description of our CPA secure Fuzzy IBE follows in below.

**4.1 The Fuzzy IBE Ⅰ**

As in [22], let $G_1$ be bilinear group of prime order $P$, and let $g$ be a generator of $G_1$. Additionally, let bilinear map $e: G_1 \times G_1 \to G_2$. We restrict the length of identities to be some fixed n. We also define the Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_P$ and a set, $S$, as elements in $\mathbb{Z}_P$ : $\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$.

Identities will be sets of $N$ elements of $\mathbb{Z}_P^*$. Let $TCR: G_1 \to \mathbb{Z}_p^*$ be a target collision-resistant hash function. Our construction follows:

$\mathrm{Setup}(u, d, 1^k)$

Parse $u$ as $\{id_1, \cdots, id_N\}$

$x_i, y_1, y_2 \leftarrow_R \mathbb{Z}_p; u_{id_i} \leftarrow g^{x_{id_i}}; v_1 \leftarrow g_T^{y_1}$

$pk \leftarrow (u_{id_1}, \cdots, u_{id_N}, v_1)$

$mk \leftarrow (x_{id_1}, \cdots, x_{id_N}, y_1)$

Return $(pk, mk)$

$\mathrm{KeyGen}(mk, \omega)$

Two $d-1$ degree polynomials $q_1(x)$ and $q_3(x)$ are randomly chosen such that $q_1(0) = y_1$.

Parse $\omega$ as $\{id_1, \cdots, id_I\}$

For $id_i \in \omega$ do $s_{1,id_i} \leftarrow q_3(id_i); d_{1,id_i} \leftarrow g^{\frac{q_1(id_i) - s_{1,id_i}}{x_{id_i} - id_i}}$

$sk_\omega \leftarrow \{(s_{1,id_i}, d_{1,id_i})_{id_i \in \omega}\}$

Return $sk_\omega$

Enc($pk, \omega', m$)

Parse $\omega'$ as $\{id_1, \cdots, id_L\}$

$r \leftarrow_R \mathbb{Z}_p ; C_{1,id_i} \leftarrow (u_{id_i} g^{-id_i})^r ; id_i \in \omega'$

$C_2 \leftarrow g_T^r ; K \leftarrow (v_1)^r ; C_3 \leftarrow m \cdot K$

$E \leftarrow (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$

Return $E$

Dec($\omega, E$)

Parse $E$ as $(\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$

Parse $\omega$ as $\{id_1, \cdots, id_I\}$

Parse $sk_\omega$ as $\{(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})_{id_i \in \omega}\}$

Randomly choose $S \subseteq \omega \cap \omega' \& |S| = d$

$$K \leftarrow \prod_{id_i \in S} (e(C_{1,id_i}, d_{1,id_i}) C_2^{s_{1,id_i}})^{\Delta_{id_i,S}(0)} ; m \leftarrow C_3 / K$$

Return $m$

We now demonstrate the accuracy of the scheme, i.e. that the $m$ computed in the encryption algorithm matches the $m$ computed in the decryption algorithm.

Correctness:

$$m = C_3 / \prod_{id_i \in S} (e(C_{1,id_i}, d_{1,id_i}) C_2^{s_{1,id_i}})^{\Delta_{id_i,S}(0)}$$

$$= C_3 / \prod_{id_i \in S} (e((u_{id_i} g^{-id_i})^r, g^{\frac{q_1(id_i) - s_{1,id_i}}{x_{id_i} - id_i}}) e(g,g)^{r s_{1,id_i}})^{\Delta_{id_i,S}(0)}$$

$$= C_3 / \prod_{id_i \in S} (e((g^{x_{id_i} - id_i})^r, g^{\frac{q_1(id_i) - s_{1,id_i}}{x_{id_i} - id_i}}) e(g,g)^{r s_{1,id_i}})^{\Delta_{id_i,S}(0)}$$

$$= C_3 / \prod_{id_i \in S} (e(g^r, g^{q_1(id_i) - s_{1,id_i}}) e(g,g)^{r s_{1,id_i}})^{\Delta_{id_i,S}(0)} = C_3 / \prod_{id_i \in S} (e(g^r, g^{q_1(id_i)}))^{\Delta_{id_i,S}(0)}$$

$$= C_3 / \prod_{id_i \in S} e(g,g)^{r q_1(id_i) \Delta_{id_i,S}(0)} = C_3 / e(g,g)^{\sum_{id_i \in S} r q_1(id_i) \Delta_{id_i,S}(0)} = C_3 / e(g,g)^{r \gamma_1} = m$$

**4.2 Security**

**Theorem 4.1** Assume $TCR$ is a target collision resistant hash function. Let $q_{ID}$ is the number of key generation queries for identity $\gamma_i$. Under the truncated $q-ABDHE$ assumption relative to generator $G_1$, the above Fuzzy IBE scheme is IND-CPA secure in the full-identity model. In particular, we have $Adv^{CPA}_{FIBE_1,t}(k) \le Adv^{q-abdhe}_{G_1,\tilde{t}}(k)$, $t = \tilde{t} - o(q \cdot q_{ID} \cdot \max_i |\gamma_i| \cdot t_{\exp})$ where $t_{\exp}$ is the time

required to exponentiate in $G_1$.

First we give some main points of intuition behind the reduction. Then we follow with a more formal proof in Appendix A.

We will show that we can reduce the $q-ABDHE$ problem to the problem of breaking our encryption scheme. That means we are given $(g, g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, T)$ and asked to distinguish $T = e(g^z, g)^{x^{q+1}}$ from a random element in $G_2$. We assume there exists an adversary that can break the security properties of our Fuzzy IBE system (as defined in Section 2) and we show that we could use such an adversary to solve this problem.

The difficult is to answer the key generation query and simulate the challenge ciphertext using $(g, g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, T)$. We picks a random degree $q$ polynomial $f_1(X)$ and defines $u = g^x$, $v_1 = e(g,g)^{f_1(x)}$. $u_{id_i} = u^{e_{id_i}} g^{id_i}$ where $e_{id_i}$ is randomly chosen from $\mathbb{Z}_p^*$.

KeyGen$(mk, \gamma)$ **for identity** $<\gamma>$ **where** $\left|\gamma \cap \alpha^*\right| < d$ **:** $\Gamma'$ can be any set such that $\Gamma' \subseteq \gamma$, $\left|\Gamma'\right| = d-1$, and $S = \Gamma' \cup \{0\}$.

1) For $id_i \in \Gamma'$ : we choose a random element $s_{1,id_i} \leftarrow_R \mathbb{Z}_p$ , and pick a random degree $q$ polynomial $f_{1,id_i}(X)$ such that $f_{1,id_i}(0) = s_{1,id_i}$, then define a degree $q-1$ polynomial $F_{1,id_i}(X) = \dfrac{f_{1,id_i}(X) - s_{1,id_i}}{X}$. Let $d_{1,id_i} \leftarrow (g^{F_{1,id_i}(x)})^{\frac{1}{e_{id_i}}}$. The intuition behind these assignments is that we are implicitly choosing two random $d-1$ degree polynomials $q_1(Y)$ and $q_3(Y)$ by choosing its value for the $d-1$ points in $\Gamma'$ randomly by setting $q_1(id_i) = f_{1,id_i}(x)$ and $q_3(id_i) = f_{1,id_i}(0) = s_{1,id_i}$ , In addition to having $q_1(0) = y_1 = f_1(x)$ and $q_3(0) = f_1(0)$.

2) We also need to calculate the decryption key values for all $id_i' \in \gamma - \Gamma'$. We calculate these points to be consistent with our implicit choice of $q_1(Y)$ and $q_3(Y)$.

**For generation of the challenge ciphertext for** $\alpha^*$, we proceed as follows. It define a $q$ degree polynomial $F^*(X) = \dfrac{X^{q+2}}{X} = X^{q+1}$ , let $r^* = zF^*(x)$ , $C_{1,id_i^*}{}^* = (g^{zx^{q+2}})^{e_{id_i^*}}$ , $C_2^* = T$ , $K^* = \prod_{id_i^* \in S} (e(C_{1,id_i^*}^*, d_{1,id_i^*}^*)(C_2^*)^{s_{1,id_i^*}^*})^{\Delta_{id_i^*,S}(0)}$, $C_3^* = M_b \cdot K^*$ where $b$ is a random bit.

We refer the reader to Appendix A for more details.

## 5 CCA Secure Fuzzy IBE

We now present an efficient Fuzzy IBE system that is full-identity CCA secure without random oracles under the truncated decision $q-ABDHE$ assumption. It is based on modification of CCA secure Gentry's IBE which introduced by Kiltz and Vahlis [20].

### 5.1 The Fuzzy IBE Ⅱ

As in [22], let $G_1$ be bilinear group of prime order $P$, and let $g$ be a generator of $G_1$. Additionally, let bilinear map $e: G_1 \times G_1 \to G_2$. We restrict the length of identities to be some fixed n. We also define the Lagrange coefficient $\Delta_{i,S}$ [22] for $i \in \mathbb{Z}_P$ and a set, $S$, as elements in $\mathbb{Z}_P: \Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. Identities will be sets of $N$ elements of $\mathbb{Z}_P^*$. Let $TCR: G_1 \to \mathbb{Z}_p^*$ be a target collision-resistant hash function. Our construction follows:

Setup$(u, d, 1^k)$

Parse $u$ as $\{id_1, \cdots, id_N\}$

$x_i, y_1, y_2 \leftarrow_R \mathbb{Z}_p$; $u_{id_i} \leftarrow g^{x_{id_i}}$; $v_1 \leftarrow g_T^{y_1}$; $v_2 \leftarrow g_T^{y_2}$

$pk \leftarrow (u_{id_1}, \cdots, u_{id_N}, v_1, v_2)$

$mk \leftarrow (x_{id_1}, \cdots, x_{id_N}, y_1, y_2)$

Return $(pk, mk)$

KeyGen$(mk, \omega)$

Four $d-1$ degree polynomials $q_1(x)$, $q_2(x)$, $q_3(x)$ and $q_4(x)$ are randomly chosen such that $q_1(0) = y_1$ and $q_2(0) = y_2$.

Parse $\omega$ as $\{id_1, \cdots, id_I\}$

For $id_i \in \omega$ do $s_{1,id_i} \leftarrow q_3(id_i)$, $s_{2,id_i} \leftarrow q_4(id_i)$

$d_{1,id_i} \leftarrow g^{\frac{q_1(id_i) - s_{1,id_i}}{x_{id_i} - id_i}}$ ; $d_{2,id_i} \leftarrow g^{\frac{q_2(id_i) - s_{2,id_i}}{x_{id_i} - id_i}}$

$sk_\omega \leftarrow \{(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})_{id_i \in \omega}\}$

Return $sk_\omega$

Enc$(pk, \omega', m)$

Parse $\omega'$ as $\{id_1, \cdots, id_L\}$

$r \leftarrow_R \mathbb{Z}_p$; $C_{1,id_i} \leftarrow (u_{id_i} g^{-id_i})^r$ $for: id_i \in \omega'$, $C_2 \leftarrow g_T^r$

$t \leftarrow TCR(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$, $K \leftarrow (v_1^t v_2)^r$, $C_3 \leftarrow E_k(m)$

$E \leftarrow (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$

Return $E$

$\mathrm{Dec}(\omega, E)$

Parse $E$ as $(\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$ where $\omega' = (id_1, \cdots, id_L)$

Parse $\omega$ as $\{id_1, \cdots, id_I\}$

Parse $sk_\omega$ as $\{(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})_{id_i \in \omega}\}$

Randomly choose $S \subseteq \omega \cap \omega' \& |S| = d$

$t \leftarrow TCR(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$

$K \leftarrow \prod_{id_i \in S} (e(C_{1,id_i}, d_{1,id_i}^t d_{2,id_i}) C_2^{s_{1,id_i} t + s_{2,id_i}})^{\Delta_{id_i,S}(0)}$

$m \leftarrow D_K(C_3)$

Return $m$

We now demonstrate the accuracy of the scheme, i.e. that the symmetric key $K$ computed in the encryption algorithm matches the key $K$ computed in the decryption algorithm.

Correctness:

$$K = \prod_{id_i \in S} (e(C_{1,id_i}, d_{1,id_i}^t d_{2,id_i}) C_2^{s_{1,id_i} t + s_{2,id_i}})^{\Delta_{id_i,S}(0)}$$

$$= \prod_{id_i \in S} (e((u_{id_i} g^{-id_i})^r, (g^{\frac{q_1(id_i) - s_{1,id_i}}{x_{id_i} - id_i}})^t g^{\frac{q_2(id_i) - s_{2,id_i}}{x_{id_i} - id_i}}) e(g,g)^{(s_{1,id_i} t + s_{2,id_i}) r})^{\Delta_{id_i,S}(0)}$$

$$= \prod_{id_i \in S} (e(g^r, (g^{q_1(id_i) - s_{1,id_i}})^t g^{q_2(id_i) - s_{2,id_i}}) e(g,g)^{(s_{1,id_i} t + s_{2,id_i}) r})^{\Delta_{id_i,S}(0)}$$

$$= \prod_{id_i \in S} (e(g^r, (g^{q_1(id_i)})^t g^{q_2(id_i)}) e(g^r, (g^{-s_{1,id_i}})^t g^{-s_{2,id_i}}) e(g,g)^{(s_{1,id_i} t + s_{2,id_i}) r})^{\Delta_{id_i,S}(0)}$$

$$= \prod_{id_i \in S} e(g^r, g^{q_1(id_i) t + q_2(id_i)})^{\Delta_{id_i,S}(0)} = e(g^r, g^{\sum_{id_i \in S} (\Delta_{id_i,S}(0) q_1(id_i) t + \Delta_{id_i,S}(0) q_2(id_i))})$$

$$= e(g^r, g^{y_1 t + y_2}) = (v_1^t v_2)^r$$

**5.2 Security**

**Theorem 5.1** Assume $TCR$ is a target collision resistant hash function and $SE = (E, D)$ is an AE-OT-secure symmetric scheme. Let $q_{ID}$ is the number of key generation queries for identity $\gamma_i$ and $q_C$ is the number of decryption queries. Under the truncated $q - ABDHE$ assumption relative to generator $G_1$, the above Fuzzy IBE scheme is IND-CCA secure in the full-identity model. In particular, we have

$$Adv^{CCA}_{FIBE_2,t}(k) \le Adv^{q-abdhe}_{G_1,\tilde{t}}(k) + Adv^{TCR}_{TCR,\tilde{t}}(k) + 2 \cdot q_C \cdot Adv^{CT-INT}_{SE,\tilde{t}}(k) + Adv^{IND}_{SE,\tilde{t}}(k) + q_C / p$$

$t = \tilde{t} - o(q \cdot q_{ID} \cdot \max_i |\gamma_i| \cdot t_{\exp})$ where $t_{\exp}$ is the time required to exponentiate in $G_1$.

The proof of Theorem 5.1 will be given in Appendix B. We give some intuition why the scheme is IND-CCA secure. The idea comes from [20]. As we can known, the proof of Gentry[15] can be used to show that consistent decryption queries (well-formed ciphertexts) for the challenge identity $\alpha^*$ are basically useless for an adversary attacking the scheme (unless it can efficiently solve the $q-ABDHE$ problem). However, inconsistent decryption queries (ill-formed ciphertexts) with respect to the challenge identity $\alpha^*$ may leak information about the hidden bit $b$. As the same argument as Cramer-Shoup, the notion of linear independence. More specifically, when one expresses the adversary's knowledge (from the public key, queries, etc.) as equations in the simulator's private key variables, one may ask whether a target equation that the adversary is trying to solve is linearly independent to the equations in its knowledge base; if so, then in certain circumstances, the adversary can be said to have an unconditionally negligible probability of finding a solution to the target equation. This will be come clearer below, the user secret-key $sk_{\alpha^*}=\{(s^*_{1,id_i^*}, d^*_{1,id_i^*}, s^*_{2,id_i^*}, d^*_{2,id_i^*})_{id_i^*\in\alpha^*}\}$ come from the internal random polynomials $q_3(Y)$ and $q_4(Y)$ that is initially hidden from the adversary's view. During the simulation of the IND-CCA environment the challenge ciphertext will leak (in an information-theoretic sense) one linear equation on the hidden random polynomials $q_3(Y)$ and $q_4(Y)$. Decryption queries of inconsistent ciphertexts will use a key $K$ for symmetric decryption that is computed as a linear equation in $q_3(Y)$ and $q_4(Y)$, which is linearly independent from the equation the adversary knows. Hence, one single key $K$ is uniformly distributed over $G_2$. By the ciphertext authenticity property of $SE$ the adversary will not be able to come up with an inconsistent ciphertext $E=(\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$ where $|\alpha^*\cap\omega'|\geq d$ such that $D_K(C_3)$ does not reject. Consequently, all inconsistent ciphertext will get rejected by the scheme.

## 6 Comparison

In this section we compare our schemes with known Fuzzy IBE schemes without random oracles from the literature.

### 6.1 Efficiency

Table1 summarizes the size of various parameters and the cost of computing sub-algorithms of the proposed fuzzy IBE schemes and the Sahai and Waters' construction[22].

$SW_1$: Sahai and Waters' simple (basic) construction.

$SW_2$ : Sahai and Waters' "large universe" construction.

$Our_1$: Our CPA secure fuzzy IBE scheme from Section 4.

$Our_2$ : Our CCA secure fuzzy IBE scheme from Section 5.

From the table 1 it is observed that our CPA secure fuzzy IBE scheme from Section 4 gives comparable generalization performance as that of Sahai and Waters' "large universe" construction at full identity model. Further, the results show that our fuzzy IBE scheme from Section 5 gives full identity CCA secure than the Sahai and Waters' construction which is selective identity CPA secure albeit to a more private key size.

| | Public key size | Ciphertext size | Private key size | Encryption cost | Decryption cost | model |
|---|---|---|---|---|---|---|
| $SW_1$ | $\|u\|\cdot\|G_1\|+\|G_2\|$ | $n\|G_1\|+\|G_2\|$ | $n\|G_1\|$ | $nT_{G_1}+T_{G_2}$ | $d\cdot T_e$ | sID |
| $SW_2$ | $(\|u\|+2)\|G_1\|$ | $(n+1)\|G_1\|+\|G_2\|$ | $2n\|G_1\|$ | $(n+1)T_{G_1}+T_{G_2}+T_e$ | $2d\cdot T_e$ | sID |
| $Our_1$ | $\|u\|\cdot\|G_1\|+\|G_2\|$ | $n\|G_1\|+2\|G_2\|$ | $n(\|G_1\|+\|\mathbb{Z}_p\|)$ | $nT_{G_1}{}'+2T_{G_2}$ | $d(T_{G_2}+T_e)$ | full |
| $Our_2$ | $\|u\|\cdot\|G_1\|+2\|G_2\|$ | $(n+1)\|G_1\|+\|G_2\|$ | $2n(\|G_1\|+\|\mathbb{Z}_p\|)$ | $nT_{G_1}{}'+T_{G_2}$ | $d(T_{G_1}{}'+T_{G_2}+T_e)$ | full |

Table1: Comparisons of Various Fuzzy IBE Schemes without random oracles. Identities will be element subsets of some universe $u$. Abbreviations: $|S|$- the bit-length of an element in set (or group) $S$; $n$-the number of elements in an identity; $T_{G_1}$ and $T_{G_2}$-the computation time for a single exponentiation in $G_1$ and $G_2$; $T_{G_1}{}'$ and $T_{G_2}{}'$-the computation time for a single multiplication in $G_1$ and $G_2$; $T_e$-the computation time for a single pairing operation; $d$-an error tolerance parameter.

**6.2 Remarks on the Tightness of the Reduction**

In the reduction, ***B***'s success probability and time complexity are the same as A's, except for additive factors $(q\cdot q_{ID}\cdot \max_i|\gamma_i|\cdot t_{\exp})$. Note that in our scheme there is no restriction that $q_{ID}+1\le q$. Due to the recent attacks by Cheon [11] it seems reasonable that the $q-ABDHE$ assumption is $\sqrt{q}$ times less secure than the BDDH assumption. So, we stress that our IBE system has a tight security reduction in the full identity model. Being compared with Sahai and Waters' scheme which is secure in the full-identity model with a factor of $\binom{|u|}{n}$ in the reduction, our scheme provides a non-exponential loss of security in the full model.

**7 Conclusions**

In this paper, we present the first and efficient CPA secure Fuzzy IBE scheme in the full identity model which gives comparable generalization performance as that of Sahai and Waters' "large universe" construction and a tightness reduction. We give a standard-model security proof reducing the intractability of decisional augmented bilinear Diffie-Hellman exponent ($q-ABDHE$) problem to breaking the CPA security of our scheme without random oracles .

In addition, the same technique used to the modification of CCA secure Gentry's IBE which introduced by Kiltz and Vahlis to get the CCA secure Fuzzy IBE in the full-identity model.

**References**

[1]. J. Baek, W. Susilo, J. Zhou, New constructions of fuzzy identity-based encryption, Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security, ACM New York, NY, USA, 2007, pp. 368-370.

[2]. D. Boneh, C. Gentry, M. Hamburg, Space-Efficient Identity Based Encryption Without Pairings, Proc. of FOCS 2007, IEEE Computer Society Washington, DC, USA, 2007, pp. 647-657.

[3]. D. Boneh, X. Boyen, Efficient selective-ID Identity based encryption without random oracles, Proc. of EUROCRYPT 2004, LNCS 3027, Springer-Verlag, 2004, pp. 223-238.

[4]. D. Boneh, X. Boyen, Secure identity based encryption without random oracles, Proc. of CRYPTO 2004, LNCS 3152, Springer-Verlag, 2004, pp. 221-238.

[5]. D. Boneh, M. K. Franklin, Identity-based encryption from the Weil pairing, Proc. of the 21st Annual International Cryptology Conference, LNCS 2139, Springer-Verlag, 2001, pp. 213-229.

[6]. X. Boyen, General Ad Hoc encryption from exponent inversion IBE, Proc. of EUROCRYPT 2007, LNCS 4515, Springer-Verlag, 2007, pp. 394-411.

[7]. X. Boyen, Q. Mei, B. Waters, Direct chosen ciphertext security from identity-based techniques, Proc. of ACM CCS 05, ACM, 2005, pp. 221-238.

[8]. R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited, In Proc. of in 30th ACM STOC, Texas, USA, May 23-26, ACM, 1998, pp. 209-218.

[9]. R. Canetti, S. Halevi, J. Katz, A forward-secure public-key encryption scheme, Proc. of EUROCRYPT 2003, LNCS 2656, Springer-Verlag, 2003, pp. 255-271.

[10]. M. Chase, Multi-authority attribute based encryption, Proc. of TCC 2007, LNCS 4392, Springer-Verlag, 2007, pp. 515-534.

[11]. J.H. Cheon, Security analysis of the strong Diffie-Hellman problem, In Proc. of EUROCRYPT 2006, LNCS 4004, Springer-Verlag, Berlin, Germany, 2006, pp. 1-11.

[12]. C. Cocks, An identity based encryption scheme based on quadratic residues, Proc. of the 8th IMA International Conference on Cryptography and Coding, LNCS 2260, 2001, pp. 360-363.

[13]. L.M. Fang, J.D. Wang, Y.J. Ren, J.Y. Xia, S.Z. Bian, Cryptology ePrint Archive: Report 2008/139, 2008 (http://eprint.iacr.org/).

[14]. E. Fujisaki, T. Okamoto, Secure integration of asymmetric and symmetric encryption schemes, Proc. of the 19th Annual International Cryptology Conference, LNCS 1666, Springer-Verlag, 1999, pp. 537-554.

[15]. C. Gentry, Practical identity-based encryption without random oracles, Proc. of EUROCRYPT 2006, LNCS 4004, Springer-Verlag, 2006, pp. 457-464.

[16]. V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, Proc. of CCS, 89-98, New York, ACM Press, 2006, pp. 221-238.

[17]. D. Hofheinz, E. Kiltz, Secure hybrid encryption from weakened key encapsulation, Proc. of CRYPTO 2007, LNCS 4622, Springer-Verlag, Berlin, Germany, August 2007, 2007, pp. 553-571.

[18]. E. Kiltz, Chosen-ciphertext secure key-encapsulation based on Gap Hashed Diffie-Hellman, Proc. of PKC 2007, LNCS 4450, Springer-Verlag, 2007, pp. 282-297.

[19]. E. Kiltz, D. Galindo, Direct chosen-ciphertext secure identity-based key encapsulation without random oracles, Proc. of ACISP 2006, LNCS 4058, Springer-Verlag. 2006, pp. 336-347.

[20]. E. Kiltz, Y. Vahlis, CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption, Proc. of CT-RSA 2008, LNCS 4964, Springer-Verlag, 2008, pp. 221-238.

[21]. M. Pirretti, P. Traynor, P. McDaniel, B. Waters, Secure Attribute-Based Systems, Proc. of ACM CCS'06, ACM, 2006, pp. 99-112.

[22]. A. Sahai, B. Waters, Fuzzy identity-based encryption, Proc. of EUROCRYPT 2005, LNCS 3494, Springer-Verlag, 2005, pp. 457-473.

[23]. A. Shamir, Identity-based cryptosystems and signature schemes, Proc. of CRYPTO 84,

Springer-Verlag, 1985, pp. 47-53.

[24]. B. Waters, Efficient identity based encryption without random oracles, Proc. of EUROCRYPT 2005, LNCS 3494, Springer-Verlag, 2005, pp. 114-127.

**A Proof of Theorem 4.1**

**Proof:** Suppose there exists a polynomial-time adversary, ***A***, that can attack our scheme in the full-ID model. We build a simulator ***B*** that can play a truncated $q-ABDHE$ game.

The simulation proceeds as follows: We first let the challenger set the groups $G_1$ and $G_2$ with an efficient bilinear map $e$ and a generator $g$ of $G_1$. Adversary ***B*** inputs a truncated $q-ABDHE$ instance $(g, g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, T)$, and has to distinguish $T = e(g^z, g)^{x^{q+1}}$ from a random element in $G_2$. We assume adversary ***A*** makes exactly $q_{ID}$ key generation queries, all with distinct identities.

**Setup:** ***B*** picks a random degree $q$ polynomial $f_1(X)$ and defines $u = g^x$, $v_1 = e(g,g)^{f_1(x)}$. $u_{id_i} = u^{e_{id_i}} g^{id_i}$ where $e_{id_i}$ is randomly chosen from $\mathbb{Z}_p^*$, using the values $g, g^x, \cdots, g^{x^q}$. Note that this does not change the distribution of the public-key $pk \leftarrow (u_{id_1}, \cdots, u_{id_N}, v_1)$. This implicitly defines the secret key values as $y_1 = f_1(x)$.

**Phase 1:** $\mathrm{KeyGen}(mk, \gamma)$ **for identity** $<\gamma>$ **where** $|\gamma \cap \alpha^*| < d$ **:**

Suppose ***A*** requests a private key $\gamma$ where $|\gamma \cap \alpha^*| < d$. Firstly, we define three sets $\Gamma', S$ in the following manner: $\Gamma'$ can be any set such that $\Gamma' \subseteq \gamma$, $|\Gamma'| = d-1$, and $S = \Gamma' \cup \{0\}$. Next, we define the decryption key components $(s_{1,id_i}, d_{1,id_i})$.

For $id_i \in \Gamma'$ as: ***B*** chooses a random elements $s_{1,id_i} \leftarrow_R \mathbb{Z}_p$, and picks a random degree $q$ polynomial $f_{1,id_i}(X)$ such that $f_{1,id_i}(0) = s_{1,id_i}$, then defines a degree $q-1$ polynomial $F_{1,id_i}(X) = \dfrac{f_{1,id_i}(X) - s_{1,id_i}}{X}$ and let $d_{1,id_i} \leftarrow (g^{F_{1,id_i}(x)})^{\frac{1}{e_{id_i}}}$.

Correctness: $d_{1,id_i} = (g^{F_{1,id_i}(x)})^{\frac{1}{e_{id_i}}} = (g^{\frac{f_{1,id_i}(x) - s_{1,id_i}}{x}})^{\frac{1}{e_{id_i}}} = g^{\frac{f_{1,id_i}(x) - s_{1,id_i}}{e_{id_i} x}} = g^{\frac{f_{1,id_i}(x) - s_{1,id_i}}{e_{id_i} x + id_i - id_i}} = g^{\frac{f_{1,id_i}(x) - s_{1,id_i}}{x_{id_i} - id_i}}$.

The intuition behind these assignments is that we are implicitly choosing two random $d-1$ degree

polynomials $q_1(Y)$ and $q_3(Y)$ by choosing its value for the $d-1$ points in $\Gamma'$ randomly by setting $q_1(id_i) = f_{1,id_i}(x)$ and $q_3(id_i) = f_{1,id_i}(0) = s_{1,id_i}$, In addition to having $q_1(0) = y_1 = f_1(x)$ and $q_3(0) = f_1(0)$.

The simulator also needs to calculate the decryption key values for all $id_i' \in \gamma - \Gamma'$. We calculate these points to be consistent with our implicit choice of $q_1(Y)$ and $q_3(Y)$.

We define a degree $q-1$ polynomial:

$$F_{1,id_i'}(X) = \frac{(f_1(X) - f_1(0))\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} (f_{1,id_i}(X) - f_{1,id_i}(0))\Delta_{id_i,S}(id_i')}{X}$$

The key components for $id_i' \in \gamma - \Gamma'$ are calculated as:

$$s_{1,id_i'} = f_1(0)\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} s_{1,id_i}\Delta_{id_i,S}(id_i') = f_1(0)\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} f_{1,id_i}(0)\Delta_{id_i,S}(id_i')$$

$$d_{1,id_i'} = (g^{F_{1,id_i'}(x)})^{\frac{1}{e_{id_i'}}}.$$

Correctness:

$$d_{1,id_i'} = (g^{F_{1,id_i'}(x)})^{\frac{1}{e_{id_i'}}} = (g^{\frac{(f_1(x) - f_1(0))\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} (f_{1,id_i}(x) - f_{1,id_i}(0))\Delta_{id_i,S}(id_i')}{x}})^{\frac{1}{e_{id_i'}}}$$

$$= (g^{\frac{\{f_1(x)\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} f_{1,id_i}(x)\Delta_{id_i,S}(id_i')\} - \{f_1(0)\Delta_{0,S}(id_i') + \sum_{id_i \in \Gamma'} f_{1,id_i}(0)\Delta_{id_i,S}(id_i')\}}{x}})^{\frac{1}{e_{id_i'}}}$$

$$= (g^{\frac{f_{1,id_i'}(x) - s_{1,id_i'}}{x}})^{\frac{1}{e_{id_i'}}} = g^{\frac{f_{1,id_i'}(x) - s_{1,id_i'}}{e_{id_i'} \cdot x}} = g^{\frac{f_{1,id_i}(x) - s_{1,id_i'}}{e_{id_i'} \cdot x + id_i' - id_i'}} = g^{\frac{f_{1,id_i'}(x) - s_{1,id_i'}}{x_{id_i'} - id_i'}}$$

Therefore, the simulator is able to construct a private key for the identity $\gamma$. Furthermore, the distribution of the private key for $\gamma$ is identical to that of original scheme since our choices of $q_1(id_i) = f_{1,id_i}(x)$ and $q_3(id_i) = f_{1,id_i}(0) = s_{1,id_i}$ induce two random $d-1$ degree polynomials $q_1(Y)$ and $q_3(Y)$ and our construction of the private key components $(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})$.

**Challenge:** ***A*** outputs challenge identity $\alpha^*$ and two messages $m_0$ and $m_1$, ***B*** generates a random bit $b \in \{0,1\}$. For generation of the challenge ciphertext for $\alpha^*$, ***B*** proceeds as follows. Parse

$\alpha^*$ as $\{id_1^*, \cdots, id_J^*\}$ .The experiment first internally generates a random instance of the user secret key $sk_{\alpha^*} = \{(s^*_{1,id_i^*}, d^*_{1,id_i^*})_{id_i^* \in \alpha^*}\} \leftarrow_R \text{KeyGen}(mk, \alpha^*)$.

It define a $q$ degree polynomial $F^*(X) = \dfrac{X^{q+2}}{X} = X^{q+1}$, let $r^* = zF^*(x)$, $C_{1,id_i^*}{}^* = (g^{zx^{q+2}})^{e_{id_i^*}}$ $C_2^* \leftarrow T$ , The symmetric key $K^*$ is then computed as in decryption as: $K^* = \prod_{id_i^* \in S} (e(C^*_{1,id_i^*}, d^*_{1,id_i^*})(C_2^*)^{s^*_{1,id_i^*}})^{\Delta_{id_i^*,S}(0)}$ where $t^* \leftarrow TCR(C^*_{1,id_1^*}, \cdots, C^*_{1,id_J^*}, C_2^*)$ . Finally, $C_3^*$ is computed as $C_3^* \leftarrow m_b \cdot K^*$ and $b$ is a random bit.

Return the ciphertext $E^* = (\alpha^*, C^*_{1,id_1^*}, \cdots, C^*_{1,id^*_{|\alpha^*|}}, C_2^*, C_3^*)$.

Correctness:

$$C^*_{1,id_i^*} = (u_{id_i^*} g^{-id_i^*})^{zF^*(x)} = (g^{e_{id_i^*}x + id_i^* - id_i^*})^{zF^*(x)} = (g^{e_{id_i^*}x})^{zF^*(x)} = ((g^x)^{z\frac{x^{q+2}}{x}})^{e_{id_i^*}} = (g^{zx^{q+2}})^{e_{id_i^*}}$$

$$C_2^* \leftarrow g_T^{r^*} = e(g,g)^{zF^*(x)} = e(g,g)^{z\frac{x^{q+2}}{x}} = e(g,g)^{zx^{q+1}} = T$$

Note that the challenge ciphertext can be entirely computed from ***B***'s input values from $(g, g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, T)$.

**Phase 2:** ***A*** makes key generation queries, and ***B*** responds as in Phase 1.

**Guess:** Finally, the adversary outputs a bit $b'$, ***B*** outputs 1 if $b = b'$ and 0, otherwise.

**B Proof of Theorem 5.1**

***A*** be an adversary on the IND-CCA security of Fuzzy IBE in the full identity model. We will consider a sequence of games, Game 1, Game 2, $\cdots$, each game involving ***A***. Let $X_i$ be the event that the adversary succeeds in Game i, it holds that $b = b'$.

Let $\text{Dec}(\omega, E)$ is a decryption query, Parse $E$ as $(\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)$ where $\omega' = (id_1, \cdots, id_L)$, parse $\omega$ as $\{id_1, \cdots, id_I\}$, parse $sk_\omega$ as $\{(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})_{id_i \in \omega}\}$. $S \subseteq \omega \cap \omega' \& |S| = d$ is randomly chosen for decryption. For a tuple $(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$, we consider $r_{1,id_i} = \log_{u_{id_i} g^{-id_i}} C_{1,id_i}$ , $r_2 = \log_{g_T} C_2$ , where $t \leftarrow TCR(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ . We

say $(C_{1,id_1},\cdots,C_{1,id_L},C_2)$ relative to $S$ is consistent where $S\subseteq\omega\,\&\,|S|=d$ if $\{r_{1,id_i}=r_2\}_{id_i\in S}$ and inconsistent otherwise.

We assume adversary ***A*** makes exactly $q_{ID}$ key generation queries, all with distinct identities.

We further assume that ***A*** makes exactly $q_C$ decryption queries $\mathrm{Dec}(\omega,E)$.

**Game1.** Let Game1 be the CCA security experiment run with adversary ***A***. Our goal is to put an upper bound on $Adv^{CCA}_{Fuzzy-IBE,A,t}(k)\equiv\left|\Pr[X_1]-\frac{1}{2}\right|$

**Game 2**. We now change the generation of the challenge ciphertext $<\alpha^*,E^*>$ as follows. Parse $\alpha^*$ as $\{id_1^*,\cdots,id_J^*\}$ where $J=|\alpha^*|$. The experiment first internally generates a random instance of the user secret key $sk_{\alpha^*}=\{(s^*_{1,id_i^*},d^*_{1,id_i^*},s^*_{2,id_i^*},d^*_{2,id_i^*})_{id_i^*\in\alpha^*}\}\leftarrow_R \mathrm{KeyGen}(mk,\alpha^*)$. Then it picks a random $r_1\in\mathbb{Z}_p$ and for $id_i^*\in\alpha^*$ computes

$$C^*_{1,id_i^*}\leftarrow(u_{id_i^*}g^{-id_i^*})^{r_1};C_2^*\leftarrow e(g,g)^{r_1}. \qquad (1)$$

The symmetric key $K^*$ is then computed as in decryption as:

$$K^*=\prod_{id_i^*\in S}(e(C^*_{1,id_i^*},(d^*_{1,id_i^*})^{t^*}d^*_{2,id_i^*})(C_2^*)^{s^*_{1,id_i^*}t^*+s^*_{2,id_i^*}})^{\Delta_{id_i^*,S}(0)} \qquad (2)$$

where $t^*\leftarrow TCR(C^*_{1,id_1^*},\cdots,C^*_{1,id_J^*},C_2^*)$. Finally, $C_3^*$ is computed as $C_3^*\leftarrow E_{k^*}(m_b)$. Since this change is purely conceptual,

$$\Pr[X_2]=\Pr[X_1].$$

**Game 3.** In this game the experiment stops if the adversary queries the challenge ciphertext in the first phase. Since $C_2^*$ is generated as $C_2^*\leftarrow e(g,g)^{r_1}$, independently from ***A***'s view until it sees the challenge ciphertext, we have

$$|\Pr[X_3]-\Pr[X_2]|\le q_C/p$$

**Game 4.** For generation of the challenge ciphertext the experiment proceeds as follows. The experiment now generates $C_2^*$ from Equation (1) by picking $r_2\in\mathbb{Z}_p/\{r_1\}$ and computing $C_2^*\leftarrow e(g,g)^{r_2}$.

**Lemma B.1** $|\Pr[X_3]-\Pr[X_4]|\le Adv^{q-abdhe}_{G,\tilde{t}}(k)$

**Proof:** We show that there exists an adversary ***B*** with $t_B \approx t_A$ such that $Adv_{G,\tilde{t}}^{q-abdhe}(k) = \left|\Pr[X_2] - \Pr[X_4]\right|$. Adversary ***B*** inputs a truncated $q-ABDHE$ instance

$$(g, g^x, \cdots, g^{x^q}, g^z, g^{zx^{q+2}}, T), \quad (3)$$

and has to distinguish $T = e(g^z, g)^{x^{q+1}}$ from a random element in $G_2$. For key generation ***B*** picks two random degree $q$ polynomial $f_1(X)$ , $f_2(X)$ and defines

$$u = g^x, u_{id_i} = u^{e_{id_i}} g^{id_i}, v_1 = e(g,g)^{f_1(x)}, v_2 = e(g,g)^{f_2(x)}$$

Using the values $g, g^x, \cdots, g^{x^q}$ from Equation (3). Note that this does not change the distribution of the public-key $pk \leftarrow (u_{id_1}, \cdots, u_{id_N}, v_1, v_2)$. This implicitly defines the secret key values as $y_1 = f_1(x)$ and $y_2 = f_2(x)$.

$\mathrm{KeyGen}(mk, \gamma)$ **for identity** $\gamma$ **where** $\left|\gamma \cap \alpha^*\right| < d$ **:**

We generate the private key components $(s_{1,id_i}, d_{1,id_i})$ correctly as the same as the CPA game, using the same technique we also get the private key components $(s_{2,id_i}, d_{2,id_i})$. So, using the values $g, g^x, \cdots, g^{x^q}$ from Equation (3), we can construction of the private key components $(s_{1,id_i}, d_{1,id_i}, s_{2,id_i}, d_{2,id_i})$ where $id_i \in \gamma$.

**For generation of the challenge ciphertext for** $\alpha^*$ : B proceeds as follows. It defines the $q$ degree polynomial

$$F^*(X) = \frac{X^{q+2}}{X} = X^{q+1}, \text{ let } r^* = zF^*(x), \; C_{1,id_i^*}{}^* = (g^{zx^{q+2}})^{e_{id_i^*}}$$

$$C_2^* \leftarrow T, C_3^* \leftarrow_R E_{K^*}(M_b),$$

where the challenge key $K^*$ is computed from $C_2^*, C_3^*$ as in Equation (2) and $b$ is a random bit.

$E^* = (\alpha^*, C_{1,id_1^*}^*, \cdots, C_{1,id_{|\alpha^*|}^*}^*, C_2^*, C_3^*)$; Return $E^*$.

Correctness:

$$C_{1,id_i^*}^* = (u_{id_i^*} g^{-id_i^*})^{zF^*(x)} = (g^{e_{id_i^*}x + id_i^* - id_i^*})^{zF^*(x)} = (g^{e_{id_i^*}x})^{zF^*(x)} = ((g^x)^{z\frac{x^{q+2}}{x}})^{e_{id_i^*}} = (g^{zx^{q+2}})^{e_{id_i^*}}$$

$C_2^* \leftarrow g_T^{r^*} = e(g,g)^{zF^*(x)} = e(g,g)^{z\frac{x^{q+2}}{x}} = e(g,g)^{zx^{q+1}} = T$

Note that the challenge ciphertext can be entirely computed from ***B***'s input values from Equation (3). Adversary ***B*** runs $A_2$ on input $(E^*, St)$, answering all oracle queries as above, and inputting a bit $b'$, Finally, ***B*** outputs1 if $b = b'$ and 0, otherwise.

We make the following claim that completes the proof of the lemma: if $T = e(g^z, g)^{x^{q+1}}$ then ***A***'s view is the same as in Game 2. If $T \in G_2$, then ***A***'s view is the same as in Game 4.

To prove the claim we have to consider the distribution of the challenge ciphertext in Games 2 and 4. Note that the element $T \in G_2$ only leaks through ***B***'s simulation in the element $C_2^*$ from the challenge as ciphertext. We write $C_{1,id_i^*}^*$:

$C_{1,id_i^*}^* = (g^{zx^{q+2}})^{e_{id_i^*}} = (g^{e_{id_i^*}x})^{zF^*(x)} = (g^{e_{id_i^*}x + id_i^* - id_i^*})^{zF^*(x)} = (u_{id_i^*} g^{-id_i^*})^{zF^*(x)} = (u_{id_i^*} g^{-id_i^*})^{r_1}$, for $r_1 = zF^*(x)$. If $T = e(g^z, g)^{x^{q+1}}$, then

$C_2^* = T = e(g,g)^{zx^{q+1}} = e(g,g)^{zF^*(x)} = e(g,g)^{r_1}$.

**Game 5.** Let $E^* = (\alpha^*, C_{1,id_1^*}^*, \cdots, C_{1,id_J^*}^*, C_2^*, C_3^*)$ be the challenge ciphertext for $\alpha^*$ and let $t^* \leftarrow TCR(C_{1,id_1^*}^*, \cdots, C_{1,id_J^*}^*, C_2^*)$. In this game the experiment changes the answers to the decryption oracle as follows. If, for a decryption query $\mathrm{Dec}(\omega, E)$ where $E = (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3); L = |\omega'|$ it holds that $(C_{1,id_1^*}^*, \cdots, C_{1,id_J^*}^*, C_2^*) \neq (C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ but $TCR(C_{1,id_1^*}^*, \cdots, C_{1,id_J^*}^*, C_2^*) = t^* = t = TCR(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ then the experiment aborts. We claim that there exists an adversary ***F*** with $t_F \approx t_A$ such that

$$\left|\Pr[X_5] - \Pr[X_4]\right| \leq Adv_{TCR,F}^{TCR}(k)$$

**Game 6.** Game 6 is like Game 5 with the difference that all decryption queries $\mathrm{Dec}(\alpha^*, E = (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3))$ for which $(C_{id_1,1}, \cdots, C_{id_L,1}, C_2)$ relative to $S$ is inconsistent where $S \subseteq \omega \cap \alpha^* \,\&\, |S| = d$ is randomly chosen get rejected.

**Lemma B.2** $\left|\Pr[X_6] - \Pr[X_5]\right| \leq q_C Adv_{SE,\tilde{t}}^{IND}(k)$

**Proof:** Let $sk_{\alpha^*} = \{(s^*_{1,id_i^*}, d^*_{1,id_i^*}, s^*_{2,id_i^*}, d^*_{2,id_i^*})_{id_i^* \in \alpha^*}\}$ be the uniquely defined and fixed user secret-key for $\alpha^*$. We first claim that in the view of adversary *A*, one single decryption query $<\alpha^*, E = (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)>$ for which $(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ is inconsistent relative to $S$ where $S \subseteq \omega' \cap \alpha^* \,\&\, |S| = d$ yields a uniform symmetric key $K \in G_2$. We say $(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ relative to $S$ is consistent if $\{r_{1,id_i} = r_2\}_{id_i \in S}$ and inconsistent otherwise. The consequence is as follows. In Game 5 the decryption oracle returns $\perp$ (reject) if $D_K(C_3) = \perp$. Since $K$ is uniform in $G_2$, this happens exactly with probability $\Pr_{K' \leftarrow_R G_2}[D_{K'}(C_3) = \perp]$ which equals the advantage of a suitable adversary in the ciphertext integrity experiment of the symmetric ciphertext $SE$. On the other hand, in Game 6 such a query gets always rejected. A standard argument [20]shows that considering all $q_C$ decryption queries one obtains

$$\left|\Pr[X_6] - \Pr[X_5]\right| \le q_C Adv^{CT-INT}_{SE,\tilde{t}}(k)$$

To prove the above claim, consider the hidden random polynomials $q_3(Y)$ and $q_4(Y)$ for generating the user secret key $sk_{\alpha^*} = \{(s^*_{1,id_i^*}, d^*_{1,id_i^*}, s^*_{2,id_i^*}, d^*_{2,id_i^*})_{id_i^* \in \alpha^*}\}$ that is used by the experiment when generating the challenge ciphertext. Consider the symmetric key $K^*$ which is obtained from the inconsistent challenge ciphertext ( $C^*_{1,id_i^*} = (u_{id_i^*} g^{-id_i^*})^{r_1^*}$ , $C^*_2 = e(g,g)^{r_2^*}$ ) by computing

$$K^* = \prod_{id_i^* \in S} (e(C^*_{1,id_i^*}, (d^*_{1,id_i^*})^{t^*} d^*_{2,id_i^*})(C^*_2)^{s^*_{1,id_i^*} t^* + s^*_{2,id_i^*}})^{\Delta_{id_i^*,S}(0)}$$

$$= e(g,g)^{r_1^*(y_1 t^* + y_2) + \sum_{id_i^* \in S} (\Delta_{id_i^*,S}(0)(r_2^* - r_1^*)(q_3(id_i^*)t^* + q_4(id_i^*)))}$$

$$= e(g,g)^{r_1^*(y_1 t^* + y_2) + (r_2^* - r_1^*)(q_3(0)t^* + q_4(0))}$$

Let $l^* = q_3(0)t^* + q_4(0)$ , $q_3(Y) = q_{3,0} + q_{3,1}Y + \cdots + q_{3,d-1}Y^{d-1}$ , $q_4(Y) = q_{4,0} + q_{4,1}Y + \cdots + q_{4,d-1}Y^{d-1}$.

Now consider the virtual key $K$ that is computed from a ciphertext $<\alpha^*, E = (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, C_3)>$ of a decapsulation query such that $(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ relative to $S$ is inconsistent with $\alpha^*$. We claim that in the view of ***A***, $K$ is a uniform element in $G_2$.

$$K = \prod_{id_i^* \in S} (e(C_{1,id_i^*}, (d_{1,id_i^*}^*)^t d_{2,id_i^*}^*)(C_2)^{s_{1,id_i^*}^* t + s_{2,id_i^*}^*})^{\Delta_{id_i^*,S}(0)}$$

$$= e(g,g)^{r_1^*(y_1 t + y_2) + \sum_{id_i^* \in S} (\Delta_{id_i^*,S}(0)(r_2^* - r_1^*)(q_3(id_i^*)t + q_4(id_i^*)))}$$

$$= \prod_{id_i^* \in S} (e(g^{r_{1,id_i^*}}, (g^{q_1(id_i^*) - s_{1,id_i^*}^*})^t g^{q_2(id_i^*) - s_{2,id_i^*}^*}) e(g,g)^{(s_{1,id_i^*}^* t + s_{2,id_i^*}^*) r_2})^{\Delta_{id_i^*,S}(0)}$$

$$= e(g,g)^{\sum_{id_i^* \in S} (\Delta_{id_i^*,S}(0) r_{1,id_i^*}(q_1(id_i^*)t + q_2(id_i^*))) + \sum_{id_i^* \in S} (\Delta_{id_i^*,S}(0)(r_2 - r_{1,id_i^*})(q_3(id_i^*)t + q_4(id_i^*)))}$$

Let $l = \sum_{id_i^* \in S} b_{id_i^*}(q_3(id_i^*)t + q_4(id_i^*)))$ where $b_{id_i^*} = \Delta_{id_i^*,S}(0)(r_2 - r_{1,id_i^*})$.

**Claim B.1** $l$ is linearly independent to the equation $l^*$ in adversary ***A***'s knowledge base.

**Proof:** Let $l^* = q_3(0)t^* + q_4(0) = q_{3,0}t^* + q_{4,0}$, we have $q_{4,0} = l^* - q_{3,0}t^*$, so

$$l = \sum_{id_i^* \in S} (b_{id_i^*}((q_{3,0} + q_{3,1}(id_i^*) + \cdots + q_{3,d-1}(id_i^*)^{d-1})t + q_{4,0} + q_{4,1}(id_i^*) + \cdots + q_{4,d-1}(id_i^*)^{d-1}))$$

$$= \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^0(q_{3,0}t + q_{4,0})) + \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^1(q_{3,1}t + q_{4,0})) + \cdots + \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^{d-1}(q_{3,d-1}t + q_{4,d-1}))$$

$$= \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^0(q_{3,0}t + l^* - q_{3,0}t^*)) + \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^1(q_{3,1}t + q_{4,0})) + \cdots$$

$$+ \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^{d-1}(q_{3,d-1}t + q_{4,d-1}))$$

$$= \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^0 l^*) + \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^0 q_{3,0}(t - t^*)) + \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^1(q_{3,1}t + q_{4,1})) + \cdots$$

$$+ \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^{d-1}(q_{3,d-1}t + q_{4,d-1}))$$

if $l$ is linearly dependent to the equation $l^*$, then we have:

$$\sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^0) = 0, \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^1) = 0, \cdots, \sum_{id_i^* \in S} (b_{id_i^*}(id_i^*)^{d-1}) = 0,$$

so $\begin{pmatrix} (id_1^*)^0 & \cdots & (id_d^*)^0 \\ \vdots & \ddots & \vdots \\ (id_1^*)^{d-1} & \cdots & (id_d^*)^{d-1} \end{pmatrix}_{d \times d} \begin{bmatrix} b_{id_1^*} \\ \vdots \\ b_{id_d^*} \end{bmatrix}_{d \times 1} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}_{d \times 1}$, the matrix on the left contains a $d \times d$ Vandermonde matrice, so the only solution is $b_{id_1^*} = 0, \cdots, b_{id_d^*} = 0$, then $r_2 = r_{1,id_i^*}$ for $id_i^* \in S$ and this is in contradiction to $(C_{1,id_1}, \cdots, C_{1,id_L}, C_2)$ relative to $S$ is inconsistent.

**Game 7.** The challenge key $K^*$ is replaced with the random challenge key $K$ (instead of computing $K^*$ as in Equation (2)). The proof of Lemma B.2 essentially shows that from the adversary's point of view, $K^*$ looks like a uniform element in $G_2$ and hence

$$\Pr[X_7] = \Pr[X_6]$$

Finally, in Game7 the adversary ***A*** basically carries out a chosen-ciphertext attack on the symmetric cipher since ***A*** is still allowed to query ciphertext of the form $< \omega, E = (\omega', C_{1,id_1}, \cdots, C_{1,id_L}, C_2, *) >$ for which $S \subseteq \alpha^*$ and $(C_{1,i} = C_{1,i}^*)_{i \in S}$ & $C_2 = C_2^*$ which are answered using a uniform key $K^*$. Consequently, using the fact that chosen-ciphertext security is implied by AE-OT security we obtain

$$\left| \Pr[X_7] - \frac{1}{2} \right| \leq q_C Adv_{SE,\tilde{t}}^{CT-INT}(k) + Adv_{SE,\tilde{t}}^{IND}(k)$$

**Summary.** We now summarize the above statements into a bound on the advantage of the adversary in the CCA game:

$$Adv_{FIBE_2,t}^{CCA}(k) \leq Adv_{G_1,\tilde{t}}^{q-abdhe}(k) + Adv_{TCR,\tilde{t}}^{TCR}(k) + 2 \cdot q_C \cdot Adv_{SE,\tilde{t}}^{CT-INT}(k) + Adv_{SE,\tilde{t}}^{IND}(k) + q_C / p$$