Chosen-Ciphertext Secure Fuzzy Identity-Based Key Encapsulation without ROM

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
2. E-mail: aics@nuaa.edu.cn
3. E-mail: renyj100@126.com
4. E-mail: xiajinyue@yahoo.com.cn
5. E-mail: bianshizhu@hotmail.com

Abstract. We use hybrid encryption with Fuzzy Identity-Based Encryption (Fuzzy-IBE) schemes, and present the first and efficient fuzzy identity-based key encapsulation mechanism (Fuzzy-IB-KEM) schemes which are chosen-ciphertext secure (CCA) without random oracle in the selective-ID model. To achieve these goals, we consider Fuzzy-IBE schemes as consisting of separate key and data encapsulation mechanisms (KEM-DEM), and then give the definition of Fuzzy-IB-KEM. Our main idea is to enhance Sahai and Waters' "large universe" construction, chosen-plaintext secure (CPA) Fuzzy-IBE, by adding some redundant information to the ciphertext to make it CCA-secure.

Keywords: chosen-ciphertext security; hybrid encryption; fuzzy identity based encryption; key encapsulation mechanism

1 Introduction

In an Identity-Based Encryption (IBE) scheme, a user's public key may be an arbitrary string, such as an email address or other identifier. IBE can simplify public key and certificate management in a public key infrastructure (PKI). Shamir (1985) proposed the concept of IBE in 1984, and the first IBE systems were given by Boneh and Franklin (2001) and Cocks (2001). Ever since then, a rapid development of IBE has taken place, and a series of papers (Boneh and Boyen, 2004a, b; Canetti et al., 2003; Gentry, 2006; Waters, 2005) have been striving to achieve stronger notions of security in the standard model.

However, we don't necessarily have a unique string identifier for each person. Instead, we often identify people by their attributes. For example, an airport might want to send a ciphertext to any A380 plane which belongs to Eastern Airlines or Southern Airlines. To fulfill this task, the concept of Fuzzy-IBE recently introduced by Sahai and Waters (2005) is to provide an error-tolerance property for IBE. Namely, in Fuzzy-IBE, a user with the secret key for the identity ω can decrypt a ciphertext encrypted with the public key ω' if ω and ω' are within a certain distance of each other. Since Sahai and Waters' first work, Fuzzy-IBE has been discussed in the context to the attribute-based encryption (ABE). Recently, 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 to realize their secure information management architecture. In 2007, Baek et al. (2007) 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. Chase (2007) presented a scheme which allows any polynomial number of independent authorities to monitor attributes and distribute secret keys.

Chosen-ciphertext security: In a chosen ciphertext attack (CCA), the adversary is given access to a decryption oracle that allows him to obtain the decryptions of ciphertexts of his choosing. For different reasons, the notion of CCA-secure has emerged as the "right" notion of security for encryption schemes. We stress that, in general, CCA-secure is a much stronger security requirement than chosen-plaintext attacks (CPA), because in CPA an attacker is not given access to the decryption oracle. To the best of our knowledge, all (Sahai and Waters, 2005; Goyal et al., 2006; Pirretti et al., 2006; Baek et al., 2007; Chase, 2007) are CPA-secure. We can use the Fujisaki-Okamoto transformation (Fujisaki and Okamoto, 1999) to achieve CCA-secure, but the drawback of this technique is to use random oracle. Unfortunately a proof in the random oracle model can only serve as a heuristic argument and has proved to possibly lead to insecure schemes when the random oracles are implemented in the standard model (Canetti et al., 1998).

Arbitrary-length plaintexts: As is often the case with most public-key and identity-based encryption schemes, the fuzzy identity-based encryption (Fuzzy-IBE) schemes can only be used to encrypt relatively short messages, typically about 160 bits. To encrypt longer messages, one will have to resort to hybrid techniques (Hofheinz and Kiltz, 2007; Kiltz, 2007; Kiltz and Galindo, 2006): the sender uses the Fuzzy-IBE to encrypt a fresh symmetric key K and encrypts the actual message under the key K .

Our contributions: In this paper, we use hybrid encryption with Fuzzy Identity-Based Encryption (Fuzzy-IBE) schemes that consist of separate key and data encapsulation mechanisms (KEM-DEM) to give the definition of Fuzzy-IB-KEM. Here, the Fuzzy-IB-KEM encrypts a random key under a fuzzy identity, while the DEM encrypts the actual data under this random key. In addition, we present the first and efficient fuzzy identity-based key encapsulation mechanism (Fuzzy-IB-KEM) schemes which are CCA-secure without random oracle in the selective-ID model. Our main idea is to enhance CPA-secure Fuzzy-IBE by adding some redundant information to the ciphertext (consisting of a single group element) to make it CCA-secure. The redundant information is used to check whether a given Fuzzy-IB-KEM ciphertext was "properly generated" by the encryption algorithm or not. Intuitively, this "consistency" checking gives us the necessary leverage to deal with the CCA.

The rest of the paper is organized as follows. In Section 2 we formally define a Fuzzy Identity-Based Key Encapsulation scheme and the security model. Then, we describe the security assumptions. We follow with a description of our construction In Section 3. In Section 4, we prove the security of our scheme. Finally, we conclude in Section 5.

2 Preliminaries

Below, we first introduce the definition of security for a Fuzzy Identity-Based Key Encapsulation system (Fuzzy-IB-KEM), then review the definition of a bilinear map and discuss the complexity assumption on which the security of our system is based.

2.1 Security Model for Fuzzy Identity-Based Key Encapsulation

Similar to the IB-KEM scheme Kiltz and Galindo (2006), a Fuzzy-IB-KEM system consists of four algorithms:

Setup: Setup establishes the PKG's parameter *params* and a master key.

KeyGeneration: KeyGeneration applies the master-key to an identity to generate the private key for that identity.

Encapsulation: Encapsulation takes an identity and *params* as input, and outputs a random session key K and a corresponding ciphertext E .

Decapsulation: Decapsulation decapsulates a ciphertext for an identity by using a private key for that identity to get back the session key K .

A Fuzzy-sID-KEM-CCA game: The Fuzzy-sID-KEM-CCA game is very similar to the Fuzzy-sID-CPA game (Sahai and Waters, 2005).

Init: The adversary declares the identity, α , that he wishes to be challenged upon.

Setup: The challenger runs Setup, and forwards *params* to the adversary.

Challenge: The challenger selects a random bit $b \in \{0,1\}$ and a random key $K_0^* \in$ KeySpace, sets $< E^*, K_1^* > =$ Encapsulation$(params, \alpha)$, $K^* = K_b^*$ and sends $< E^*, K^* >$ to the adversary as its challenge ciphertext.

Guess-stage: Proceeding adaptively, the adversary issues queries $q_1, \cdots, q_m$ where q_i is one of the following:

Key generation query $< \gamma_i >$ where $|\gamma_i \cap \alpha| < d$: The challenger runs KeyGeneration on γ_i and forwards the resulting private key to the adversary.

Decapsulation query $< \gamma_i, E_i >$: The adversary can not request a Decapsulation query $< \gamma_i, E_i >$ where $|\gamma_i \cap \alpha| \geq d$ and E_i and E^* are equivalent. Otherwise, the challenger runs KeyGeneration on γ_i , decapsulates E_i using the private key, and sends the resulting session key K to the adversary.

Guess. The adversary submits a guess $b' \in \{0,1\}$. The adversary wins if $b' = b$.

We call an adversary *A* a Fuzzy-sID-KEM-CCA adversary in the above game.

Definition 1: An Fuzzy-IB-KEM system is $(t, q_{ID}, q_C, \varepsilon)$ Fuzzy-sID-KEM-CCA secure if all t-time Fuzzy-sID-KEM-CCA adversaries making at most q_{ID} Key generation queries and at most q_C chosen ciphertext queries have advantage at most ε in winning the above game.

Note that in contrast to the definition of IB-KEM that given by Kiltz and Galindo (2006), we consider a simplified (but equivalent) security experiment without a "find-stage". This is because the adversary declares the challenge identity firstly in the selective-ID model.

2.2 Bilinear Maps

We briefly review the facts about groups with efficiently computable bilinear maps. We refer the reader to previous literature (Boneh and Franklin, 2001) 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, $e: G_1 \times G_1 \rightarrow G_2$, 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 that $e(g,g)\neq 1$.

2.3 Complexity Assumptions

We state our complexity assumptions below.

Definition 2 (Decisional Bilinear Diffie-Hellman (BDH) Assumption): Suppose a challenger chooses $a,b,c\in\mathbb{Z}_p$ at random. The Decisional BDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^{abc})$ from the tuple $(A=g^a,B=g^b,C=g^c,Z=e(g,g)^z)$ with more than a negligible advantage.

3 Our Construction

Our construction can be viewed as a modification of the Sahai and Waters' "large universe" construction. We modify their scheme by adding some redundant information to the ciphertext (consisting of a single group element) in the Encapsulation algorithm and as a result, the consistency of the ciphertext in Decapsulation algorithm needs to be tested before decapsulating.

3.1 Description

As in the Sahai and Waters (2005), 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 $\Delta_{\mathrm{i,\,S}}$ for $i\in\mathbb{Z}_P$ and a set, S, as elements in $\mathbb{Z}_P:\Delta_{\mathrm{i,\,S}}(x)=\prod_{j\in S,j\neq i}\frac{\mathrm{x}-\mathrm{j}}{\mathrm{i}-\mathrm{j}}$.

Identities will be sets of n elements of $\mathbb{Z}_P{}^*$. Our construction follows:

Setup (n, d)**:** First, choose $g_1=g^y,g_2\in G_1$, $u\in G_2{}^*$, and Let $H:G_1\to\mathbb{Z}_p$ be a target collision-resistant hash function.

Next, choose $t_1,\cdots,t_{n+1}$ uniformly at random from G_1. Let N = $\{1,\cdots,n+1\}$ and we define a function, T, as: $T(x)=g_2{}^{x^n}\prod_{i=1}^{n+1}t_i{}^{\Delta_{i,N}(x)}$ .We can view T as the function $g_2{}^{x^n}g^{h(x)}$ for some n degree polynomial h.

The public key is: $mpk=(g_1,g_2,u,t_1,\cdots,t_{n+1})$.

The master key is: $msk=y$.

KeyGeneration: To generate a private key for identity ω, the following steps are taken. A $d-1$ degree polynomial $q(x)$ is randomly chosen such that $q(0)=y$ .The private key is

$d_{\omega} = ((D_i)_{i\in\omega}, (d_i)_{i\in\omega})$ where $D_i = g_2^{\,q(i)} T(i)^{r_i}$ and $d_i = g^{r_i}$ for r_i is a random member of $\mathbb{Z}_P$.

Return $d_{\omega} = ((D_i)_{i\in\omega}, (d_i)_{i\in\omega})$.

Encapsulation: Encapsulation with the public key of ω' proceeds as follows.

First, a random value $s \in \mathbb{Z}_p$ is chosen. The ciphertext is then published as:

$$C_1 = g^s, \{E_i = T(i)^s\}_{i\in\omega'}, t = H(C_1),\ \Pi = (g_1^{\,t} u)^s, K = e(g_1, g_2)^s.$$

$$E = (\omega', C_1, \{E_i\}_{i\in\omega'}, \Pi).$$

Return (E, K).

Note that the identity, ω', is included in the ciphertext.

Decapsulation: Suppose that a ciphertext, $E = (\omega', C_1, \{E_i\}_{i\in\omega'}, \Pi)$, is encapsulated with a key for identity ω' and we have a private key $d_{\omega} = ((D_i)_{i\in\omega}, (d_i)_{i\in\omega})$ where $|\omega \cap \omega'| \geq d$ .First we test the consistency of the ciphertext : let $t = H(C_1)$.

If $(g, C_1, T(i), E_i)_{i\in\omega'}$ and $(g, C_1, u_1^{\,t} u_2, \Pi)$ is a DH-tuple, then we choose an arbitrary d -element subset, S , of $\omega \cap \omega'$. After that, the ciphertext can be decapsulated as: return $K = \prod_{i\in S} (\frac{e(D_i, C_1)}{e(d_i, E_i)})^{\Delta_{i,S}(0)}$ .Otherwise return a random K ($K \in G_2^{\,*}$).

Correctness: If the ciphertext is consistent, then

$$K = \prod_{i\in S} (\frac{e(D_i, C_1)}{e(d_i, E_i)})^{\Delta_{i,S}(0)} = \prod_{i\in S} (\frac{e(g_2^{\,q(i)} T(i)^{r_i}, g^s)}{e(g^{r_i}, T(i)^s)})^{\Delta_{i,S}(0)} = \prod_{i\in S} (\frac{e(g_2^{\,q(i)}, g^s) e(T(i)^{r_i}, g^s)}{e(g^{r_i}, T(i)^s)})^{\Delta_{i,S}(0)}$$

$$= \prod_{i\in S} e(g_2, g)^{sq(i)\Delta_{i,S}(0)} = e(g_2, g)^{s\sum_{i\in S}(q(i)\Delta_{i,S}(0))} = e(g_2, g)^{sy} = e(g_1, g_2)^s = K$$

Definition 3: A ciphertext $E = (\omega, C_1, \{E_i\}_{i\in\omega}, \Pi)$ is consistent if and only if $(g, C_1, T(i), E_i)_{i\in\omega}$ and $(g, C_1, g_1^{\,t} u, \Pi)$ is a DH-tuple, i.e. $\{e(C_1, T(i)) = e(g, E_i)\}_{i\in\omega}$ and $e(C_1, g_1^{\,t} u) = e(g, \Pi)$.

Definition 4: We say two ciphertexts $E' = (\omega', C_1', \{E_i'\}_{i\in\omega'}, \Pi')$ and $E'' = (\omega'', C_1'', \{E_i''\}_{i\in\omega'}, \Pi'')$ are equivalent if and only if following situations hold: 1)both E' and E'' is consistent; 2) $|\omega' \cap \omega''| \geq d$; 3) $C_1' = C_1''$; 4) $\Pi' = \Pi''$.

3.2 Efficiency

As in Kiltz and Galindo (2006) we make the Diffie-Hellman consistency checking implicit so that the decapsulation algorithm will be more efficient. This is done by choosing a random values $l_i, l \in \mathbb{Z}_p^*$ and computing the session key as:

$$K=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}\frac{e(C_1,\sum_{i\in S}T(i)^{l_i}+(g_1{}^t u)^l)}{e(g,\sum_{i\in S}E_i^{l_i}+\Pi^l)}.$$

It is easy to see

$$K=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}\frac{e(C_1,\sum_{i\in S}T(i)^{l_i}+(g_1{}^t u)^l)}{e(g,\sum_{i\in S}E_i^{l_i}+\Pi^l)}$$

$$=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}(\frac{e(C_1,\sum_{i\in S}T(i)^{l_i})}{e(g,\sum_{i\in S}E_i^{l_i})})(\frac{e(C_1,(g_1{}^t u)^l)}{e(g,\Pi^l)})$$

$$=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}\prod_{i\in S}(\frac{e(C_1,T(i)^{l_i})}{e(g,E_i^{l_i})})(\frac{e(C_1,(g_1{}^t u)^l)}{e(g,\Pi^l)})$$

$$=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}\prod_{i\in S}(\frac{e(C_1,T(i))}{e(g,E_i)})^{l_i}(\frac{e(C_1,g_1{}^t u)}{e(g,\Pi)})^l$$

$$=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}\prod_{i\in S}(\varphi_i)^{l_i}(\varphi)^l$$

If $\{e(C_1,T(i))=e(g,E_i)\}_{i\in\omega}$ and $e(C_1,g_1{}^t u)=e(g,\Pi)$, then $\varphi_i=\frac{e(C_1,T(i))}{e(g,E_i)}=1$, $\varphi=\frac{e(C_1,g_1{}^t u)}{e(g,\Pi)}=1$. So $K=\prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)}$, otherwise is a random group element.

Compared to Sahai and Waters' "large universe" construction (Sahai and Waters, 2005), our scheme contains two more elements of the public key, one more element of ciphertext, $o(d)$ times exponentiation and computes two more pairings in decapsulation.

3.3 Public Verifiability

The consistency of a ciphertext $E=(\omega,C_1,\{E_i\}_{i\in\omega},\Pi)$ can be publicly checked by using bilinear map, i.e. by verifying if $\{e(C_1,T(i))=e(g,E_i)\}_{i\in\omega}$ and $e(C_1,g_1{}^t u)=e(g,\Pi)$. This property is denoted as public verifiability of the ciphertext and it gives rise to a public-key threshold Fuzzy-IB-KEM (Kiltz and Galindo, 2006).

4 Proof of Security

We prove that the security of our scheme in the Fuzzy-sID-KEM-CCA model reduces to the hardness of the Decisional BDH assumption. The theorem and proof are straightforward generalizations to the Fuzzy-IBE case of Sahai and Waters (2005).

Theorem: Assume the (t,ε)-Decisional BDH assumption holds. Then, the above Fuzzy-IB-KEM system is $(t',q_{ID},q_C,\varepsilon')$-Fuzzy-sID-KEM-CCA secure for $t'=t-o(t)$ and $\varepsilon'=\varepsilon$.

Proof: Suppose there exists a polynomial-time adversary, *A*, that can attack our scheme in the selective-ID model with advantage ε'. We build a simulator *B* that can play the Decisional BDH game with advantage $\varepsilon=\varepsilon'$.

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.The challenger flips a fair binary coin μ outside of *B*'s view. If $\mu=0$, the challenger sets $(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^{abc})$; otherwise it sets $(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^z)$ for random a,b,c,z.

Init: *B* will run *A* and receive the challenge identity, α, an n element set of members of $\mathbb{Z}_P$.

Setup: The simulator *B* assigns the public parameters $g_1=A$ and $g_2=B$, $t^*=H(C)$, $u=A^{-t^*}g^d$ for random d. It then chooses a random n degree polynomial $f(x)$ and calculates a n degree polynomial $u(x)$ such that $u(x)=-x^n$ for all $x\in\alpha$ and $u(x)\neq -x^n$ for some other x. Our construction assures that $\forall x(u(x))=-x^n$ if and only if $x\in\alpha$.

Then, for i from 1 to $n+1$the simulator sets $t_i=g_2{}^{u(i)}g^{f(i)}$. Note that since $f(x)$ is a random n degree polynomial all t_i will be chosen independently at random as in the construction and we implicitly have $T(i)=g_2{}^{i^n+u(i)}g^{f(i)}$.

Challenge: The process of computing is as below:

$C_1^*=C,\{E_i^*=C^{f(i)}\}_{i\in\alpha},\Pi^*=C^d,K^*=Z,E^*=(\alpha,C_1^*,\{E_i^*\}_{i\in\alpha},\Pi^*)$. The simulator *B* implicitly selects a random bit $\nu=\mu$.

Then, it sends $<E^*,K^*>$ to the adversary *A* as its challenge ciphertext.

If $\nu=\mu=0$, then $Z=e(g,g)^{abc}$. Then the ciphertext is:

$\{E_i^*=(g^c)^{f(i)}=T(i)^c\}_{i\in\alpha}$, $t^*=H(g^{s^*})=H(g^c)=H(C)=H(C_1)$

$\Pi^*=(g_1{}^{t^*}u)^{s^*}=(g^{at^*}g^{a(-t^*)}g^d)^c=(g^d)^c=C^d$, $K^*=Z=e(g,g)^{abc}=K_0{}^*$.This is a valid ciphertext and session key K^* under the identity α for randomness c. Otherwise, if $v = \mu = 1$, then $Z = e(g,g)^z$ and $K^* = Z = e(g,g)^z = K_1^*$. Since z is random, K^* will be a random element of G_2 from the adversaries view.

Guess-stage:

Key generation query $<\gamma>$ where $|\gamma \cap \alpha| < d$:

Suppose *A* requests a private key γ where $|\gamma \cap \alpha| < d$. Firstly, we define three sets Γ, Γ', S in the following manner:

$\Gamma = \gamma \cap \alpha$, Γ' can be any set such that $\Gamma \subseteq \Gamma' \subseteq \gamma$, $|\Gamma'| = d-1$, and $S = \Gamma' \cup \{0\}$.

Next, we define the decryption key components D_i and d_i for $i \in \Gamma'$ as:

$D_i = g_2^{\lambda_i} T(i)^{r_i}$ where r_i , λ_i are chosen randomly in $\mathbb{Z}_p$ and we let $d_i = g^{r_i}$.

The intuition behind these assignments is that we are implicitly choosing a random $d-1$ degree polynomial $q(x)$ by choosing its value for the $d-1$ points in Γ randomly by setting $q(i) = \lambda_i$ In addition to having $q(0) = a$ .The simulator also needs to calculate the decryption key values for all $i \in \gamma - \Gamma'$.We calculate these points to be consistent with our implicit choice of $q(x)$. The key components are calculated as:

$$D_i = (\prod_{j \in \Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_1^{\frac{-f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}, \text{ and } d_i = (g_1^{\frac{-1}{i^n+u(i)}} g^{r_i'})^{\Delta_{0,S}(i)}.$$

The value $i^n + u(i)$ will be non-zero for all $i \notin \alpha$, which includes all $i \in \gamma - \Gamma'$. Let $r_i = (r_i' - \frac{a}{i^n + u(i)})\Delta_{0,S}(i)$ and let $q(x)$ be defined as above. We then have:

$$D_i = (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_1^{\frac{-f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}$$

$$= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g^{\frac{-af(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}$$

$$= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_2^{a}(g_2^{i^n+u(i)} g^{f(i)})^{\frac{-a}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}$$

$$= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_2^{a}(g_2^{i^n+u(i)} g^{f(i)})^{r_i' - \frac{a}{i^n+u(i)}})^{\Delta_{0,S}(i)}$$

$$= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}) g_2^{a\Delta_{0,S}(i)} (T(i))^{r_i} = g_2^{q(i)} (T(i))^{r_i}$$

Additionally, we have:

$$d_i = (g_1^{\frac{-1}{i^n+u(i)}} g^{r_i'})^{\Delta_{0,S}(i)} = (g^{r_i' - \frac{a}{i^n+u(i)}})^{\Delta_{0,S}(i)} = g^{r_i}$$

Therefore, the simulator is able to construct a private key for the identity γ. Furthermore, the distribution of the private key for γ is identical to that of original scheme since our choices of λ_i induce a random $d-1$ degree polynomial and our construction of the private keys components D_i and d_i.

Decapsulation query $<\gamma, E>$ **: The** simulator *B* first checks that whether the ciphertext $E = (\omega, C_1, \{E_i\}_{i\in\omega}, \Pi)$ is consistent.

If E is not consistent, then the simulator *B* rejects the query.

Else E is consistent, there are two cases.

Case 1: $|\gamma \cap \alpha| < d$: the simulator *B* can first query the Key generation query and get the private key, then decapsulate it.

Case 2: $|\gamma \cap \alpha| \geq d$: there are three sub-cases:

Case 2a: if $s = s^*$, then $t = t^*$. In this case, consistency implies $\Pi' = \Pi''$, then E and E^* are equivalent, so the query made by *A* is illegal. Therefore it may be rejected by simulator *B*.

Case 2b: if $s \neq s^*$ and $t = t^*$, then $C_1 \neq C_1^*$ this is not possible since simulator *B* can found a collision $C_1 \neq C_1^*$ in TCR function H with $H(C_1) = H(C_1^*)$.

Case 2c: if $s \neq s^*$ and $t \neq t^*$, then return $K = e((\frac{\Pi}{C_1^{\,d}})^{\frac{1}{t-t^*}}, B)$.

Correctness: In the original Decapsulation algorithm, first the secret key for identity γ is computed as $\{D_i = g_2^{q(i)}T(i)^{r_i}\}_{i\in\gamma}$ $\{d_i = g^{r_i}\}_{i\in\gamma}$ for random r_i, and then the session key K is reconstructed as:

$$
\begin{aligned}
K &= \prod_{i\in S}(\frac{e(D_i,C_1)}{e(d_i,E_i)})^{\Delta_{i,S}(0)} = \prod_{i\in S}(\frac{e(g_2^{q(i)}T(i)^{r_i},C_1)}{e(g^{r_i},E_i)})^{\Delta_{i,S}(0)} \\
&= \prod_{i\in S}(\frac{e(g_2^{q(i)},C_1)e(T(i)^{r_i},C_1)}{e(g^{r_i},E_i)})^{\Delta_{i,S}(0)} = \prod_{i\in S}(e(g_2^{q(i)},C_1))^{\Delta_{i,S}(0)}\prod_{i\in S}(\frac{e(T(i)^{r_i},C_1)}{e(g^{r_i},E_i)})^{\Delta_{i,S}(0)} \\
&= e(g_2^{q(0)},C_1)\prod_{i\in S}((\frac{e(T(i),C_1)}{e(g,E_i)})^{r_i})^{\Delta_{i,S}(0)} = e(g_2,(C_1)^a)\prod_{i\in S}((\frac{e(T(i),C_1)}{e(g,E_i)})^{r_i})^{\Delta_{i,S}(0)} \\
&= e(g_2,(\frac{\Pi}{(C_1)^d})^{\frac{1}{t-t^*}})\prod_{i\in S}((\rho_i)^{r_i})^{\Delta_{i,S}(0)}
\end{aligned}
$$

Define $\{\rho_i = \frac{e(T(i),C_1)}{e(g,E_i)}\}_{i\in\gamma}$. Since $(\rho_i)^{r_i} = 1$, if $e(T(i),C_1) = e(g,E_i)$ and $(\rho_i)^{r_i}$ is a random element in G_2 otherwise, the decapsulated session key K in the original scheme is distributed as in the simulation.

Guess: *A* will submit a guess v' of v, the simulator *B* will output a guess $\mu' = v'$ of μ .It is easy to see $\mu' = v'$ and $\mu = v$.

If $v' = 0$ the simulator will output $\mu' = 0$ to indicate that it was given a BDH-tuple. Otherwise it will output $\mu' = 1$ indicating it was given a random 4-tuple.

As shown in the construction the simulator's generation of public parameter and private keys is identical to that of the actual scheme.

Let F_B be the event that the simulator *B* wins its DBDH game, then

$$
\begin{aligned}
&\varepsilon = \Pr[F_B] = \Pr[\mu' = 1 | \mu = 1]\Pr[\mu = 1] + \Pr[\mu' = 0 | \mu = 0]\Pr[\mu = 0] \\
&= \Pr[v' = 1 | v = 1]\Pr[v = 1] + \Pr[v' = 0 | v = 0]\Pr[v = 0] \\
&= \varepsilon'
\end{aligned}
$$

5 Conclusions and Future Work

We present first efficient fuzzy identity-based key encapsulation mechanisms (Fuzzy-IB-KEM) schemes which are selective-ID-CCA-secure without random oracle. Compared to Sahai and Waters' "large universe" construction (Sahai and Waters, 2005), our scheme contains two more elements of the public key, one more element of ciphertext, $o(d)$ times exponentiation and computes two more pairings in decapsulation.

Chase (2007) showed how to apply their techniques to achieve a CPA secure multi-authority version of the large universe fine grained access control ABE presented by Goyal et al. (2006). We want to make it CCA secure.

Acknowledgement

The authors wish to thank many anonymous referees for their suggestions to improve this paper.

References

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

Boneh, D., Boyen, X., 2004a. Efficient selective-ID Identity based encryption without random oracles, In Advances in Cryptology–EUROCRYPT 2004, volume 3027 of LNCS, pages 223-238. Springer-Verlag.

Boneh, D., Boyen, X., 2004b. Secure identity based encryption without random oracles, In advances in Cryptology-CRYPTO 2004, volume 3152 of LNCS, pages 443-459. Springer-Verlag.

Boneh, D., Franklin, M.K., 2001. Identity-based encryption from the Weil pairing, In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213-229. Springer-Verlag.

Boyen, X., 2007. General Ad Hoc encryption from exponent inversion IBE, In Advances in Cryptology-EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, pages 394-411. Springer-Verlag.

Boyen, X., Mei, Q., Waters, B., 2005. Direct chosen ciphertext security from identity-based techniques, In V.Atluri, C.Meadows, and A.Juels, editors, ACM CCS 05, pages 320-329. ACM Press, Nov.

Canetti, R., Goldreich, O., Halevi, S., 1998. The random oracle methodology, revisited, In 30th ACM STOC, pages 209-218 Dallas, Texas, USA, May 23-26. ACM Press.

Canetti, R., Halevi, S., Katz, J., 2003. A forward-secure public-key encryption scheme, In Proceedings of EUROCRYPT 2003. Springer-Verlag.

Chase, M., 2007. Multi-authority attribute based encryption. Lecture Notes in Computer Science, Springer Berlin / Heidelberg.

Cocks, C., 2001. An identity based encryption scheme based on quadratic residues, In Proceedings of the 8th IMA International Conference on Cryptography and Coding.

Fujisaki, E., Okamoto, T., 1999. Secure integration of asymmetric and symmetric encryption schemes, In Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, pages 537-554. Springer-Verlag.

Gentry, C., 2006. Practical identity-based encryption without random oracles, In Advances in Cryptology-EUROCRYPT 2006, Lecture Notes in Computer Science. Springer-Verlag.

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

Hofheinz, D., Kiltz, E., 2007. Secure hybrid encryption from weakened key encapsulation, In Alfred Menezes, editor, CRYPTO 2007, LNCS, pages 553–571. Springer-Verlag, Berlin, Germany, August 2007. (Cited on page 2, 3, 22.).

Kiltz, E., 2007. Chosen-ciphertext secure key-encapsulation based on Gap Hashed Diffie-Hellman, In Proceedings of PKC 2007, volume 4450 of LNCS, pages 282-297. http://eprint.iacr.org/2007/036 . (Cited on page 3, 4, 17, 18.) .

Kiltz, E., Galindo, D., 2006. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles, In: Batten, L.M., Safavi-Naini, R.(eds.) ACISP 2006. LNCS, vol. 4058, pp. 336-347. Springer, Heidelberg.

Pirretti, M., Traynor, P., McDaniel, P., Waters, B., 2006. Secure Attribute-Based Systems, In ACM CCS'06, to appear.

Sahai, A., Waters, B., 2005. Fuzzy identity-based encryption, In Advances in Cryptology-EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science. Springer-Verlag.

Shamir, A., 1985. Identity-based cryptosystems and signature schemes, In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47-53. Springer-Verlag New York Inc.

Waters, B., 2005. Efficient identity based encryption with out random oracles, In Advances in Cryptology–EUROCRYPT 2005, volume 3494 of LNCS, pages 114–127. Springer-Verlag.