Fuzzy Identity Based Encryption Scheme with Some Assigned Attributes

XiMing Li, Bo Yang, YuBin Guo
College of Informatics
South China Agricultural University
GuangZhou, China. 510642
Email: liximing, byang, guoyubin@scau.edu.cn

Abstract—In this paper the concept of Fuzzy IBE schemes with some fixed attributes (SAA-FIBE) is proposed and one construction of it is presented. SAA-FIBE scheme can be viewed as a variant of SW scheme described in [1] which demanding no fixed positive or negative attributes. In our scheme, a user with identity \( \omega \) can decrypt the message that is encrypted with a set of attributes, \( \omega' \), if and only if \( |\omega' \cap \omega| \geq d \) and \( \omega \) must have or must have not some attributes described in encryption policy.

The scheme are both error-tolerant and secure against collusion attacks in the SPID-FIBE attack model.

Keywords—Fuzzy Identity-Based Encryption, Attribute-Based Encryption, Decisional Bilinear Diffie-Hellman Assumption, Encryption Policy.

I. INTRODUCTION

The concept of Fuzzy Identity-Based Encryption (FIBE) introduced by Sahai and Waters in [1] is a generalization of identity-based cryptosystems. FIBE allows for a private key for an identity, \( \omega \), to decrypt a ciphertext encrypted with an identity, \( \omega' \), if and only if the identities \( \omega \) and \( \omega' \) are close to each other as measured by the “set overlap” distance metric. In other words, a user with identity \( \omega \) can decrypt the message that is encrypted with a set of attributes, \( \omega' \), if and only if \( |\omega' \cap \omega| \geq d \).

The contribution of the Sahai-Water’s approach is that public key of any user is fuzzy and described as a set of attributes but haven’t threshold property.

For example, in a social network each user dictates their own policy in order to restrict access to their personal information. A principal’s policy can be viewed as a description of attributes they find desirable in other principals. If Bob is only interested in meeting women with long black hair or women with medium wealth or women with medium weight, he can encrypt his information with attribute list \( \{ \text{women} \land (\text{longblackhair} \lor \text{mediumwealth} \lor \text{mediumweight}) \} \), but it can not be implemented in scheme introduced in [1].

It is a natural problem in FIBE system when someone encrypt message with a set and he demand that the receiver must have some assigned attributes in the set or must not have some attributes outside of the set. In this paper we give a new primitive named SAA-FIBE to resolve the problem promoted in the example.

A. Our Contribution

We propose a construction of SAA-FIBE in which we view identities as a policy and a set of descriptive attributes and the expression of identity is just as simple as that in [1] except that it demand that the decryptor must have or must not have some attributes assigned in policy. Security proof can be reduced to k-BDH Assumption which is proved to be as hard as MBDH Assumption.

In SAA-FIBE scheme, a user with the secret key for the identity \( \omega \) can decrypt a ciphertext encrypted with the public key \( \omega' \) if and only if \( |\omega' \cap \omega| \geq d \) and \( \omega \) has or has not some special attributes assigned in ciphertext. Our system allows for a certain amount of error-tolerance in the identities.

B. Related Work

Shamir [2] first proposed the concept of Identity-Based Encryption. It wasn’t until much later that Boneh and Franklin [3] presented the first Identity-Based Encryption scheme that was both practical and secure. The construction for Hierarchical Identity Based Encryption(HIBE) was introduced in [4], [5]. HIBE can be used to construct FIBE, but the FIBE will be less efficient than true FIBE schemes.

Since the introduction of FIBE by Sahai and Waters in [1], there have been several papers [6], [7], [8] that have proposed different varieties of FIBE (or Attribute-Based Encryption).

The expression of identity in the works [7], [6], [8], [9], [10], [11] is more complex than that in [1] because most of the works have been done on monotonic access structure over attributes. In [12] Ling Cheung and Calvin C. Newport proposed ABE scheme which can treat positive and negative attributes but haven’t threshold property.

C. Organization

The rest of the paper is organized as follows. In Section II we formally define a Fuzzy Identity-Based Encryption scheme with dynamic threshold including the Selective-ID security model. Then, we describe our security assumptions. We follow with a description of our construction in Section III and in Section IV we prove the security of our scheme.
Finally, we give discussions and conclusions in Section V.

II. PRELIMINARIES

We begin by presenting our definition of security. We follow with a brief review of bilinear maps, and then state the complexity assumptions we use for our proofs of security.

A. Definitions

In this section we define our Selective PolicyID models of security for Fuzzy Identity Based Encryption game (SPID-FIBE). The SPID-FIBE game is very similar to the standard Selective-ID model for Identity-Based Encryption. Before attack adversary must declare the policy and identity \((\alpha, p)\).

For every attribute \(i\) in universe, policy \(p\) is defined as follows: \(p_i = 1\), if the \(i\)th attribute of the universe is an element of \(\alpha\) and is required to be an element of decryptor’s public key; \(p_i = 0\), if the \(i\)th attribute of the universe isn’t an element of \(\alpha\) and is not required to be an element of decryptor’s public key; \(p_i = *\), if the \(i\)th attribute of the universe is not considered by the encryptor.

The adversary is only allowed to query for secret keys for identity and policy tuple \((\gamma, p')\) with the restriction as follows:

\[
(p' \oplus p \neq 0 \text{ and } |\gamma \cap \alpha| \leq d) \quad (1)
\]

\[
(p' \oplus p = 0 \text{ and } |\gamma \cap \alpha| \leq d) \quad (2)
\]

\[
(p' \oplus p \neq 0 \text{ and } |\gamma \cap \alpha| \geq d) \quad (3)
\]

SPID-FIBE game.

Init. The adversary declares the policy and identity, \((\alpha, p)\), that he wishes to be challenged upon.

Setup. The challenger runs the setup phase of the algorithm and tells the adversary the public parameters.

Phase 1. The adversary is allowed to issue queries for private keys for identity-policy tuple \((\gamma_j, p_j)\) which agree with Eq.1, Eq.2, Eq.3 for all \(j\).

Challenge. The adversary submits two equal length messages \(M_0, M_1\). The challenger flips a random coin, \(b\), and encrypts \(M_b\) with \((\alpha, p)\). The ciphertext is passed to the adversary.

Phase 2. Phase 1 is repeated.

Guess. The adversary outputs a guess \(b'\) of \(b\).

The advantage of an adversary \(A\) in this game is defined as

\[
Pr[b = b'] - \frac{1}{2}
\]

Definition 1: (SPID-FIBE).

A scheme is secure in the SPID-FIBE model of security if all polynomial-time adversaries have at most a negligible advantage in the above game.

B. Bilinear Maps

We briefly review the facts about groups with efficiently computable bilinear maps. We refer the reader to previous literature [3] 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.

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

2) The map is non-degenerate: \(e(g, g) \neq 1\).

C. Complexity Assumptions

We state a series of complexity assumptions below.

Definition 2: Decisional Bilinear Diffie-Hellman (DBDH) Assumption. Suppose a challenger chooses \(a, b, c, z \in \mathbb{Z}_p\) 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.

Def. 2 was first used in [3].

Definition 3: Decisional Modified Bilinear Diffie-Hellman (MBDH) Assumption. Suppose a challenger chooses \(a, b, c, z \in \mathbb{Z}_p\) at random. Decisional MBDH 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.

Def. 3 used in [1] is variant of Def. 2.

Definition 4: \(k\)-Decisional Bilinear Diffie-Hellman (\(k\)-BDH) Assumption. Suppose a challenger chooses \(a, b, c, z \in \mathbb{Z}_p\), \(a_1, \ldots, a_k, b, c, d, z_1, \ldots, z_k, z'_1, \ldots, z'_k \in \mathbb{Z}_p\) at random. \(k\)-BDH assumption is that no polynomial-time adversary is to be able to distinguish tuple \((A = g^{a_i}, B = g^b, C = g^c, D = g^d, Z_i = e(g, g)^{abc}, Z'_i = e(g, g)^{bcd})\) from \((A = g^{a_i}, B = g^b, C = g^c, D = g^d, Z_i = e(g, g)^{z_i}, Z'_i = e(g, g)^{z'_i})\) for every \(i (i \in \{1, \ldots, k\})\), with more than a negligible advantage.

III. OUR CONSTRUCTION

We view identities as sets of attributes \(\omega\) and we let the value \(d\) represent the biggest threshold. A detailed description of our scheme follows.

A. Description

We wish to create an IBE scheme in which a ciphertext created using identity \((\omega', p)\) can be decrypted only by a secret key \(\omega\) where \(|\omega' \cap \omega| \geq d\) and \(\omega\) agree with the policy \(p\). Let \(G_1\) be bilinear group of prime order \(p\), and let \(g\) be a generator of \(G_1\). Additionally, let \(e: G_1 \times G_1 \rightarrow G_2\) denote the bilinear map. A security parameter \(K\), will determine the size of the groups.
We also define the Lagrange coefficient $\Delta_{i,S}$ for $i \in \mathbb{Z}_p$ and a set, $S$, of elements in $\mathbb{Z}_p$.

$$\Delta_{i,S}(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$$  \hspace{1cm} (4)

Identities will be element subsets of some universe, $\mathcal{U}$, of size $|\mathcal{U}|$. We denote it as $n$. We will associate each element with a unique integer in $\mathbb{Z}_p$. (In practice an attribute will be associated with each element so that identities will have some semantics.) Our construction follows:

**Setup.** First, define the universe, $\mathcal{U}$. For simplicity, we can take the first $n$ elements of $\mathbb{Z}_p$ to be the universe. Namely, the integers $1, \ldots, n \pmod{p}$.

Choose $f$ uniformly at random from $\mathbb{Z}_p^*$, denote $e(g, g)^f$ as $Y_f$.

Next, choose $t_i, a_i, \tilde{a}_i, a'_i$ uniformly at random from $\mathbb{Z}_p$ for $1 \leq i \leq n$. Finally, choose $y_i (i \in \{1, \ldots, d\})$ uniformly at random in $\mathbb{Z}_p^*$.

The published public parameters are:

$$d, Y_f, Y_i = e(g, g)^{y_i} \quad (1 \leq i \leq d)$$

$$T_i = g^{t_i}, A_i = g^{a_i}, \tilde{A}_i = g^{\tilde{a}_i}, A'_i = g^{a'_i} \quad (1 \leq i \leq n)$$

The master key is:

$$t_i, a_i, \tilde{a}_i, a'_i \quad (1 \leq i \leq n)$$

$$f, y_i \quad (1 \leq i \leq d)$$

**Key Generation.** To generate a private key for identity $\omega \subseteq \mathcal{U}$, the following steps are taken. $d$ polynomials $q_j (j \in \mathbb{Z}_d^*)$ with degree $d$ is randomly chosen such that $q_j(0) = y_j$. The private key consists of components, $(D_{i,j})_{i \in \omega, j \in \mathbb{Z}_d^*}$, where $D_{i,j} = g^{q_j(i)}$. This means that every attribute of $\omega$ has $d$ values, then $\omega$ has $|\omega| \times d$ values.

Next, the trusted authority picks up random values $s_i \in \mathbb{Z}_p$ for $1 \leq i \leq n$, sets $s = \sum_{i=1}^n s_i$, and computes $D_0 = g^{f-s}$. For $1 \leq i \leq n$, the authority also computes $[D_{i,j}, D_{i}'] = [g^{\tilde{a}_i}, g^{a'_i}]$ if $i \in \omega$, and $[D_{i,j}, D_{i}'] = [g^{\tilde{a}_i}, g^{a'_i}]$ if $i \notin \omega$. The secret key $SK_{\omega}$ is $D_{0,0}, [D_{i,j}], [D_{i,}'] |_{1 \leq i \leq n, 1 \leq j \leq d}$.  

**Encryption.** Encryption with the public key $\omega'$ and message $M \in \mathbb{G}_2$ proceeds as follows. Ciphertext policy $p_{\omega'} = \{p_1, \ldots, n\}$ is defined as follows: $p_i = 1$ if we demand attribute $i \in \omega'$, $p_i = 0$ if we demand attribute $i \notin \omega'$; $p_i = *$ if we don’t care attribute $i$. Let $m$ denote the count number of 1 in $p_{\omega'}$. Two random values $r, r_f, r_d \in \mathbb{Z}_p$ are chosen. The ciphertext is then published as:

$$E = (p_{\omega'}, \omega', E_0, \{E_{f_i}\}_{1 \leq i \leq n}, \{E_{d_i}\}_{i \in \omega'}\text{ and }p_{\omega'} = *)$$

$$E' = MY_{f}^{r_f}Y_{d-m}^{r_d}$$

$$E_0 = g^{r_d}$$

**Decryption.** Suppose that a ciphertext, $E = (p_{\omega'}, \omega', E_0, \{E_{f_i}\}_{1 \leq i \leq n}, \{E_{d_i}\}_{i \in \omega'}\text{ and }p_{\omega'} = *)$, is encrypted with a key for identity $\omega'$ and we have a private key for identity $\omega$, where $\omega' \cap \omega \supseteq d \geq 0$ and $\omega$ agree with the policy in the ciphertext. Denote $\omega'$ as the set composed of the attributes that the encryptor did not describe as 1 in the policy. Denote $\omega' \cap \omega$ as $S$. Denote $d - m$ as $k$.

For $1 \leq i \leq n$, let

$$D'_i = \begin{cases} D_i & (p_i \neq *) \\ D'_i & (p_i = *) \end{cases}$$

The recipient decrypts the ciphertext as follows.

$$E' = \frac{e(E_0, D_0)\prod_{i=1}^m e(E_{f_i}, D'_i)\prod_{i \in S}(e(E_{d_i}, D_{i,k}))\Delta_{i,S}(0)}{M Y_f^{r_f} Y_{d-m}^{r_d}}$$

$$= \frac{e(g^{r_f}, g^{r-d})\prod_{i=1}^m e(E_{f_i}, D'_i)\prod_{i \in S}(e(g^{q_i(t_i)}, g^{q_i(a'_i)}))\Delta_{i,S}(0)}{M e(g,g)^{r_f} e(g,g)^{r_d}}$$

$$= \frac{e(g,g)^{r_f} e(g,g)^{r_d} (e(g,g))^{y_{k,d}}} {M}$$

The last equality is derived from using polynomial interpolation in the exponents. Since, the polynomial $q_k(x)$ is of degree $k - 1$ it can be interpolated using $k$ points.

**IV. OVERVIEW OF SECURITY PROOF**

We prove that the security of our scheme in the Selective-ID model and reduce it to the hardness of the $k$-BDH assumption.

**Theorem 1:** If an polynomial challenger $c$ have advantage $\varepsilon$ in resolving $k$-BDH problem defined in Def.4, then there will be a challenger $c2$ gain advantage $\varepsilon/2$ in resolving MBDH problem defined in Def.3.

**Proof:** Suppose adversary $Adv$ can gain advantage $\varepsilon$ in Assumption 4. We construct a simulator $Sim$ that can distinguish a TBDH tuple from a random tuple with advantage $\varepsilon$. Let $G_1, G_2$ be groups of prime order $p$, and let $g$ be a generator of $G_1$. First the MBDH challenger selects at random: $a, b, c, z \in \mathbb{Z}_p, v \in \{0, 1\}$. It defines $Z = e(g, g)^v$ if $v = 1$ else $Z = e(g, g)^{\frac{z}{k}}$. The challenger then gives $(A = g^a, B = g^b, C = g^c, Z)$ to $Sim$.

Sim selects at random: $(a_i)_{i \in \mathbb{Z}_k^+} \in \mathbb{Z}_p$ it defines $(D = g^d, Z_i = Z^{a_i}, Z'_i = e(B, C)^{d_i})$. Sim then gives $(A^{a_i}, B, C, D, Z_i, Z'_i)_{i \in \mathbb{Z}_{k-1}^+}$ and $(A, B, C, D, Z, Z')$ to $Adv$. The tuple given to $Adv$ is a well-formed $k$-BDH tuple.

$Adv$ produces a guess $v'$ and give it to $Sim$. $Sim$ outputs $v'$ for $v$.
As shown in the construction the simulator’s generation of the tuple is identical to that of the actual $k$-BDH tuple.

In the case where $v = 1$ the adversary gains no information about $v$, so we have $\Pr(v' = v|v = 1) = 1/2$. If $v = 0$, $\Pr(v' = v|v = 0) = 1/2 + \epsilon$.

The overall advantage of the simulator in the MBDH game is $\frac{1}{2}\Pr(v' = v|v = 1) + \frac{1}{2}\Pr(v' = v|v = 0) - \frac{1}{2} = \frac{1}{2} \left( \frac{1}{2} + \frac{1}{2} \right) + \epsilon - \frac{1}{2} = 1/2 + \epsilon$.

**Theorem 2:** If a probabilistic polynomial-time adversary can win the SPID-FIBE game with non-negligible advantage, then we can construct a simulator that can distinguish $k$-BDH tuple from a random tuple with non-negligible advantage.

This scheme combines a policy encryption FIBE scheme and a dynamic threshold FIBE scheme which were introduced by authors of the paper [1], [6]. Security proof of our scheme is largely a combination of the two schemes’ proof. In the proof we give a $k$-BDH tuple to a challenge $C$ and $C$ will construct a simulator $B$ which will use an adversary $A$ to get the right answer of $k$-BDH problem.

In the proof process $B$ sets up a SAA-FIBE system and puts the difficult problem in the parameters secretly and then $B$ uses $A$ as a subroutine in the the SPID-FIBE game to defeat the system. If $A$ can defeat the system then $B$ will get the right answer of $k$-BDH problem. So $C$ wins. Due to space limitation the completed proof is omitted here.

V. CONCLUSIONS AND DISCUSSIONS

The concept of Fuzzy Identity Based Encryption with Some Assigned Attributes was introduced which allows for error-tolerance between the identity of a private key and the public key used to encrypt a ciphertext. User with identity $\omega$ can decrypt the message that is encrypted with a set of attributes, $\omega'$, if and only if $|\omega' \cap \omega| \geq d$ and $\omega$ must have or must have not some attributes described in ciphertext.

A construction of SAA-FIBE is presented and the security of our construction can be proved under the SPID-FIBE model by reducing it to $k$-BDH assumption. Proof of $k$-BDH assumption’s hardness is given in the paper.

ACKNOWLEDGMENT

This work is supported by the National Natural Science Foundation of China under Grants 60773175 and 60673077.

REFERENCES


