Fuzzy Identity Based Signature

Piyi Yang, Zhenfu Cao [1] and Xiaolei Dong

Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

Abstract

We introduce a new cryptographic primitive which is the signature analogue of fuzzy identity based encryption(IBE). We call it *fuzzy identity based signature*(IBS). It possesses similar error-tolerance property as fuzzy IBE that allows a user with the private key for identity ω to decrypt a ciphertext encrypted for identity ω' if and only if ω and ω' are within a certain distance judged by some metric. A fuzzy IBS is useful whenever we need to allow the user to issue signature on behalf of the group that has certain attributes. Fuzzy IBS can also be applied to biometric identity based signature. To our best knowledge, this primitive was never considered in the identity based signature before.

We give the definition and security model of the new primitive and present the first practical implementation based on Sahai-Waters construction[6] and the two level hierarchical signature of Boyen and Waters[9]. We prove that our scheme is existentially unforgeable against adaptively chosen message attack without random oracles.

Key words: fuzzy, identity based signature, biometric, attribute based signature, unforgeable

1 Introduction

The concept of fuzzy identity based encryption(IBE) was introduced by Sahai and Waters [6] and further developed in a line of works, e.g., [1,3,5]. In a nutshell a fuzzy identity based encryption allows a user with the private key for identity ω to decrypt a ciphertext encrypted for identity ω' if and only if ω and ω' are within a certain distance judged by some metric.

[1] Corresponding author (E-mail: zfcao@cs.sjtu.edu.cn)

In this paper we introduce a novel cryptographic primitive that is the signature analogue of a fuzzy identity based encryption, we call it *fuzzy identity based signature*. A fuzzy identity based signature(IBS) allows a user with identity ω to issue a signature which could be verified with identity ω' if and only if ω and ω' are within a certain distance judged by some metric. Fuzzy IBS can be directly applied to identity based signature system that uses biometric identities. Another interesting application is attribute based signature. In this application, a user can issue a signature on behalf of the group that has a certain set of attributes. For example, an IT company might want a C++ senior programmer whose age is above 50 to sign the technical report. In this scenario, it will sign to the identity {"C++","senior programmer","above 50"}. Any user who has an identity that contains all of these attributes could issue the signature.

1.1 Our contribution.

In this paper, we first contribute the definition, formalization, and security model of fuzzy identity based signature. We then construct a practical fuzzy identity based signature based on Sahai-Waters construction[6]. We prove that our scheme is existentially unforgeable against adaptively chosen message attack as defined in section 3.2 without random oracles. To our best knowledge, there is no fuzzy identity based signature scheme that has been formally presented before.

2 Preliminaries

2.1 Bilinear Pairings and Assumptions

Let us consider two multiplicative group G and G_T of the same prime order p. A bilinear pairing is a map $e : G \times G \rightarrow G_T$ with the following properties[2]:

1. Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$, where $u, v \in G$, and $a, b \in \mathbb{Z}_p^*$

2. Non-degeneracy: there exists $u \in G$ and $v \in G$ such that $e(u, v) \neq 1$

3. Computability: It is efficient to compute $e(u, v)$ for all $u, v \in G$

2.2 Computational Diffie-Hellman(DH) Assumption

We briefly review the Computational Diffie-Hellman(DH) Assumption. We refer the reader to previous literature[2,4] for more details.

The challenger chooses $a, b \in \mathbb{Z}_p$ at random and outputs $(g, A = g^a, B = g^b)$. The adversary then attempts to output $g^{ab} \in \mathbb{G}$. An adversary, $\mathcal{B}$, has at least an ϵ advantage if

$$Pr[\mathcal{B}(g, g^a, g^b) = g^{ab}] \geq \epsilon$$

where the probability is over the randomly chosen a, b and the random bits consumed by $\mathcal{B}$.

Definition 1 *The computational $(t, \epsilon) - DH$ assumption holds if no t-time adversary has at least ϵ advantage in solving the above game.*

2.3 Threshold Secret Sharing Schemes

Secret sharing schemes were introduced by Shamir[7]. A (n, t) threshold secret sharing scheme distributes a secret s among a set of players $\mathcal{P} = \{R_1, .., R_n\}$ of n players by a dealer. Each player R_i will privately receive s_i as a share of the secret by the dealer. Then, those subsets with at least t players could recover the secret, while other subsets containing less than t players couldn't gain any information about the secret.

Shamir's solution[7] uses polynomial interpolation. Let $GF(q)$ be a finite field with $q \geq n$ elements, and let $s \in GF(q)$ be the secret to be shared. The dealer randomly picks a polynomial $f(x)$ of degree $t-1$, and the constant of $f(x)$ is s. So $f(x)$ has the form $f(x) = s + \sum_{j=1}^{t-1} a_j x^j$.

If we assign every player R_i with a unique field element α_i. Then the dealer sends the secret share $s_i = f(\alpha_i)$ to R_i through a private channel. Now if the set of players $S \subset \mathcal{P}$ such that $|S| \geq t$, then they could recover the secret $s = f(0)$ by using the following formula:

$$f(x) = \sum_{R_i \in S} \Delta_{\alpha_i, S}(x) f(\alpha_i) = \sum_{R_i \in S} \Delta_{\alpha_i, S}(x) s_i$$

where

$$\Delta_{\alpha_i,S}(x) = \prod_{R_l \in S, l \neq i} \frac{x - \alpha_l}{\alpha_i - \alpha_l}.$$

On the other hand, it can be proved that if the subset $B \subset \mathcal{P}$ such that $|B| < t$ couldn't get any information about the polynomial $f(x)$.

3 Definitions

3.1 Fuzzy Identity Based Signature

The generic fuzzy identity based signature(FIBS) scheme consists of the following algorithms.

- Setup(1^k): The Setup algorithm is a probabilistic algorithm that takes as input a security parameter 1^k. It generates the master key mk and public parameters $params$ which contains an error tolerance parameter d. Note that $params$ is made public and mk is kept secret.
- Extract(msk, ID): The Private Key Extraction algorithm is a probabilistic algorithm that takes as input the master key mk and an identity ID. It outputs a private key associate with ID, denoted by D_{ID}.
- Sign($params, D_{ID}, M$): The signing algorithm is a probabilistic algorithm that takes as input the public parameters $params$, a private key D_{ID} associated with ID and a message M. It outputs the signature σ.
- Verify($params, ID', M, \sigma$): The verification algorithm is a deterministic algorithm that takes as input the public parameters $params$, an identity ID' such that $|ID' \cap ID| \geq d$, the message M and the corresponding signature σ. It returns a bit b, where $b = 1$ means that the signature is valid.

3.2 Security Model.

Definition 2 *(UF-FIBS-CMA). Let $\mathcal{A}$ be an adversary assumed to be a probabilistic Turing machine taking as input a security parameter k. Consider the following game in which $\mathcal{A}$ interacts with a challenger $\mathcal{C}$.*

- ***Setup*** *The challenger $\mathcal{C}$ runs the setup phase of the algorithm and tells the adversary $\mathcal{A}$ the public parameters.*

- ***Phase 1*** *$\mathcal{A}$ issues private key queries and signature queries for any identities γ_i adaptively.*
- ***Phase 2*** *$\mathcal{A}$ declares the target identity α, where $|\alpha \cap \gamma_i| < d$ for all γ_i got from Phase 1.*
- ***Phase 3*** *$\mathcal{A}$ issues private key queries for many identities γ_j, where $|\gamma_j \cap \alpha| < d$ for all j. $\mathcal{A}$ issues signature queries for any identities.*
- ***Phase 4*** *$\mathcal{A}$ outputs $(\alpha, \tilde{M}, \tilde{\sigma})$, where $\tilde{\sigma}$ is α's valid signature on the message $\tilde{M}$ and $\mathcal{A}$ does not make a signature query on $(\tilde{M}, \tilde{\sigma})$ for identity α .*

We define $\mathcal{A}$'s success probability by

$$Succ_{FIBS,\mathcal{A}}^{UF-FIBS-CMA}(k) = \mathbf{Pr}[Verify(\alpha, \tilde{M}, \tilde{\sigma}] = 1$$

The fuzzy identity based signature scheme FIBS is said to be UF-FIBS-CMA secure if $Succ_{FIBS,\mathcal{A}}^{UF-FIBS-CMA}(k)$ is negligible in the security parameter k.

4 Fuzzy Identity Based Signature Scheme

Our scheme is extended from the two level hierarchical signature presented by Boyen and Waters[9].

The description that follows assumes that groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order p such that a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be constructed, and g is a generator of $\mathbb{G}$.

Identities will be sets of n elements of $\mathbb{Z}_p^*$. We use the definition of Lagrange coefficient $\Delta_{i,S}(x)$ as in section 2.3.

Setup(n,d) To setup the system, first, choose $g_1 = g^y, g_2 \in \mathbb{G}$. Next, choose $t_1, ..., t_{n+1}$ uniformly at random from $\mathbb{G}$. Let N be the set $\{1, ..., n+1\}$ and we define a function, T, as:

$$T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}.$$

Next, select a random integer $z' \in \mathbb{Z}_p$ and a random vector $\vec{z} = (z_1, ...z_m) \in \mathbb{Z}_p^m$

The public parameters of the system and the master key is given by,

$$\mathbf{PP} = (g_1, g_2, t_1, ..., t_{n+1}, v' = g^{z'},$$

$$v_1 = g^{z_1}, ..., v_m = g^{z_m}, A = e(g_1, g_2)) \in \mathbb{G}^{n+m+4} \times \mathbb{G}_T$$

$$\mathbf{MK} = y.$$

Extract(PP,MK,ω) To generate the private key for the identity ω, first choose a random $d-1$ degree polynomial q such as $q(0) = y$, and return $K_\omega = (\{D_i\}_{i\in\omega}, \{d_i\}_{i\in\omega}) \in \mathbb{G}^{2n}$, where the elements are constructed as

$$\begin{aligned} D_i &= g_2^{q(i)} T(i)^{r_i}, \\ d_i &= g^{-r_i}. \end{aligned}$$

where r_i is a random number from $\mathbb{Z}_p$ defined for all $i \in \omega$.

Sign(PP,K_ω, M) To sign a message represented as a bit string $M = (\mu_1 \cdots \mu_m) \in \{0,1\}^m$ for identity ω, using private key $K_\omega = (\{D_i\}_{i\in\omega}, \{d_i\}_{i\in\omega}) \in \mathbb{G}^{2n}$, select a random $s_i \in \mathbb{Z}_p$ for each i in ω , and output

$$\begin{aligned} S &= (\{D_i \cdot (v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{s_i}\}_{i\in\omega}, \{d_i\}_{i\in\omega}, \{g^{-s_i}\}_{i\in\omega}) \\ &= (\{g_2^{q(i)} \cdot T(i)^{r_i} \cdot (v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{s}\}_{i\in\omega}, \{g^{-r_i}\}_{i\in\omega}, \{g^{-s_i}\}_{i\in\omega}) \in \mathbb{G}^{3n}. \end{aligned}$$

Verify(PP,ω',M,σ) To verify a signature $S = (\{S_1^{(i)}\}_{i\in\omega}, \{S_2^{(i)}\}_{i\in\omega}, \{S_3^{(i)}\}_{i\in\omega})$ against an identity ω', where $|\omega' \cap \omega| \geq d$, and a message $M = (\mu_1, ..., \mu_m) \in \{0,1\}^m$, choose an arbitrary $d-$element subset S of $\omega \cap \omega'$ and verify that

$$\begin{aligned} &\textstyle\prod_S (e(S_1^{(i)}, g) \cdot e(S_2^{(i)}, T(i)) \cdot e(S_3^{(i)}, v' \textstyle\prod_{j=1}^m v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\ &= \textstyle\prod_S (e(g_2^{q(i)} \cdot T(i)^{r_i} \cdot (v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{s_i}, g) \cdot e(g^{-r_i}, T(i)) \cdot e(g^{-s_i}, v' \textstyle\prod_{j=1}^m v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\ &= \textstyle\prod_S (e(g_2^{q(i)}, g) \cdot e(T(i)^{r_i}, g) \cdot e((v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{s_i}, g) \cdot e(g^{-r_i}, T(i)) \cdot e(g^{-s_i}, v' \textstyle\prod_{j=1}^m v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\ &= \textstyle\prod_S e(g_2^{q(i)}, g)^{\Delta_{i,S}(0)} = A. \end{aligned}$$

If the equality holds, output **valid**; otherwise, output **invalid**.

5 Security proofs

We show security as in Theorem 1, the approach is based on that of [6][9].

Theorem 1 . *Let $\mathcal{A}$ be an adversary that makes at most $l \ll p$ signature queries and produces a successful forgery against our scheme with probability ϵ in time t. Then there exists an algorithm $\mathcal{B}$ that solves the CDH problem in $\mathbb{Z}_p$ with probability $\tilde{\epsilon} \geq \epsilon/(4p^n nl)$ in time $\tilde{t} \approx t$.*

Proof. The simulator $\mathcal{B}$ is given an instance $(g, g^a, g^b) \in \mathbb{G}^3$ of the CDH problem, and must produce g^{ab}. The simulation proceeds as follows:

Setup $\mathcal{B}$ first selects a random identity α^*. Next, $\mathcal{B}$ chooses a random $k \in \{0, ..., m\}$, and random numbers $x', x_1, ..., x_m$ in the interval $\{0, ..., 2l-1\}$. It also chooses additional random exponents $z', z_1, ..., z_m \in \mathbb{Z}_p$. It lets $g_1 = g^a, g_2 = g^b$. It then chooses a random n degree polynomial $f(x)$ and an n degree polynomial $u(x)$ such that $\forall x\ u(x) = -x^n$ if and only if $x \in \alpha$. $\mathcal{B}$ sets $t_i = g_2^{u(i)} g^{f(i)}$ for i from 1 to $n+1$. Since t_i is chosen independently at random, we have $T(i) = g_2^{i^n} \prod_{j=1}^{n+1} (g_2^{u(j)} g^{f(j)})^{\Delta_{j,N}(i)} = g_2^{i^n+u(i)} g^{f(i)}$. The simulator give the public parameters,

$$\mathbf{PP} = (g, g_1, g_2, t_1, ..., t_{n+1}, v' = g_2^{x'-2kl} g^{z'}, (v_j = g_2^{x_j} g^{z_j})_{j=1,...,m}, A = e(g_1, g_2))$$

The corresponding master key, $\mathbf{MK} = a$, is unknown to $\mathcal{B}$.

To answer a private key query on identity γ that $|\gamma \cap \alpha^*| < d$, the simulator $\mathcal{B}$ proceeds as follows. We first define three sets Γ, Γ', S in the following manner:

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

Then we define the private key K_γ for $i \in \Gamma'$ as: $(\{D_i\}_{i\in\Gamma'} = \{g_2^{\lambda_i} T(i)^{r_i}\}_{i\in\Gamma'}, \{d_i\}_{i\in\Gamma'} = \{g^{r_i}\}_{i\in\Gamma'})$, where λ_i, r_i are chosen randomly in $\mathbb{Z}_p$. We define $d-1$ degree polynomial $q(x)$ as $q(i) = \lambda_i, q(0) = a$.

Next we computes the private key K_γ for $i \in \gamma - \Gamma'$ as follows:

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

Since $i \notin \alpha$, $i^n + u(i)$ will be none-zero. We claim that such construction is a valid response to this private key query. To see this, let $r_i = (r_i' - \frac{a}{i^n+u(i)})\Delta_{0,S}(i)$.

Then we have that,

$$\begin{aligned}
D_i &= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_1^{\frac{-f(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i{}'})^{\Delta_{0,S}(i)} \\
&= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g^{\frac{-af(i)}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i{}'})^{\Delta_{0,S}(i)} \\
&= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_2^{a}(g_2^{i^n+u(i)} g^{f(i)})^{\frac{-a}{i^n+u(i)}}(g_2^{i^n+u(i)} g^{f(i)})^{r_i{}'})^{\Delta_{0,S}(i)} \\
&= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)})(g_2^{a}(g_2^{i^n+u(i)} g^{f(i)})^{r_i' - \frac{a}{i^n+u(i)}})^{\Delta_{0,S}(i)} \\
&= (\prod_{j\in\Gamma'} g_2^{\lambda_j \Delta_{j,S}(i)}) g_2^{a\Delta_{0,S}(i)} (T(i))^{r_i} \\
&= g_2^{q(i)} T_i^{r_i} \\
d_i &= (g_1^{\frac{-1}{i^n+u(i)}} g^{r_i'})^{\Delta_{0,S}(i)} = (g^{r_i' - \frac{a}{i^n+u(i)}})^{\Delta_{0,S}(i)}.
\end{aligned}$$

It shows that D_i, d_i have the correct distribution. To answer the signature query on identity γ that $|\gamma \cap \alpha^*| < d$, $\mathcal{B}$ uses K_γ to create a signature on M exactly as in the actual scheme, and outputs the result.

To answer the signature query on identity α^* for some $M = (\mu_1 \cdots \mu_m)$, we define $F = -2kl + x' + \sum_{j=1}^m x_j \mu_j$ and $J = z' + \sum_{j=1}^m z_j \mu_j$. If $F \equiv 0 (mod\ p)$, the simulator aborts. Otherwise, $\mathcal{B}$ selects a random set Λ such that $\Lambda \subset \alpha^*$ and $|\Lambda| = d - 1$ and define $g^{q'(i)} = g^{\lambda_i'}$ for $i \in \Lambda$ where λ_i' is chosen randomly in $\mathbb{Z}_p$. Then it computes $g^{q'(i)} = (\prod_{j=1}^{d-1} g^{\lambda_j' \Delta_{j,\alpha^*}(i)}) g^{a\Delta_{0,\alpha^*}(i)}$ for $i \in \alpha^* - \Lambda$. $\mathcal{B}$ picks random r_i, s_i for $i \in \alpha^*$ and computes,

$$\begin{aligned}
S_1^{(i)} &= (g^{q'(i)})^{-J/F} g^{f(i) r_i} (g^J g_2^F)^{s_i} \\
S_2^{(i)} &= g^{-r_i} \\
S_3^{(i)} &= (g^{q'(i)})^{1/F} g^{-s_i}.
\end{aligned}$$

For $\tilde{s_i} = s_i - q'(i)/F$, we have that,

$$\begin{aligned}
S_1^{(i)} &= (g^{g'(i)})^{-J/F} g^{f(i) r_i} (g^J g_2^F)^{s_i} = (g^{q'(i)})^{-J/F} g^{f(i) r_i} g^{q'(i) J/F} g_2^{q'(i)} (g^J g_2^F)^{s_i - q'(i) F} \\
&= g_2^{q'(i)} g^{f(i) r_i} (g^J g_2^F)^{\tilde{s_i}} = g_2^{q'(i)} T(i)^{r(i)} (v' \prod_{j=1}^m v_j^{\mu_j})^{\tilde{s_i}} \\
S_3^{(i)} &= (g^{q'(i)})^{1/F} g^{-s_i} = (g^{q'(i)})^{1/F} g^{-q'(i)/F} g^{-\tilde{s_i}} = g^{-\tilde{s_i}}.
\end{aligned}$$

It shows that $S_1^{(i)}, S_2^{(i)}, S_3^{(i)}$ have the correct distribution.

Eventually, $\mathcal{A}$ outputs a valid forgery $S^* = (\{S_1^{(i)*}\}_{i\in\alpha}, \{S_2^{(i)*}\}_{i\in\alpha}, \{S_3^{(i)*}\}_{i\in\alpha})$ on M^* where $M^* = (\mu_1^* \cdots \mu_m^*) \in \{0,1\}^m$ for identity α. Let $F^* = -2kl + x' + \sum_{j=1}^m x_j\mu_j^*$ and $J^* = z' + \sum_{j=1}^m z_j\mu_j^*$. If $\alpha \neq \alpha^*$ or if $F^* \not\equiv 0 (\text{mod } p)$, $\mathcal{B}$ aborts. Otherwise, the forgery must be the following form, for some $r_i^*, s_i^* \in \mathbb{Z}_p$,

$$
\begin{aligned}
S_1^{(i)} &= g_2^{q^*(i)} T(i)^{r_i^*} (v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{s_i^*} = g_2^{q^*(i)} g^{f(i)r_i^*} g^{J^* s_i^*} \\
S_2^{(i)} &= g^{-r_i^*} \\
S_3^{(i)} &= g^{-s_i^*}.
\end{aligned}
$$

We select a random set Λ' such that $\Lambda' \subset \alpha$ and $|\Lambda'| = d$, and computes as follows,

$$
\begin{aligned}
S_1^* &= \textstyle\prod_{i\in\Lambda'} (S_1^{(i)})^{\Delta_{i,\alpha}(i)} = \prod_{i\in\Lambda'} (g_2^{\Delta_{i,\alpha}(i)q^*(i)} T(i)^{\Delta_{i,\alpha}(i)r_i^*} (v' \textstyle\prod_{j=1}^m v_j^{\mu_j})^{\Delta_{i,\alpha}(i)s_i^*}) \\
&= \textstyle\prod_{i\in\Lambda'} (g_2^{\Delta_{i,\alpha}(i)q^*(i)} g^{\Delta_{i,\alpha}(i)f(i)r_i^*} g^{\Delta_{i,\alpha}(i)J^* s_i^*}) = g^{ab} \prod_{i\in\Lambda'} (g^{\Delta_{i,\alpha}(i)f(i)r_i^*} g^{\Delta_{i,\alpha}(i)J^* s_i^*}) \\
S_2^* &= \textstyle\prod_{i\in\Lambda'} (S_2^{(i)})^{\Delta_{i,\alpha}(i)f(i)} = \prod_{i\in\Lambda'} g^{-\Delta_{i,\alpha}(i)f(i)r_i^*} \\
S_3^* &= \textstyle\prod_{i\in\Lambda'} (S_3^{(i)})^{\Delta_{i,\alpha}(i)} = \prod_{i\in\Lambda'} g^{-\Delta_{i,\alpha}(i)s_i^*}.
\end{aligned}
$$

$\mathcal{B}$ could solve the CDH instance by outputting $S_1^* \cdot S_2^* \cdot (S_3^*)^{J^*} = g^{ab}$.

$Pr[\text{the simulation not aborting}]$

$= Pr[\alpha = \alpha^*] \cdot Pr[F \not\equiv 0 (\text{mod } p)] \cdot Pr[F^* \equiv 0 (\text{mod } p)]$

$= \frac{1}{p^n} \cdot (1 - \frac{1}{2l}) \cdot \frac{1}{2nl} \leq \frac{1}{4p^n nl}$.

$\tilde{\epsilon} \geq \epsilon \cdot Pr[\text{the simulation not aborting}] \geq \epsilon \cdot \frac{1}{4p^n nl}$. $\square$

6 Acknowledgements

This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 60572155 and 60673079, and the National Research Fund for the Doctoral Program of Higher Education of China under Grant No. 20060248008.

7 Conclusion

In this paper, we first contribute the definition, formalization, and security model of fuzzy identity based signature. We then construct a practical fuzzy identity based signature based on Sahai-Waters construction[6] and the two level hierarchical signature of Boyen and Waters[9]. Finally, We prove that our scheme is existentially unforgeable against adaptively chosen message attack as defined in section 3.2 without random oracles by reducing it to the Chosen Diffie-Hellman assumption.

References

[1] Joonsang Baek, Willy Susilo, Jianying Zhou, New Constructions of Fuzzy Identity-Based Encryption, In ASIACCS 2007, to appear.

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

[3] V. Goyal, O. Pandey, A. Sahai and B. Waters, Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, In ACM CCS ' 06, 2006, to appear.

[4] A. Joux, K. Nguyen, Separating decision Diffie-Hellman from Diffie-Hellman in cryptographic groups, Cryptology ePrint Archive: Report 2001/03

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

[6] A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, Advances in Cryptology - In Eurocrypt 2005, LNCS 3494, pp. 457-473, Springer-Verlag, 2005.

[7] A. Shamir. How to share a secret. Communications of the ACM 22 (11) (1979) 612-613.

[8] A. Shamir, Identity-based cryptosystems and signature schemes, in: G.R. Blakley, D. Chaum (Eds.), Advances in Cryptology - CRYPTO84, LNCS 196, Springer-Verlag, 1985, pp. 47C53.

[9] B. Waters. Efficient identity-based encryption without random oracles. In EUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 114C127. Springer-Verlag, 2005.