Fuzzy Identity-Based Signature
Seminar Biometry & Security WS09/10

Kittipat Virochsiri

January 26, 2010

1 Introduction

A problem in public-key signing schemes is identifying the owner of the key. Traditionally, the key must be signed by an authority in order to verify the validity of the key. To overcome the problem, an identity-based scheme was introduced. An identity-based scheme uses some properties that are unique for each entity in the interested group, e.g., e-mail address, as the public key. Biometrics are natural choices of the public key in this scheme as they are unique to a person. However, in practice, the biometric reads of the same person are usually slightly different from each other. Thus, biometrics cannot be used directly as a key in an identity-based scheme. Fuzzy extractor can derive some consistent properties out of the inconsistent biometric reads. Therefore, biometrics can be indirectly used in the identity-based scheme via fuzzy extractor.

Biometrics could also be directly used as the key if the scheme is error tolerant. Yang et al. [9] proposed a fuzzy identity-based signature scheme, which was a error-tolerant identity-based signature scheme. The work converted the fuzzy identify-based encryption scheme by Sahai and Waters [5] into a signature scheme using the method described in [1], and also incorporated the two level hierarchical signature of Waters [8]. In this scheme, a signature issued by an identity ω could be verified by another identity ω', provided that both identities differ from each other within a certain distance.

Apart form the use in biometric, the fuzzy identity-based signature scheme can also be applied to attribute-based signature [6, 3]. The set of attributes is considered as the identity in the scheme. This allows person with certain attributes to sign messages on behalf of a group, and other people in the group can verify the signature.

2 Preliminaries

This section discuss the foundation of the scheme.

2.1 Bilinear pairing

Let $\mathbb{G}$ and $\mathbb{G}_T$ be multiplicative groups of the same prime order p. A bilinear pairing is a map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the following properties [1, 8, 9]:

1. Bilinear: $e(u^a, v^b) = e(u, v)^{ab}$, where $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy: Let g be a generator of $\mathbb{G}$, $e(g, g) \neq 1$.
3. Computability: It is efficient to compute $e(u, v)$ for all $e, v \in \mathbb{G}$.

This mapping is a building block of the scheme.

2.2 Computational Diffie-Hellman (DH) Assumption

The computational Diffie-Hellman (CDH) problem is the defined as follow [8, 1, 9]. The challenger randomly chooses $a, b \in \mathbb{Z}_p$ and outputs $(g, A = g^a, B = g^b)$. The adversary answers $g^{ab} \in \mathbb{G}$. An adversary, $\mathcal{B}$, has advantage ϵ if

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

where the probability is over the random choice of $a, b \in \mathbb{Z}_p$ and the random bits of $\mathcal{B}$.

The computational (t, ϵ) Diffie-Hellman assumption holds if no t-time adversary has ϵ advantage in solving the above game.

Note that the CDH problem is difficult because obtaining n from g^n is hard. Technically, the problem is the discrete logarithm problem, which is an NP problem [2]. On the other hand, given g and n, computing g^n is easy. There exists an $O(\log n)$ algorithm that solves the problem [4].

2.3 Threshold Secret Sharing Schemes

Shamir [7] introduced secret sharing schemes. A (n, d) threshold secret sharing scheme distributes a secret over the set of n players. A subset of at least d players can recover the secret from their shares of secret. A subset of less than d players has no chance to recover the secret.

Shamir's solution [7] uses polynomial interpolation. Let $GF(p)$ be a finite field with $p \geq n$ elements, $s \in GF(q)$ be the secret to be shared. The dealer randomly chooses a polynomial $f(x)$ of degree $d - 1$, where $f(0) = s$. In other words, $f(x)$ has the form $f(x) = s + \sum_{j=1}^{d-1} a_j x^j$, where $a_1, \ldots, a_{d-1}$ are random numbers chosen from $GF(p)$.

Let $\mathcal{P} = \{R_1, \ldots, R_n\}$ be the set of players. Each player R_i is assigned with a unique field element α_i. The dealer privately sends the secret share $s_i = f(\alpha_i)$ to R_i. A subset of player S where $|S| \geq d$ can 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 $\Delta_{\alpha_i,S}(x)$ is the Lagrange interpolation coefficient, defined as

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

To see this, consider a 1 degree polynomial, i.e., $f(x) = ax + b$. If we know a point on the polynomial, we cannot reconstruct the polynomial. However, if we know a second point, it is enough to reconstruct the polynomial.

3 Definitions

3.1 Fuzzy Identity-Based Signature

The generic fuzzy identity-based signature (FIBS) scheme consists of the following algorithms [9].

- $Setup(1^k)$: 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. The master key mk is kept secret and the public parameters $params$ is made public.
- $Extract(mk, ID)$: The private key extractor algorithm is a probabilistic algorithm that takes as input the master key mk and an identity ID. It outputs a private key associated 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.

Figure 1 depicts the scheme.

3.2 Security Model

Here is the summary of security model described in [9]. Let $\mathcal{A}$ be an adversary assumed to be a probabilistic Turing machine taking as input a security parameter k.

- **Phase 1** $\mathcal{A}$ issues private key queries and signature queries for any identities.
- **Phase 2** $\mathcal{A}$ declares the target identity α which is considered different from identities in Phase 1.

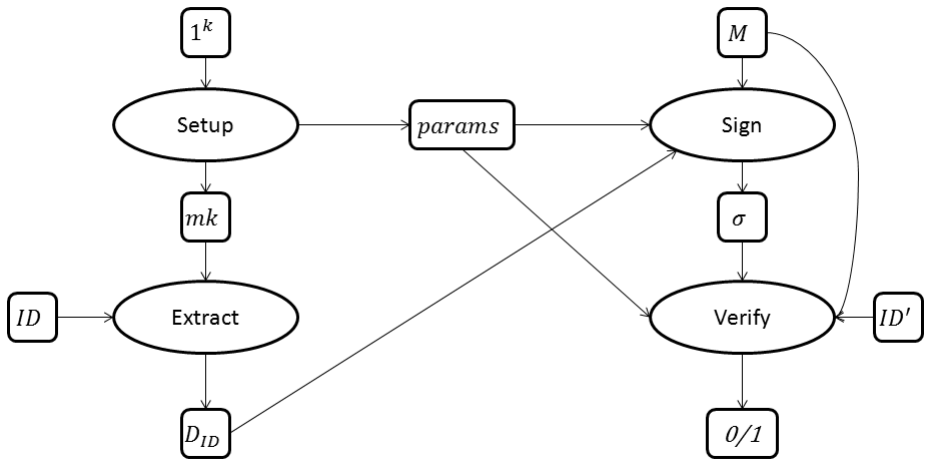

Figure 1: Fuzzy identity-based signature scheme

- **Phase 3** $\mathcal{A}$ issues private key queries for many identities γ_i which is considered different from the target identity. $\mathcal{A}$ issues signature queries for any identities.
- **Phase 4** $\mathcal{A}$ outputs σ^* which is α's valid signature on the message M^* and $\mathcal{A}$ does not make a signature query on M^* for identity α.

Figure 2 depicts the game.

Yang et al. [9] defined $\mathcal{A}$'s success probability as

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

The fuzzy identity-based signature scheme FIBS is said to be unforgeable FIBS chosen message attack (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

Here is the scheme presented in [9]. Let $\mathbb{G}$ and $\mathbb{G}_T$ be multiplicative groups of prime order p such that a bilinear pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ can be constructed, and g be a generator of $\mathbb{G}$. Identities are set of n elements of $\mathbb{Z}_p^*$.

4.1 $Setup(n, d)$

Choose the master key $MK = y$ from $\mathbb{Z}_p$. Set $g_1 = g^y$. Choose $g_2 \in \mathbb{G}$. Choose $t_1, \ldots, t_{n+1}$ uniformly at random from $\mathbb{G}$. Let N be the set $\{1, \ldots, n+1\}$.

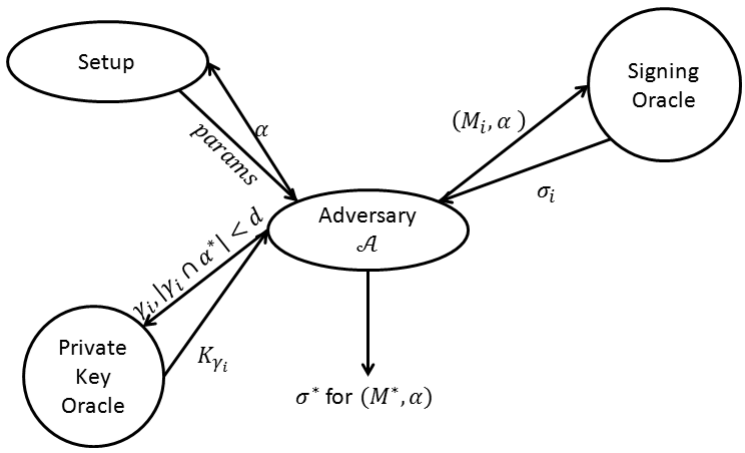

Figure 2: Security model

Define a function, T, as:

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

Select a random integer $z' \in \mathbb{Z}_p$ and a random vector $\overrightarrow{z} = (z_1, \ldots, z_m) \in \mathbb{Z}_p^m$, where m is the length of the longest bit string.

The public parameters PP is given by

$$PP = (g_1, g_2, t_1, \ldots, t_{n+1}, v' = g^{z'}, v_1 = g^{z_1}, \ldots, v_m = g^{z_m}, A = e(g_1, g_2)) \in \mathbb{G}^{n+m+4} \times \mathbb{G}_T.$$

4.2 $Extract(PP, MK, \omega)$

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

$$\begin{aligned} D_i &= g_2^{q(i)} T9i)^{r_i}, \\ d_i &= g^{-r_i}, \end{aligned}$$

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

4.3 $Sign(PP, K_\omega, M)$

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_ω, select a random $s_i \in \mathbb{Z}_p$ for each $i \in \omega$ and

output

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

4.4 $Verify(PP, \omega', M, \sigma)$

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 $M = (\mu_1 \cdots \mu_m) \in \{0,1\}^m$, choose an arbitrary d-element subset S of $\omega' \cap \omega$ and verify that

$$
\prod_S (e(S_1^{(i)}, g) \cdot e(S_2^{(i)}, T(i)) \cdot e(S_3^{(i)}, v' \prod_{j=1}^{m} v_j^{\mu_j}))^{\Delta_{i,S}(0)} = A.
$$

If the equality holds, output valid; otherwise, output invalid. This is correct because

$$
\begin{aligned}
& \prod_S (e(S_1^{(i)}, g) \cdot e(S_2^{(i)}, T(i)) \cdot e(S_3^{(i)}, v' \prod_{j=1}^{m} v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\
= & \prod_S (e(g_2^{q(i)} \cdot T(i)^{r_i} \cdot (v' \prod_{j=1}^{m} v_j^{\mu_j})^{s_i}, g) \cdot e(g^{-r_i}, T(i)) \cdot e(g^{-s_i}, v' \prod_{j=1}^{m} v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\
= & \prod_S (e(g_2^{q(i)}, g) \cdot e(T(i)^{r_i}, g) \cdot e((v' \prod_{j=1}^{m} v_j^{\mu_j})^{s_i}, g) \cdot e(g^{-r_i}, T(i)) \cdot e(g^{-s_i}, v' \prod_{j=1}^{m} v_j^{\mu_j}))^{\Delta_{i,S}(0)} \\
= & \prod_S (e(g_2^{q(i)}, g))^{\Delta_{i,S}(0)} \\
= & e(g_2, g^{\Sigma_S \Delta_{i,S}(0) q(i)}) \\
= & e(g_2, g^y) \\
= & e(g_2, g_1) \\
= & e(g_1, g_2) \\
= & A.
\end{aligned}
$$

5 Security Proofs

Yang et al. [9] provided a security proof for the fuzzy identity-based signature scheme. The proof demonstrated how a simulator could be constructed to solve the CDH problem. However, the claim regarding the probability of solving the problem was unsound. Shahandashti and Safavi-Naini [6] proposed a similar scheme. However, they only claimed that their scheme is secure (under a model) if the CDH is hard.

To solve an instances $(g, g^a, g^b) \in \mathbb{G}^3$ of the CDH problem, a simulator, $\mathcal{B}$, proceeds as follow.

Setup First of all, $\mathcal{B}$ selects a random identity α^*. $\mathcal{B}$ lets $g_1 = g^a$ and $g_2 = g^b$. Then, $\mathcal{B}$ chooses a random $k \in \{0, \ldots, m\}$, random numbers $x', x_1, \ldots, x_m$ in the interval $\{0, \ldots, 2l-1\}$, and random exponents $z', z_1, \ldots, z_m \in \mathbb{Z}_p$. $\mathcal{B}$ 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 $n+1$. Function $T(i)$ is defined as $T(i) = g_2^{i^n} \prod_{j=1}^{n+1} (g_2^{u(j)} g^{f(i)})^{\Delta_{j,N}(i)} = g_2^{i^n + u(i)} g^{f(i)}$. $\mathcal{B}$ give the public parameters,

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

Note that the corresponding master key, a, is unknown to $\mathcal{B}$.

To answer a private key query on an identity γ that $|\gamma \cap \alpha *| < d$, the simulator $\mathcal{B}$ proceeds as follow. $\mathcal{B}$ defines three sets – Γ, Γ', and S – such that $\Gamma = \gamma \cap \alpha$, $\Gamma \subseteq \Gamma' \subseteq \gamma$, $|\Gamma'| = d-1$, and $S = \Gamma' \cup \{0\}$. The elements of private key K_γ are defined in two manners.

For $i \in \Gamma'$,

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

where λ_i and r_i are chosen randomly in $\mathbb{Z}_p$.

For $i \in \gamma - \Gamma'$,

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

where λ_j and r_i are defined in the same manner as the previous case.

A $d-1$ degree polynomial $q(x)$ is defined as $q(i) = \lambda_i, q(0) = a$. In the latter case, since $i \notin \alpha$, $i^n + u(i)$ will be non-zero. To see that this is valid response to

the private key query, let $r_i = (r'_i - \frac{a}{i^n+u(i)})^{\Delta_{0,S}(i)}$. Then, it can be shown that,

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

It shows that D_i and d_i have the correct distribution. To answer the signature query on identity γ such 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 $\alpha^*$for some $M = (\mu_1 \cdots \mu_m)$, for the ease of proof, F and J are defined as $F = -2kl + x' + \Sigma_{j=1}^m x_j\mu_j$ and $J = z' + \Sigma_{j=1}^m z_j\mu_j$. If $F \equiv 0(mod p)$, the simulation aborts. Otherwise, $\mathcal{B}$ selects a random set Λ such that $\Lambda \subset \alpha^*$ and $|\Lambda| = d-1$. A function $q'(i)$ is defined as:

$$q'(i) = \begin{cases} \lambda'_i & i \in \Lambda \\ a\Delta_{0,\alpha^*}(i) + \Sigma_{j=1}^{d-1}\lambda'_j\Delta_{j,\alpha^*}(i) & i \in \alpha^* - \Lambda \end{cases}.$$

$\mathcal{B}$ then 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 $\tilde{s_i} = s_i - q'9i)/F$, it can be shown that,

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

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

To produce a valid forgery $S^* = (\{S_1^{(i)}\}_{i\in\alpha}, \{S_2^{(i)}\}_{i\in\alpha}, \{S_3^{(i)}\}_{i\in\alpha}\}$ on $M* = (\mu_1^* \ldots \mu_m^*) \in \{0,1\}^m$ for identity α. Let $F^* = -2kl + x' + \Sigma_{j=1}^m x_j \mu_j^*$ and $J^* = z' + \Sigma_{j=1}^m z_j \mu_j^*$. If $\alpha \neq \alpha^*$ or $F^* \not\equiv 0(mod\, p)$, $\mathcal{B}$ aborts. Otherwise, $\mathcal{A}$ produces the forgery in the following form, for some $r_i^* s_i^* \in \mathbb{Z}_p$, $q^*(i)$ is defined in the same manner as $q'(i)$,

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

The condition $F \equiv 0(mod\, p)$ is necessary to show that

$$\begin{aligned}
S_1^{(i)} &= g_2^{q^*(i)} T(i)^{r_i^*} (v' \prod_{j=1}^{m} v_j^{\mu_j})^{s_i^*} \\
&= g_2^{q^*(i)} T(i)^{r_i^*} (g_2^{x'-2kl} g^{z'} \prod_{j=1}^{m} (g_2^{x_j} g^{z_j})^{\mu_j})^{s_i^*} \\
&= g_2^{q^*(i)} T(i)^{r_i^*} (g_2^{x'-2kl} g^{z'} (g_2^{\Sigma_{j=1}^m x_j \mu_j} g^{\Sigma_{j=1}^m z_j \mu_j}))^{s_i^*} \\
&= g_2^{q^*(i)} T(i)^{r_i^*} (g_2^{x'-2kl+\Sigma_{j=1}^m x_j \mu_j} g^{z'+\Sigma_{j=1}^m z_j \mu_j})^{s_i^*} \\
&= g_2^{q^*(i)} T(i)^{r_i^*} (g_2^{F^*} g^{J^*})^{s_i^*} \\
&= g_2^{q^*(i)} g^{f(i)r_i^*} g^{J^* s_i^*}.
\end{aligned}$$

To solve the CDH instance, $\mathcal{B}$ selects a random set Λ' such that $\Lambda' \subset \alpha$

and $|\Lambda'| = d$, and computes as follow,

$$\begin{aligned}
S_1^* &= \prod_{i\in\Lambda'} (S_1^{(i)})^{\Delta_{i,\alpha}(i)} \\
&= \prod_{i\in\Lambda'} (g_2^{q^*(i)} g^{f(i)r_i^*} g^{J^* s_i^*})^{\Delta_{i,\alpha}(i)} \\
&= \prod_{i\in\Lambda'} (g_2^{\Delta_{i,\alpha}(i)q^*(i)} g^{\Delta_{i,\alpha}(i)f(i)r_i^*} g^{\Delta_{i,\alpha}(i)J^* s_i^*}) \\
&= g_2^a \prod_{i\in\Lambda'} (g^{\Delta_{i,\alpha}(i)f(i)r_i^*} g^{\Delta_{i,\alpha}(i)J^* s_i^*}) \\
&= g^{ab} \prod_{i\in\Lambda'} (g^{\Delta_{i,\alpha}(i)f(i)r_i^*} g^{\Delta_{i,\alpha}(i)J^* s_i^*}) \\
S_2^* &= \prod_{i\in\Lambda'} (S_2^{(i)})^{\Delta_{i,\alpha}(i)f(i)} \\
&= \prod_{i\in\Lambda'} g^{-\Delta_{i,\alpha}(i)f(i)r_i^*} \\
S_3^* &= \prod_{i\in\Lambda'} (S_3^{(i)})^{\Delta_{i,\alpha}(i)} \\
&= \prod_{i\in\Lambda'} g^{-\Delta_{i,\alpha}(i)s_i^*}.
\end{aligned}$$

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

However, Yang et al. [9] failed to prove the probability of solving the CDH problem if the scheme can be broken. Others [6, 3] presented similar schemes but did not provide detailed analysis either.

6 Conclusion

Yang et al. [9] presented an fuzzy identity-based signature scheme which was a derivative of fuzzy identity-based encryption [5] and two level hierarchical signature [8]. In this scheme, a signature on a message M signed by an identity ω could be verified by another identity ω', if the two identities overlap each other beyond a certain threshold. This scheme is secure against chosen message attack if the computational Diffie-Hellman problem is hard. This scheme does not provided privacy to the signer [3, 6]. Moreover, in this scheme, the private key must be issued under the control of a well-trained operator.

References

[1] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229, London, UK, 2001. Springer-Verlag.

[2] David S. Johnson. The np-completeness column: An ongoing guide. *Journal of Algorithms*, 7(4):584 – 601, 1986.

[3] Jin Li and Kwangjo Kim. Attribute-based ring signatures. Cryptology ePrint Archive, Report 2008/394, 2008.

[4] Peter L. Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, 1987.

[5] Amit Sahai and Brent Waters. Fuzzy Identity-Based encryption. In *Advances in Cryptology - EUROCRYPT 2005*, pages 457–473. 2005.

[6] Siamak F Shahandashti and Reihaneh Safavi-Naini. Threshold attribute-based signatures and their application to anonymous credential systems. Cryptology ePrint Archive, Report 2009/126, 2009.

[7] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[8] Brent Waters. Efficient Identity-Based encryption without random oracles. In *Advances in Cryptology - EUROCRYPT 2005*, pages 114–127. 2005.

[9] Piyi Yang, Zhenfu Cao, and Xiaolei Dong. Fuzzy identity based signature. Cryptology ePrint Archive, Report 2008/002, 2008.