Neyire Deniz Sarier (2008). A New Biometric Identity Based Encryption Scheme. In *Technical Sessions for 2008 International Symposium on Trusted Computing (TrustCom 2008)* in *Proceedings of the 9th International Conference for Young Computer Scientists, ICYCS 2008, Zhang Jia Jie, Hunan, China, November 18-21, 2008*, Guojun Wang, Jianer Chen, Michael R. Fellows & Huadong Ma, editors, 2061–2066. IEEE Computer Society. ISBN 978-0-7695-3398-8. URL https://dx.doi.org/10.1109/ICYCS.2008.420

A New Biometric Identity Based Encryption Scheme

Neyire Deniz Sarier

Bonn-Aachen International Center for Information Technology
Computer Security Group
Dahlmannstr. 2, D-53113 Bonn Germany
denizsarier@yahoo.com

Abstract

In this paper, we present a new and efficient biometric identity based encryption scheme (BIO-IBE) using the Sakai-Kasahara Key Construction and prove its security in the random oracle model based on the well-exploited k-BDHI computational problem. Our new scheme achieves better efficiency in terms of the key generation and decryption algorithms compared to the existing fuzzy IBE schemes. The main difference of the new BIO-IBE scheme is the structure of the key generation algorithm, where a unique biometric identity string ID obtained from the biometric attributes is used instead of picking a different polynomial for each user as in other fuzzy IBE schemes.

Keywords: Biometrics, fuzzy IBE, fuzzy extraction.

1. Introduction

Recently, Sahai and Waters proposed a new Identity Based Encryption (IBE) system called fuzzy IBE that uses biometric attributes as the identity instead of an arbitrary string like an email address. In fuzzy IBE, the private key components are generated by combining the values of a unique polynomial on each attribute with the master secret key. However, due to the noisy nature of biometrics, fuzzy IBE allows for error tolerance in the decryption stage, where a ciphertext encrypted with the biometrics w could be decrypted by the receiver using the private key corresponding to the identity w', provided that w and w' are within a certain distance of each other. Besides, the biometrics is used as public information, hence the compromise of the biometrics does not affect the security of the system.

1.1. Related Work

The first fuzzy IBE scheme is described by Sahai and Waters in [11] and the security is reduced to the MBDH problem in the standard model, where the size of the public parameters is linear in the number of the attributes of the system or the number of attributes of a user. Piretti et al [10] achieved a more efficient fuzzy IBE scheme with short public parameter size by using the random oracle model (ROM). Baek et al [1] described two new fuzzy IBE schemes with an efficient key generation algorithm and proved the security in the random oracle model based on the DBDH assumption. Besides, Burnett et al [4] described a biometric identity based signature scheme, where they used the biometric information as the identity and construct the public key of the user using a fuzzy extractor [8], which is then used in the modified SOK-IBS scheme [2].

1.2. Our Contribution

In this paper, we present a new biometric identity based encryption scheme using the Sakai Kasahara Key Construction [6] and achieve better efficiency compared to the existing fuzzy IBE schemes in terms of the key generation and decryption algorithms. First, we have a structurally simpler key generation algorithm compared to [10, 1] since we use an ordinary one-way hash function instead of a MaptoPoint hash function and we reduce the number of exponentiations in the group $\mathbb{G}$ from $3n$ as in [10] (and from $2n$ as in [1]) to n. Also, the decryption algorithm requires d bilinear pairing computations and d exponentiations, whereas the existing schemes require $d+1$ bilinear pairing computations and $2d$ exponentiations. The security of our new scheme reduces to the well exploited k-BDHI computational problem in the random oracle model. The main difference of our biometric IBE scheme is the structure of the key generation algorithm, where a unique biometric identity string ID obtained from the biometric attributes is used instead of picking a different polynomial for each user and computing the private key components for each attribute using this polynomial, the master key and the attributes. Thus, our scheme is constructed using a different approach compared to the existing fuzzy IBE schemes.

2. Definitions and Building Blocks

In order to introduce the new biometric IBE scheme, at first, we review the definitions and required computational primitives. Given a set S, $x \overset{\text{R}}{\leftarrow} S$ defines the assignment of a uniformly distributed random element from the set S to the variable x. A function $\epsilon(k)$ is defined as negligible if for any constant c, there exists $k_0 \in N$ with $k > k_0$ such that $\epsilon < (1/k)^c$. Finally, we define the Lagrange coefficient $\Delta_{\mu_i,S}$ for $\mu_i \in \mathbb{Z}_p$ and a set S of elements in $\mathbb{Z}_p$ as

$$\Delta_{\mu_i,S}(x) = \prod_{\mu_j \in S, \mu_j \neq \mu_i} \frac{x - \mu_j}{\mu_i - \mu_j}$$

Definition 2.1. Bilinear Pairing

Let $\mathbb{G}$ and $\mathbb{F}$ be multiplicative groups of prime order p and let g be a generator of $\mathbb{G}$. $\mathbb{Z}_p^*$ denotes $\mathbb{Z}_p \setminus \{0\}$ and $\mathbb{G}^*$ denotes $\mathbb{G} \setminus \{1\}$, where $\{0\}$ and $\{1\}$ are the identity elements of $\mathbb{Z}_p$ and $\mathbb{G}$, respectively. A bilinear pairing is denoted by $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$ if the following two conditions hold.

1. *$\forall\, a, b \in \mathbb{Z}_p$, we have $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$*
2. *$\hat{e}(g, g) \neq 1$, namely the pairing is non-degenerate.*

The security of our scheme is reduced to the well-exploited complexity assumption (k-BDHI) [6], which is stated as follows.

Definition 2.2. k-Bilinear Diffie-Hellman Inverse (k-BDHI)

For an integer k, and $x \overset{\text{R}}{\leftarrow} \mathbb{Z}_p^*$, $g \in \mathbb{G}^*$, $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$, given $(g, g^x, g^{x^2}, ..., g^{x^k})$, computing $\hat{e}(g, g)^{1/x}$ is hard.

2.1. Fuzzy Identity Based Encryption

In [1], the generic fuzzy IBE scheme is defined as follows.

- Setup(): Given a security parameter k_0, the Private Key Generator (PKG) generates the master secret key ms and the public parameters of the system.
- Key Generation: Given a user's identity and ms, the PKG returns the corresponding private key D_{ID}.
- Encrypt: A probabilistic algorithm that takes as input an identity $w' \in U$, public parameters and a message $m \in M$ and outputs the ciphertext $c \in C$. Here, M, C and U denote the message space, the ciphertext space and the universe of attributes.
- Decrypt: A deterministic algorithm that given the private key D^{ID} and a ciphertext encrypted with w' such that $|w \cap w'| \geq d$, returns either the underlying message m or a reject message. Here d is the error tolerance parameter of the scheme.

In our new biometric IBE scheme, the identity is equal to the biometric information of the user, from which the key generation algorithm obtains the biometric features (or attributes) w and a unique biometric identity string ID. The details of this extraction process is presented in section 2.3.

2.2. Security Model

In [11], the Selective-ID model of security for fuzzy IBE (IND-FSID-CPA) is defined using a game between a challenger and an adversary as follows.

- *Phase 1*: The adversary declares the challenge identity $w^* = (\mu_1^*, ..., \mu_n^*)$.
- *Phase 2*: The challenger runs the Setup algorithm and returns to the adversary the system parameters.
- *Phase 3*: The adversary issues private key queries for any identity w' such that $|w' \cap w^*| < d$.
- *Phase 4*: The adversary sends two equal length messages m_0 and m_1. The challenger returns the ciphertext that is encrypted using the identity w^* and the message m_β, where $\beta \overset{\text{R}}{\leftarrow} \{0, 1\}$.
- *Phase 5*: Phase 3 is repeated.
- *Phase 6*: The adversary outputs a guess β' for β.

The advantage of the adversary A is defined as

$$\text{Adv}_A^{IND-FSID-CPA} = |Pr[\beta' = \beta] - \tfrac{1}{2}|$$

For our biometric IBE scheme we give the security proof based on the notion of IND-FSID-CPA (Indistinguishability against Fuzzy Selective Identity, Chosen Plaintext Attack), but our scheme can easily be modified using the generic construction REACT [9] to be secure against CCA (Chosen Ciphertext Attack).

2.3. Biometric Fuzzy Extraction

Any biometric based encryption or signature scheme requires the biometric measurement of the receiver or the signer, respectively. Basically, the framework for biometric encryption is (1) extracting features; (2) quantization and coding per feature and concatenating the output codes; (3) applying error correction coding (ECC) and hashing [5]. After capturing the biometric information of the user through a reading device, feature extraction is applied to obtain the feature vector (or the attributes) of the biometrics. In [11, 1], each attribute is associated with a unique integer $\mu_i \in \mathbb{Z}_p^*$ using a hash function and used as the identity $w = (\mu_1, ..., \mu_n)$ in the fuzzy IBE scheme. Here, n denotes the size of the attributes of each user. Since some of the attributes could be common in some users, a unique polynomial is selected for each user and included in the key generation algorithm to bind the private key to the user. This way, different users cannot collude in order to decrypt a ciphertext that should be only decrypted by the real receiver.

In our biometric IBE scheme, we use the biometric template b of the user, which is obtained by concatenating the extracted features, in order to bind the private key to the user's identity and thus avoid collusion attacks. Instead of choosing a unique polynomial for each user, we use a fuzzy extractor to obtain a unique string ID via error correction codes from the biometric template b of the user in such a way that an error tolerance t is allowed. In other words, we will obtain the same string ID even if the fuzzy extractor is applied on a different b' such that $dis(b, b') < t$. Here, $dis()$ is the distance metric used to measure the variation in the biometric reading and t is the error tolerance parameter.

Formally, an $(\mathcal{M}, l, t)$ fuzzy extractor is defined as follows.

Definition 2.3. *Let $\mathcal{M} = \{0,1\}^v$ be a finite dimensional metric space with a distance function* **dis** $: \mathcal{M} \times \mathcal{M} \to \mathbb{Z}^+$. *Here, $b \in \mathcal{M}$ and* **dis** *measures the distance between b and b', where $b, b' \in \mathcal{M}$. An $(\mathcal{M}, l, t)$ fuzzy extractor consists of two functions* **Gen** *and* **Rep**.

- **Gen***: A probabilistic generation procedure that takes as input $b \in \mathcal{M}$ and outputs an identity string $ID \in \{0,1\}^l$ and a public parameter PAR, that is used by the* **Rep** *function to regenerate the same string ID from b' such that* **dis**$(b, b') \leq t$.

- **Rep***: A deterministic reproduction procedure that takes as input b' and the publicly available parameter PAR, and outputs ID if* **dis**$(b, b') \leq t$.

In [4], the authors describe a concrete fuzzy extractor using a $[n, k, 2t+1]$ BCH error correction code, Hamming Distance metric and a one-way hash function $H : \{0,1\}^n \to \{0,1\}^l$. Specifically,

- The **Gen** function takes the biometrics b as input and returns $ID = H(b)$ and public parameter $PAR = b \oplus C_e(ID)$, where C_e is a one-to-one encoding function.

- The **Rep** function takes a biometric b' and PAR as input and computes $ID' = C_d(b' \oplus PAR) = C_d(b \oplus b' \oplus C_e(ID))$. $ID = ID'$ if and only if **dis**$(b, b') \leq t$. Here C_d is the decoding function that corrects the errors upto the threshold t.

3. A New Efficient Biometric IBE Scheme

Our new biometric IBE scheme BIO-IBE uses Sakai-Kasahara's Key Construction [6, 12] for the generation of the private keys. This way, BIO-IBE achieves better performance over existing fuzzy IBE schemes due to the use of an ordinary hash function and due the total number of exponentiations and bilinear pairings required. Besides, the fuzzy extraction process is only performed by the sender to form the ciphertext and can be efficiently implemented on the finite field $\mathbb{F}_{2^m}$, where $m \approx 10$ as described in [4, 8]. In order to encrypt a message, the sender obtains the biometric information and the corresponding public parameter PAR of the receiver, extracts the features (attributes) and computes the biometric string ID using the fuzzy extractor. We assume that if $|w \cap w'| \geq d$, then we have **dis**$(b, b') \leq t$ and thus $ID = ID'$. The details of BIO-IBE is presented as follows.

- Setup(): Given a security parameter k_0, the parameters of the scheme are generated as follows.

    1. Generate two cyclic groups $\mathbb{G}$ and $\mathbb{F}$ of prime order $p > 2^{k_0}$ and a bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{F}$. Pick a random generator $g \in \mathbb{G}$.
    2. Pick a random $x \in \mathbb{Z}_p^*$ and compute $P_{pub} = g^x$.
    3. Pick two cryptographic hash functions $H_1 : \mathbb{Z}_p^* \times \{0,1\}^* \to \mathbb{Z}_p^*$ and $H_2 : \mathbb{F} \to \{0,1\}^{k_1}$. In addition, the PKG picks $H : b \to \{0,1\}^*$, an encoding function C_e and a decoding function C_d together with a specific feature extraction method F_e applied on the biometric b.

  The message space is $M = \{0,1\}^{k_1}$. The ciphertext space is $C = U \times \mathbb{G}^n \times \{0,1\}^{k_1}$. The master public key is $(p, \mathbb{G}, \mathbb{F}, \hat{e}, k_1, g, P_{pub}, H_1, H_2, H, C_e, C_d, F_e)$ and the master secret key is $ms = x$.

- Key Generation: First, a user's biometric attributes $w \in U$ are obtained from the raw biometric information using a reader and the feature extractor F_e and each attribute $\mu_i \in w$ is associated to a unique integer in $\mathbb{Z}_p^*$ as in [11]. Besides, the identity string $ID = H(b)$ is calculated from the biometric template b (which is composed of the μ_i's) using a fuzzy extractor as in [4]. Given a user's biometric attributes w and ID, the PKG returns $D_{\mu_i}^{ID} = g^{1/(x+H_1(\mu_i, ID))} = g^{1/(x+h_i^{ID})}$ for each $\mu_i \in w$.

- Encrypt: The sender obtains a biometric reading of the receiver together with the associated public parameter PAR, extracts the feature vector w' and computes $ID' =$ **Rep**(b', PAR). Here, if **dis**$((b, b') < t$, then $ID = ID'$. Given a plaintext $m \in M$, ID' and w', the following steps are performed.

    1. Pick a random polynomial $r(\cdot)$ of degree $d-1$ over $\mathbb{Z}_p$ such that $r(0) = r$ and compute the shares $r(\mu_i) = r_i \in \mathbb{Z}_p$ for $\mu_i \in w'$.

    2. Compute $L_i = P_{pub} \cdot g^{H_1(\mu_i, ID')} = g^{x+h_i^{ID'}}$ and the session key $V = H_2(\hat{e}(g,g)^r)$.
    3. Set the ciphertext to $c' = (w', U_i, W) = (w', L_i^{r_i}, m \oplus V)$ for each $i \in [1,n]$.

- Decrypt: Given $c' = (w', U_i, W) \in C$ and $D_{\mu_i}^{ID}$ for $\mu_i \in w$ and $i \in [1,n]$, choose an arbitrary set $S \subseteq w \cap w'$ such that $|S| = d$ and compute $m = W \oplus V$ as

$$\begin{aligned} V &= H_2(\prod_{\mu_i \in S} (\hat{e}(U_i, D_{\mu_i}^{ID}))^{\Delta_{\mu_i,S}(0)}) \\ &= H_2(\prod_{\mu_i \in S} (\hat{e}(g^{r_i(x+h_i^{ID'})}, g^{1/(x+h_i^{ID})}))^{\Delta_{\mu_i,S}(0)}) \\ &= H_2(\prod_{\mu_i \in S} (\hat{e}(g,g)^{r_i})^{\Delta_{\mu_i,S}(0)}) \\ &= H_2(\hat{e}(g,g)^r) \end{aligned}$$

Here, the polynomial $r(\cdot)$ of degree $d-1$ is interpolated using d points by polynomial interpolation in the exponents using Shamir's secret sharing method [13].
Also, $h_i^{ID'} = h_i^{ID}$ for each $\mu_i \in S$ and $ID = ID'$.

Theorem 3.1. *Suppose the hash functions H_1, H_2 are random oracles and there exists a polynomial time adversary A with advantage ϵ that can break the scheme BIO-IBE in the Fuzzy Selective ID model by making q_1, q_2 random oracle queries, and q_{ex} private key extraction queries. Then there exists a polynomial time algorithm B that solves the k-BDHI problem with $k = q_1 + q_{ex} + 1$.*

Proof. Assume that a polynomial time attacker A breaks BIO-IBE, then using A, we show that one can construct an attacker B solving the k-BDHI problem.

Suppose that B is given the k-BDHI problem $(q, g, \hat{e}, \mathbb{G}, \mathbb{F}, g^x, g^{x^2}, ..., g^{x^k})$, B will compute $\hat{e}(g,g)^{1/x}$ using A as follows.

- ***Phase 1***: A outputs the challenge identity w^*.
- ***Phase 2***: B simulates the public parameters for A.
    1. B selects $h_0, ..., h_{k-1} \in \mathbb{Z}_p^*$ and sets $f(z) = \prod_{j=1}^{k-1}(z+h_j)$, which could be written as $f(z) = \sum_{j=0}^{k-1} c_j z^j$. The constant term c_0 is non-zero because $h_j \neq 0$ and c_j are computable from h_j.
    2. B computes $Q = \prod_{j=0}^{k-1}(g^{x^j})^{c_j} = g^{f(x)}$ and $Q^x = g^{xf(x)} = \prod_{j=0}^{k-1}(g^{x^{j+1}})^{c_j}$.
    If $Q = 1$, then $x = -h_j$ for some j, then k-BDHI problem could be solved directly [7].
    3. B computes $f_j(z) = \frac{f(z)}{z+h_j} = \sum_{v=0}^{k-2} d_{j,v} z^j$ for $1 \leq j < k$ and $Q^{1/(x+h_j)} = g^{f_j(x)} = \prod_{v=0}^{k-2}(g^{x^v})^{d_{j,v}}$ [7].
    4. Set $T' = \prod_{j=1}^{k-1}(g^{x^{j-1}})^{c_j} = g^{(f(x)-c_0)/x}$ and set $T_0 = \hat{e}(T', Q \cdot g^{c_0})$.

    B returns A the public parameters $(q, g, \hat{e}, \mathbb{G}, \mathbb{F}, P_{pub}, H_1, H_2, d, FE)$, where $d \in \mathbb{Z}^+$, $P_{pub} = Q^{x-h_0}$ and H_1, H_2 are random oracles controlled by B as follows. Here, FE denotes the fuzzy extraction algorithm.

    H_1**-queries**: For a query (μ_i, ID^w), where $i \in [1,n]$, if there exists $\langle j, l, \mu_i, ID^w, h_j + h_0, Q^{1/(x+h_j)} \rangle$ in H_1List, return $h_j + h_0$. Otherwise,

    1. If $\mu_i \in w^*$, $ID^w = ID^*$ and $l \neq d$, return $h_j + h_0$ and add $\langle j, l, \mu_i, ID^*, h_j + h_0, Q^{1/(x+h_j)} \rangle$ to H_1List. Increment j and l by 1.
    2. If $\mu_i \in w^*$, $ID^w = ID^*$ and $l = d$, then return h_0, add the tuple $\langle j, d, \mu^*, ID^{w^*}, h_0, \perp \rangle$ to H_1List. Increment j by 1.
    3. Else, return $h_j + h_0$ and add the tuple $\langle j, l, \mu_i, ID^w, h_j + h_0, Q^{1/(x+h_j)} \rangle$ to H_1List. Increment j by 1.

    Here, j and l denotes the values of two counters, where $1 \leq j \leq q_1$ and $1 \leq l \leq d$.

    H_2**-queries**: Upon receiving a query R,

    1. If there exists (R, ξ) in H_2List, return ξ. Else,
    2. Choose $\xi \xleftarrow{R} \{0,1\}^{k_1}$ and return to A.

- ***Phase 3***: B simulates the private key extraction queries of A as follows.

    Extraction queries: Upon receiving a query (w, ID^w) with $|w \cap w^*| < d$, (thus $ID^w \neq ID^*$), for every $\mu_i \in w$, run the H_1-oracle simulator and obtain $\langle j, l, \mu_i, ID^w, h_j + h_0, Q^{1/(x+h_j)} \rangle$ from H_1List. If $ID^w \neq ID^*$, return $D_{\mu_i}^{ID^w} = Q^{1/(x+h_j)}$ for each $\mu_i \in w$.

    Remark 3.1. *To improve the reduction cost, we can add the following condition to the extraction queries: If the extraction query is on the challenge identity $ID^w = ID^*$, (namely $|w \cap w^*| \geq d$), A is given the first $d-1$ private key components $D_{\mu_i}^{ID^*} = Q^{1/(x+h_j)}$ upto the case when $\mu_i = \mu^*$, which is the d^{th} entry in the H_1List with respect to the second counter. Then, we slightly change the security model of our scheme by requiring the adversary A to select the arbitrary subset S of w^* for the computation of the session key such that $\mu^* \in S$ with $|S| = d$.*

- ***Phase 4***: Upon receiving the messages (m_0, m_1) with $|m_0| = |m_1|$, B generates the challenge C^*.

    1. Pick $r_i \xleftarrow{R} \mathbb{Z}_p$ for each $\mu_i \in w^*$ unless $\mu_i = \mu^*$.

2. Compute $U_{\mu_i} = Q^{r_i(x+H_1(\mu_i, ID^*))}$ for each $\mu_i \in w^*$ except for $\mu_i = \mu^*$.
3. Pick $r^* \xleftarrow{\text{R}} \mathbb{Z}_p$ and compute $U_{\mu^*} = Q^{r^*}$.
4. B chooses $\beta \in \{0, 1\}$ and $W^* \xleftarrow{\text{R}} \{0, 1\}^{k_1}$.
5. Set the ciphertext to $C^* = (w^*, U_{\mu_i}, m_\beta \oplus W^*)$ where $\mu_i \in w^*$.

Remark 3.2. *If the condition in Remark 3.1 is applied, then the only way for the adversary A to have any advantage is to query the H_2 oracle with the correct session key constructed using the d private key components, where A already knows $d-1$ of them except for μ^*. And A has to compute the private key share of μ^* due to the Remark 3.1.*

- ***Phase 5***: B answers A's random oracle and private key extraction queries as before. The only condition on the private key extraction queries is that the attacker A cannot query the private key $D_{\mu^*}^{ID^*}$.
- ***Phase 6***: At some point, A responds with its guess β' for the underlying plaintext m_β, which could only be computed from

$$m_\beta = W^* \oplus H_2(\textstyle\prod_{\mu_i \in S}(\hat{e}(U_{\mu_i}, D_{\mu_i}^{ID^*}))).$$

The only way for A to have any advantage in this game is when H_2List contains the value

$$\begin{aligned} R^* &= \prod_{\mu_i \in S} \hat{e}(U_{\mu_i}, D_{\mu_i}^{ID^*})^{\Delta_{\mu_i,S}(0)} \\ &= \hat{e}(Q, Q^{1/x})^{r^*\Delta_{\mu^*,S}(0)} \cdot \Lambda \end{aligned}$$

where $\Lambda = \prod_{\mu_i \in S, \mu_i \neq \mu^*} \hat{e}(Q, Q)^{r_i \Delta_{\mu_i,S}(0)}$

Remark 3.3. *Obviously, the value Λ can be computed by B (also computable by A if the conditions of Remark 3.1 is applied), since B knows the private key components $D_{\mu_i}^{ID^*}$ for each $\mu_i \in S, \mu_i \neq \mu^*$, and B also knows the corresponding r_i's.*

We set $T = (R^*/\Lambda)^{1/(r^*\Delta_{\mu^*,S}(0))} = \hat{e}(Q, Q^{1/x})$. The solution to the k-BDHI problem, $\hat{e}(g, g^{1/x})$, is obtained by outputting $(T/T_0)^{1/c_0^2} = \hat{e}(g, g^{1/x})$ as in [7].

$$\begin{aligned} T/T_0 &= \hat{e}(g, g)^{f(x)\cdot f(x)/x} / \hat{e}(g^{(f(x)-c_0)/x}, g^{f(x)+c_0}) \\ &= \hat{e}(g, g)^{f(x)\cdot f(x)/x - f(x)\cdot f(x)/x + c_0^2/x} \\ &= \hat{e}(g, g)^{c_0^2/x} \end{aligned}$$

Let $\mathbb{H}$ be the event that algorithm A issues a query for $H_2(R^*)$ at some point during the simulation. Pr[$\mathbb{H}$] in the simulation above is equal to Pr[$\mathbb{H}$] in the real attack [3]. Also, in the real attack we have Pr[$\mathbb{H}$]$\geq \epsilon$ due to the following facts.

If the H_2List does not contain the value R^*, then we have $Pr[\beta' = \beta|\neg\mathbb{H}] = \frac{1}{2}$.

By the definition of A, we have $|Pr[\beta' = \beta] - \frac{1}{2}| > \epsilon$.

Combining all the results and defining the event E as $E = Pr[\beta = \beta']$, we obtain the following as in [3]

$$\begin{aligned} &E = Pr[\beta = \beta'|\mathbb{H}]Pr[\mathbb{H}] + Pr[\beta = \beta'|\neg\mathbb{H}]Pr[\neg\mathbb{H}] \\ &\quad \Longleftrightarrow Pr[\beta = \beta'] \geq \tfrac{1}{2}(1 - Pr[\mathbb{H}]) \\ &\quad \Longleftrightarrow Pr[\beta = \beta'] \leq \tfrac{1}{2}(1 + Pr[\mathbb{H}]). \end{aligned}$$

Therefore,

$$\epsilon \leq |Pr[\beta = \beta'|\mathbb{H}] - \tfrac{1}{2}| \leq \tfrac{1}{2}Pr[\mathbb{H}] \Longleftrightarrow Pr[\mathbb{H}] \geq 2\epsilon.$$

It follows that B produces the correct answer by picking a random entry from the H_2List with probability at least $\frac{2\epsilon}{\binom{n}{d}\cdot q_2}$ due to the q_2 entries in the H_2List and $\begin{pmatrix} n \\ d \end{pmatrix}$ different choices for A to compute the session key. Hence,

$$2\text{Adv}^{\text{FSID-IND-CPA}}_{\text{BIO-IBE}}(A) \leq \binom{n}{d} \cdot q_2 \cdot \text{Adv}^{\text{k-BDHI}}(B)$$

When we apply the condition on Remark 3.1, the adversary A will have only one choice for the set S, thus the factor $\begin{pmatrix} n \\ d \end{pmatrix}$ is eliminated from the reduction cost resulting in

$$2\text{Adv}^{\text{FSID-IND-CPA}}_{\text{BIO-IBE}}(A) \leq q_2 \cdot \text{Adv}^{\text{k-BDHI}}(B)$$

The modified security model gives the adversary as much power as possible by providing the adversary with $d-1$ private key components, and the restriction for the set S is necessary for B to have any advantage in this game. Thus, the improved reduction cost is obtained by requiring a stronger security model than the Fuzzy Selective-ID model of [11, 1].

□

4. Conclusion

In this paper, we propose a new biometric identity based encryption scheme BIO-IBE. Due to the employment of the Sakai Kasahara Key Construction, we obtain a more efficient scheme compared to the schemes in [10, 1]. We summarize in the following tables the properties of BIO-IBE and compare the computational costs of each algorithm used in the schemes. Obviously, BIO-IBE is more efficient in terms of the sub-algorithms of the schemes. Besides, the computational cost of the fuzzy extraction FE is small, since the operations in FE algorithm are performed on the finite field of $\mathbb{F}_{2^m}$, where $m \approx 10$ according to [4]. The only disadvantage is that the reduction is not tight, however, the BIO-IBE is reduced to a well-exploited computational

Figure 1. Computational Costs of Various Fuzzy IBE Schemes [1]

	SW-RO	EFIBE-I	EFIBE-II	BIO-IBE
Size of D_{ID}	$2n\vert\mathbb{G}\vert$	$2n\vert\mathbb{G}\vert$	$2n\vert\mathbb{G}\vert$	$n\vert\mathbb{G}\vert$
Size of C	$(n+1)\vert\mathbb{G}\vert+\vert\mathbb{F}\vert$	$(n+1)\vert\mathbb{G}\vert+\vert\mathbb{F}\vert$	$(n+1)\vert\mathbb{G}\vert+\vert\mathbb{F}\vert$	$n\vert\mathbb{G}\vert+k_1$
Cost of Key Generation	$n(T_H+T_m+3T_e)$	$n(T_H+2T_e)$	$n(T_H+T_m+2T_e)$	$n(T_e+T_i)$ $+FE_{ID}$
Cost of Encrypt	$n(T_e+T_H)$ $+2T_e+T_p+T'_m$	$n(T_e+T_m+T_H)$ $+2T_e+T_p+T'_m$	$n(T_e+T_H)$ $+2T_e+T_p+T'_m$	$n(2T_e+T_m)$ $+T_p+FE_{ID}$
Cost of Decrypt	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(T_e+T_p)$

Abbreviations: |S| is the bit-length of an element in set (or group) S; n is the number of elements in an identity; T_e is the computation time for a single exponentiation in $\mathbb{G}$; T_H is the computation time for MaptoPoint hash function; T_m is the computation time for a single multiplication in $\mathbb{G}$; T_i is the computation time for a single inverse operation in $\mathbb{Z}_p$; T_p is the computation time for a single pairing operation; T'_m is the computation time for a single multiplication in $\mathbb{F}$; T'_i the computation time for a single inverse operation in $\mathbb{F}$; d is the error tolerance parameter; FE_{ID} is the computation time for the fuzzy extraction process; k_1 output size of the hash function.

problem. Finally, an open problem is to prove the security of BIO-IBE in the standard model.

Table 1. Properties of Various Fuzzy IBE Schemes

Scheme	Assumption	Hash Function	Security Model
SW-RO	Decisional BDH	MaptoPoint	ROM
EFIBE-I	Decisional BDH	MaptoPoint	ROM
EFIBE-II	Decisional BDH	MaptoPoint	ROM
BIO-IBE	Computational k-BDHI	One-way	ROM

Acknowledgement

The author is grateful to her supervisor Prof. Dr. Joachim von zur Gathen for his valuable support.

References

[1] J. Baek, W. Susilo, and J. Zhou, "New constructions of fuzzy identity-based encryption," in *ACM Symposium on Information, Computer and Communications Security* (ASIACCS 2007), ACM, 2007, pp. 368–370.

[2] M. Bellare, C. Namprempre, and G. Neven, "Security Proofs for Identity-Based Identification and Signature Schemes," in *Advances in Cryptology-EUROCRYPT 2004*, LNCS 3027, Springer, 2004, pp. 268–286.

[3] D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," *SIAM J. Comput.*, vol.32, pp. 586–615, 2003.

[4] A. Burnett, F. Byrne, T. Dowling, and A. Duffy, "A Biometric Identity Based Signature Scheme," *International Journal of Network Security*, vol.5, pp. 317–326, 2007.

[5] C. Chen, R. N. J. Veldhuis, T. A. M. Kevenaar, and A. H. M. Akkermans, "Multi-bits biometric string generation based on the likelyhood ratio," *IEEE conference on Biometrics: Theory, Applications and Systems*, 2007, pp. 1–6.

[6] L. Chen and Z. Cheng, "Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme," in *Cryptography and Coding, IMA Int. Conf.*, LNCS 3796, Springer, 2005, pp. 442–459.

[7] L. Chen, Z. Cheng, J. Malone-Lee, and N. Smart, "Efficient ID-KEM based on the Sakai-Kasahara key construction," *IEE Proceedings Information Security*, vol. 153, pp. 19–26, 2006.

[8] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," *CoRR*, abs/cs/0602007, 2006.

[9] T. Okamoto and D. Pointcheval, "REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform," in *Topics in Cryptology* (CT-RSA 2001), LNCS 2020, Springer, 2001, pp. 159–175.

[10] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," in *ACM Conference on Computer and Communications Security*, ACM, 2006, pp. 99–112.

[11] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in *Advances in Cryptology-EUROCRYPT 2005*, LNCS 3494, Springer, 2005, pp. 457–473.

[12] R. Sakai and M. Kasahara, "ID based Cryptosystems with Pairing on Elliptic Curve," Cryptology ePrint Archive, Report 2003/054, 2003.

[13] A. Shamir, "How to Share a Secret," *Commun. ACM*, vol.22, pp. 612–613, 1979.