SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks **00**: 1–11 (2008)
Published online in Wiley InterScience
(www.interscience.wiley.com) DOI: 10.1002/sec.0000

A New Biometric Identity Based Encryption Scheme Secure Against DoS Attacks

Neyire Deniz Sarier

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

Summary

Recently, Sarier [1] proposed an efficient biometric Identity Based Encryption (IBE) scheme called BIO-IBE using the Sakai Kasahara Key Construction and prove its security in the random oracle model based on the well-exploited BDHI computational problem. Despite its efficiency compared to other fuzzy IBE systems implemented for biometric identities, BIO-IBE is not secure against a new type of Denial of Service (DoS) attack that we present. In this context, we describe a new biometric IBE scheme and show that our scheme is immune against this attack due to the signature applied on the public value PAR of the user. This way, the sender can detect whether PAR of the receiver that is stored publicly is modified by an active adversary, thus the generation of a ciphertext based on a wrong identity is avoided. The main difference of the new 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. In addition to the well-defined security model for current fuzzy IBE schemes, we describe a stronger security model and prove the security of our scheme in this framework achieving a better reduction cost compared to BIO-IBE. Finally, our scheme provides security against DoS attacks and better efficiency in terms of the key generation and decryption algorithms compared to the existing fuzzy IBE schemes.

KEY WORDS: Biometrics; fuzzy IBE; fuzzy extraction; DoS Attack

1. Introduction

In Eurocrypt'04, 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. This new system combines the advantages of IBE with using biometrics as an identity, where IBE avoids the need for an online Public Key Infrastructure (PKI), which is the most inefficient and costly part of public key encryption. The use of biometrics as the identity in the framework of IBE simplifies the process of key generation at the Private Key Generator (PKG). Since biometric information is unique, unforgettable and non-transferable, the user only needs to provide his biometrics at the PKG to obtain his secret key instead of presenting special documents and credentials to convince the PKG about his identity. Also, biometrics is attached to the user, hence the public key of the user is always with him to be used for encryption during an ad hoc meeting. Finally, biometric data could be easily integrated with fuzzy IBE due to its error tolerance property, which is required for the noisy nature of

biometrics. The main feature of fuzzy IBE is the construction of the secret key based on the biometric data of the user which can decrypt a ciphertext encrypted with a slightly different measurement of the same biometrics. Specifically, 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 biometrics w', provided that w and w' are within a certain distance of each other. Besides, fuzzy IBE could be applied in the context of Attribute-Based Encryption [2, 3], where the sender encrypts data using a set of attributes such as {university, faculty, department} and the ciphertext could only be decrypted if the receiver has the secret key associated to all of these attributes or sufficient number of them. In current fuzzy IBE schemes, the private key components are generated by combining the values of a unique polynomial on each attribute with the master secret key. Besides, the biometrics is considered 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 [3] is described by Sahai and Waters in 2005 and its security is reduced to the MBDH problem in the standard model, where the size of the public parameters is linear in the size of the attribute space U or the number of attributes of a user n. Piretti et al [2] achieved a more efficient fuzzy IBE scheme with short public parameter size by employing the Random Oracle Model (ROM). Baek et al [4] described two new fuzzy IBE schemes with an efficient key generation algorithm and proved the security in ROM based on the DBDH assumption. The main disadvantage of these schemes is the use of the MapToPoint hash function, which is inefficient compared to the ordinary hash functions. Besides, Burnett et al [5] described a biometric Identity Based Signature (IBS) scheme called BIO-IBS, where they used the biometric information as the identity and construct the public key of the user using a fuzzy extractor [6], which is then used in the modified SOK-IBS scheme [7]. Recently, Sarier [1] described a new biometric IBE scheme called as BIO-IBE, which is more efficient compared to the existing fuzzy IBE schemes due to the replacement of the MapToPoint hash function with an ordinary hash function. However, BIO-IBE suffers from a new type of a DoS attack that we introduce in the next sections.

1.2. Our Contribution

In this paper, we present an efficient biometric IBE scheme by modifying the BIO-IBE of [1] in order to provide immunity against a new type of a DoS attack. To prevent DoS attacks, our modifed scheme integrates an efficient IBS scheme into BIO-IBE in order to sign the public value PAR of the receiver during the key generation phase of BIO-IBE. Besides, the encryption phase is also modified by requiring the sender to verify the signature on the PAR before the fuzzy extraction and the encryption of the message. The IBS scheme that is used to sign the PAR is currently the most efficient pairing based IBS scheme [8], which is based on the Sakai Kasahara Key Construction, thus it is very well-suited to modified BIO-IBE. Similar to BIO-IBE, the main difference of our scheme from existing fuzzy IBE systems 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 this novel approach. Despite the additional computations for verifying the signature on PAR, the modified BIO-IBE still achieves 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 [2, 4] 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 [2] (and from $2n$ as in [4]) to $n+2$. 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 ROM. Moreover, we describe a stronger security model for fuzzy IBE and prove the security of modified BIO-IBE based on this stronger model with a better reduction cost compared to BIO-IBE [1].

1.3. Outline of the Paper

In section 2, we will state the definitions of the primitives that are used in our scheme. In section 3, we review the BIO-IBE scheme and show that it is vulnerable to a new DoS attack. Next, we describe the modified BIO-IBE scheme and evaluate its security. In

section 5, we define a new security model and prove the security of our scheme in this stronger model. Finally, we compare our results with existing fuzzy IBE schemes and conclude our proposals.

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, $x \xleftarrow{R} S$ defines the assignment of a uniformly distributed random element from the set S to the variable x. $|S|$ denotes the bit-length of an element in S and μ_i denotes an attribute (or feature) in the universe U of biometric attributes.

Definition 2.1 Negligible Function: *A function $\epsilon(k) : \mathbb{N} \rightarrow \mathbb{R}$ is defined as negligible if for any constant c, there exists $k_0 \in N$ with $k > k_0$ such that $\epsilon < (1/k)^c$.*

Definition 2.2 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 $\mathbb{G} \setminus \{1_\mathbb{G}\}$, where $\{0\}$ and $\{1_\mathbb{G}\}$ are the identity elements of $\mathbb{Z}_p$ and $\mathbb{G}$, respectively. A bilinear pairing is denoted by $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$ 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. *$\hat{e}(g, g) \neq 1_\mathbb{F}$, namely the pairing is non-degenerate.*

Next, 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

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

The security of our scheme is reduced to the well-exploited complexity assumption (k-BDHI) [9], which is stated as follows.

Definition 2.3 k-Bilinear Diffie-Hellman Inverse (k-BDHI): *For an integer k, and $x \xleftarrow{R} \mathbb{Z}_p^*$, $g \in \mathbb{G}^*$, $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}$, 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 [4], 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 $w \in U$ and ms, the PKG returns the corresponding private key.
- 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 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 denotes the error tolerance parameter of the scheme.

In the modified BIO-IBE, the identity is obtained from the biometric information of the user using a feature extraction algorithm followed by a fuzzy extraction process, where the result of the former procedure (i.e. w) is combined with the output of the latter (i.e. ID) in the key generation phase to compute the private key of a user. The details of this extraction process is presented in section 2.3.

2.2. Security Model

In [3], 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 A 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 A issues private key queries for any identity w' such that $|w' \cap w^*| < d$.
- *Phase 4*: The adversary A sends two equal length messages m_0 and m_1. The challenger returns the ciphertext that is encrypted using w^* and the message m_β, where $\beta \xleftarrow{R} \{0, 1\}$.
- *Phase 5*: Phase 3 is repeated.

DOI: 10.1002/sec

- *Phase 6*: A outputs a guess β' for β.

The advantage of the adversary A is defined as

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

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 [10] to be secure against Chosen Ciphertext Attacks (CCA).

2.3. Biometric Fuzzy Extraction

Any biometric identity based encryption or signature scheme requires the biometric measurement of the receiver or the signer, respectively. For this purpose, the biometrics of the user is captured using a sensor and the raw biometric data is further processed to extract the feature vector and to obtain the biometric template b of the user. In a biometric encryption scheme, feature extraction is applied on the raw biometric data to obtain the feature vector (or the attributes) and then, each attribute is associated with a unique integer $\mu_i \in \mathbb{Z}_p^*$ to form the identity $w = (\mu_1, ..., \mu_n)$ [3, 4]. 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 a biometric IBS scheme such as BIO-IBS [5], the biometric template b is computed using the feature vector and the hash of b is used as the identity ID. Here, the template b is assumed to be a fixed length binary string, so each feature forming the original biometric template (namely the feature vector) are quantized to generate multiple bits per feature that are concatenated to obtain the binary template b. Particularly, the framework for biometric template generation consists of (1) extracting features; (2) quantization and coding per feature and concatenating the output codes; (3) applying error correction coding (ECC) and hashing [11]. During this process, many quantizers produce and use side-information, which could be published to be used later in the reconstruction of the binary template b'.

As different from existing fuzzy IBE systems, the modified BIO-IBE requires the use of the biometric template b obtained from the feature vector of the user, where feature extraction is the most costly part of the biometric template generation. Since feature extraction is already performed in any fuzzy IBE scheme, one can easily apply a fuzzy extractor on the feature vector to bind the private key components to the user's identity and thus avoid collusion attacks. Instead of choosing a unique polynomial for each user, we use the 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 of the fuzzy extractor.

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

Definition 2.4 *Let $\mathcal{M} = \{0,1\}^v$ be a finite dimensional metric space with a distance function* **dis** *: $\mathcal{M} \times \mathcal{M} \rightarrow \mathbb{Z}^+$. 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 value PAR, and outputs ID if* **dis**$(b, b') \leq t$.

In [5], 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 $H : \{0,1\}^n \rightarrow \{0,1\}^l$. 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.

DOI: 10.1002/sec

3. A New Efficient Biometric IBE Scheme

In this section, we present the modified BIO-IBE that is built upon the biometric IBE scheme of [1] except for the key generation and encryption algorithms. Our scheme uses Sakai-Kasahara's Key Construction [9, 12] for the generation of the private keys, thus it does not require a MapToPoint hash function as opposed to the schemes in [2, 4]. As it is noted in [8], it is difficult to find groups as the range of the MapToPoint hash function and to define an efficient isomorphism at the same time. Thus, our scheme avoids this problem and achieves better performance due to the use of an ordinary hash function instead of MapToPoint hash function, which is called n times for the key generation and encryption algorithms respectively. 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 $n = 2^m - 1$ is the length of the code and $m \approx 10$ for the $[905, 160, 201]$ BCH error correction code as described in [5]. In order to encrypt a message, the sender obtains the biometric information of the receiver and verifies the signature σ of the PKG on the public parameter PAR of the receiver and if σ is valid, then he extracts the features (attributes) and computes the biometric string ID using the fuzzy extractor. As in [1], we assume that if $|w \cap w'| \geq d$, then we have $\mathbf{dis}(b, b') \leq t$ and thus $ID = ID'$. First, we review the details of BIO-IBE.

- **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 $P_{pub} = g^x$ and $\hat{e}(g, g)$
  3. Pick two cryptographic hash functions $H_1 : \mathbb{Z}_p^* \times \{0,1\}^* \to \mathbb{Z}_p^*$, $H_2 : \mathbb{F} \to \{0,1\}^{k_1}$. 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.

  $M = \{0,1\}^{k_1}$ denotes the message space and $C = U \times \mathbb{G}^n \times \{0,1\}^{k_1}$ denotes the ciphertext space. The master public key is $(p, \mathbb{G}, \mathbb{F}, \hat{e}, k_1, g, P_{pub}, \hat{e}(g, g), H_1, H_2, H, C_e, C_d, F_e)$ 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, where each attribute $\mu_i \in w$ is an element of $\mathbb{Z}_p^*$ [3]. Besides, the identity string $ID = H(b)$ is calculated from the biometric template b using a fuzzy extractor as in [5]. 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 $ID' = \mathbf{Rep}(b', PAR)$. Here, if $\mathbf{dis}((b, b') < t$, 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

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

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*

DOI: 10.1002/sec

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 $k = q_1 + q_{ex} + 1$ and advantage

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

Despite the security reduction that is presented above, BIO-IBE is not secure against a new attack that we present in the next section. By modifying the key generation and encryption algorithms, BIO-IBE could be fixed against this DoS attack. The corrected scheme is called as modified BIO-IBE, which has the same decryption phase as BIO-IBE.

3.1. A New Denial of Service Attack

BIO-IBE scheme of [1] requires the public storage of the value PAR, which is the information needed for error-tolerant reconstruction of the biometric identity string ID and subsequent fuzzy extraction. Since the encryption is performed by combining each biometric feature μ_i with the biometric identity ID of the receiver, the presence of an active adversary who maliciously alters the public string PAR leads the sender to use a wrong public key for the encryption due to a different identity string computed by the fuzzy extractor. By the malicious modification of the public value PAR, an adversary cannot gain any secret information but the receiver of the ciphertext either cannot decrypt it or he obtains a wrong plaintext upon decryption. The fuzzy IBE schemes of [3, 2, 4] are immune against this attack since the biometric identity of a user consists only of the feature vector w.

The first idea to solve this problem is using a robust fuzzy extractor, which is resilient to modification of the public value PAR [14]. However, the robust fuzzy sketches/fuzzy extractors described in [14] assumes the biometrics as secret data and replaces the value PAR with $PAR^* = \langle PAR, H(b, PAR)\rangle$,where H is a hash function [14]. Since the adversary knows the biometric data b, he can easily modify the value PAR^* by computing a valid hash value, hence, the sender cannot detect the modification of the public value. Another solution could be that the user store the public value PAR in his smart card and present this to the sender during the biometric measurement. However, this defeats the purpose of biometric IBE in the first place, which enables an unprepared user to encrypt in an ad hoc meeting, where the users do not have their smartcards with them.

In [15], a similar attack called as Denial-of-Decryption (DoD) Attack in the context of certificateless encryption is defined, whose nature is similar to the well known DoS Attack. In DoD, the attacker can modify the public key of the receiver since the authenticity of the public key is not provided. The authors provide the solution against this attack by requiring the receiver to sign his public key using the private key associated to a certificateless signature scheme and store the public value together with the signature in a public storage. When the sender wants to encrypt a message, he first verifies the signature on the public value and upon validation, he starts encryption.

In order to prevent a DoS attack on our scheme, we follow a similar approach requiring the PKG to sign the public value PAR using an efficient pairing based IBS scheme [8], and publish both values.

A summary of this scheme is given as below, where the public parameters of [8] are almost equal to the parameters of BIO-IBE since both schemes are based on the same Sakai-Kasahara Key Construction method. The only difference in the public parameters of [8] is the use of an arbitrary string such as an e-mail address as the identity and two hash functions, which have a different domain. Since the signature is applied by the PKG, then the identity information is taken as the identity of the PKG. It is shown that the scheme in [8] is UF-CMA (Existential Unforgeability under Chosen Message Attack) secure [8]. Consequently, the signature on the public value PAR makes the modified BIO-IBE immune against a DoS attack.

- **Setup()**: The same as in BIO-IBE except for the hash functions $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0,1\}^* \times \mathbb{F} \rightarrow \mathbb{Z}_p^*$ that are used instead of H_1 and H_2 of BIO-IBE.
- **Key Generation**: The signing key is $D = g^{1/(x+H_3(ID))}$, where ID is the identity of the PKG.
- **Sign**: In order to sign the public value PAR,

  1. Pick a random integer $r \in \mathbb{Z}_p^*$ and compute $\hat{e}(g,g)^r \in \mathbb{F}$ and $h = H_4(PAR, \hat{e}(g,g)^r) \in \mathbb{Z}_p^*$.
  2. Compute $S = D^{r+h}$.

  Hence, the signature on PAR is $\sigma = (h, S)$.

DOI: 10.1002/sec

- **Verify**: To verify a signature $\sigma = (h, S)$ on PAR, compute

$$\begin{aligned} V &= \hat{e}(S, g^{H_3(ID)} \cdot g^x) \cdot \hat{e}(g,g)^{-h} \\ &= \hat{e}(D^{r+h}, g^{H_3(ID)} \cdot g^x) \cdot \hat{e}(g,g)^{-h} \\ &= \hat{e}(g^{(r+h)/(x+H_3(ID))}, g^{H_3(ID)+x}) \cdot \hat{e}(g,g)^{-h} \\ &= \hat{e}(g,g)^{r+h} \cdot \hat{e}(g,g)^{-h} \\ &= \hat{e}(g,g)^{r} \end{aligned}$$

  and check whether $H_4(PAR, V) = h$

After verifying the signature on the public value PAR, the sender can encrypt a message. The only additional cost for the sender is caused by the verification of the signature, namely, one exponentiation in $\mathbb{G}$ and in $\mathbb{F}$, one bilinear pairing and one multiplication in $\mathbb{F}$. Despite the additional bilinear pairing computation for the sender, our scheme is still more efficient compared to existing fuzzy IBE schemes due to the removal of n MapToPoint hash computations from each phase. Moreover, the scheme of [8] is currently the most efficient pairing-based IBS scheme in the literature, which is suitable for the modified BIO-IBE.

3.2. The modified BIO-IBE

Here, we summarize the algorithms of our new scheme, which is obtained by modifying the Key Generation and Encrypt algorithms of BIO-IBE.

- **Setup()**: The parameters of the scheme are generated as in BIO-IBE. Two additional hash functions $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0,1\}^* \times \mathbb{F} \rightarrow \mathbb{Z}_p^*$ are required for the signature scheme as described before.
- **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 [3]. Besides, the identity string $ID = H(b)$ is calculated from the biometric template b using a fuzzy extractor, which also outputs the public value PAR that is used in the reconstruction of the ID by the sender (or encryptor). Next, PAR is signed by the PKG. 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 $\mu_i \in w$. Finally, the PAR and the signature σ are stored in a public file.
- **Encrypt**: The sender obtains a biometric reading of the receiver together with the signed public parameter PAR, verifies the signature on the PAR, extracts the feature vector w' and computes $ID' = \mathbf{Rep}(b', PAR)$. Here, if $\mathbf{dis}((b, b') < t$, then $ID = ID'$. Given a plaintext $m \in M$, ID' and w', the algorithm continues as in BIO-IBE.
- **Decrypt**: The same algorithm as in BIO-IBE.

Lemma 3.1 *The modified BIO-IBE is immune against a DoS attack under the existential unforgeability of the IBS scheme of [8].*

Theorem 3.2 *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 modified 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 $k = q_1 + q_{ex} + 1$ and*

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

The security proof will be very similar to the proof of BIO-IBE as in [1].

4. A New Security Model

In this section, we describe a stronger Selective-ID model of security for fuzzy IBE (sFSID-IND-CPA) using a game between a challenger and an adversary as follows. The main difference of our new security model is that the adversary is allowed to make private key extraction queries on the challenge identity w^*, where A can obtain $d-1$ private key components of w^* that A chooses. In this model, the adversary A has more power compared to the model defined in [3, 4].

- *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 $|w' \cap w^*| < d$. In addition, if the extraction query is on the challenge identity w^*, A is given $d-1$ private key components that A chooses.

DOI: 10.1002/sec

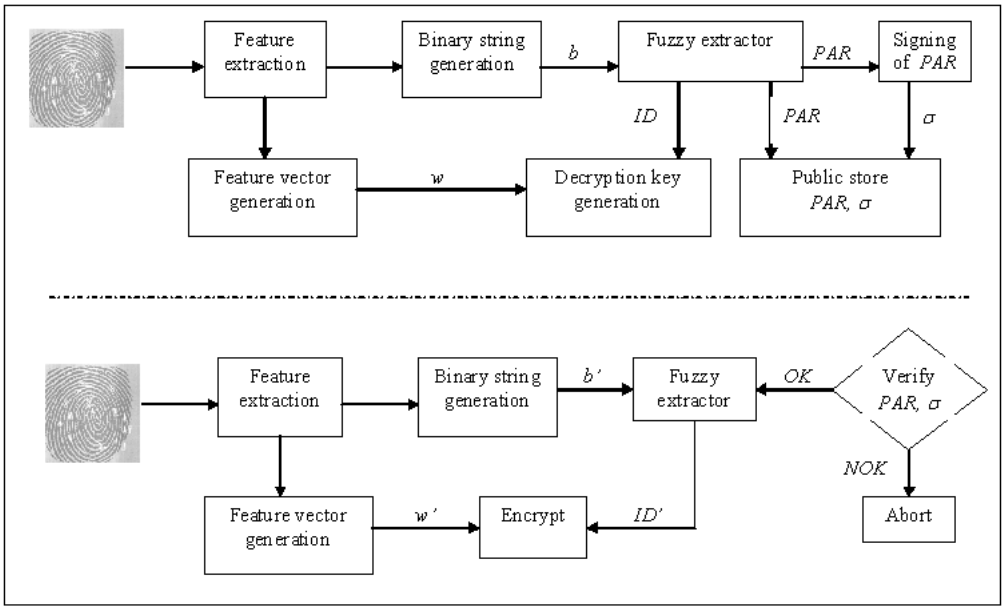

Fig. 1. Modified BIO-IBE Flow diagram

- *Phase 4*: The adversary A 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 $\beta \xleftarrow{R} \{0,1\}$ and A already has the $d-1$ private key components of w^*.
- *Phase 5*: Phase 3 is repeated. For the challenge identity, A is not allowed to issue private key queries for the remaining $n-d+1$ attributes.
- *Phase 6*: A outputs a guess β' for β.

Theorem 4.1 *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 modified BIO-IBE in the strong 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 $k = q_1 + q_{ex} + 1$ and advantage*

$$2Adv^{sFSID\text{-}IND\text{-}CPA}(A) \leq (n-d+1) \cdot Adv^{k\text{-}BDHI}(B)$$

Proof 4.1 *Assume that a polynomial time attacker A breaks our scheme, 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 $(g, g^x, g^{x^2}, ..., g^{x^k})$, B will compute $\hat{e}(g,g)^{1/x}$ using A as follows.*

- ***Phase 1***: A outputs the challenge identity $w^* = (\mu_1^*, ..., \mu_n^*)$ and B simulates the public parameters for A as follows:
  First, 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.
  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 [16].
  Next, $f_j(z) = \frac{f(z)}{z+h_j} = \sum_{v=0}^{k-2} d_{j,v} z^j$ for $1 \leq j < k$ and $Q^{1/(x+h_j)} = g^{f_j(x)} = \prod_{v=0}^{k-2}(g^{x^v})^{d_{j,v}}$ is computed [16].
  B sets $T' = \prod_{j=1}^{k-1}(g^{x^{j-1}})^{c_j} = g^{(f(x)-c_0)/x}$ 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

DOI: 10.1002/sec

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 $\langle j, d, \mu^*, ID^*, h_0, \perp\rangle$ to H_1List. Increment j and l 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 $1 \leq l \leq n$.
H_2**-queries**: Upon receiving a query R,

1. If there exists (R, ξ) in H_2List, return ξ.
2. Else, 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),

1. If $|w \cap w^*| < d$, (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 $\mu_i \in w$.
2. Otherwise, return the $d-1$ private key components $D_{\mu_i^*}^{ID^*} = Q^{1/(x+h_j)}$ that A chooses except for the component associated to the attribute μ^*.

- ***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 $r^* \xleftarrow{R} \mathbb{Z}_p$ and compute $U_{\mu^*} = Q^{r^*}$.
4. B chooses a random $\beta \in \{0,1\}$ and $W^* \xleftarrow{R} \{0,1\}^{k_1}$.
5. Set the ciphertext to $C^* = (w^*, U_{\mu_i}, m_\beta \oplus W^*)$ where $\mu_i \in w^*$.

- ***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 challenge private key for the remaining $n - d + 1$ components.
- ***Phase 6***: At some point, A responds with the guess β' for the underlying plaintext m_β, which could only be computed from

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

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

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

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 [16].

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

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 [17]. 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, $|Pr[\beta' = \beta] - \frac{1}{2}| > \epsilon$.

Combining all the results and defining the event E as $E = Pr[\beta = \beta']$, we obtain the following as in [17]

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

Therefore,

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

Obviously, the value Λ can be computed by B and the adversary A, since A already knows the $d-1$ private key components of w^*, hence, the set S is composed of the $d-1$ components and another attribute $\mu_i \in w^*$ that A decides. 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 d private key components, where A already knows $d-1$ of them and 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 previously. The adversary A will have only $n-d+1$ different choices for the set S, so, the factor $\binom{n}{d}$ is eliminated from the reduction cost resulting in a non-exponential loss of security as

$$2\text{Adv}^{\text{sFSID-IND-CPA}}(A) \leq (n-d+1) \cdot \text{Adv}^{\text{k-BDHI}}(B)$$

The modified security model gives the adversary as much power as possible by providing the adversary with $d-1$ private key components of the challenge identity. Thus, the improved reduction cost is obtained by requiring a stronger security model than the Fuzzy Selective-ID model of [3, 4].

5. Comparison

We summarize in the following tables the properties of the modified BIO-IBE and compare the computational costs of each algorithm used in the schemes that are provably secure in ROM. The abbreviations that are used in Figure 2 are listed in Table II. Obviously, the new scheme is more efficient in terms of the key generation and decryption algorithms. Compared to BIO-IBE, the encryption algorithm requires additionally one bilinear pairing and 2 exponentiations due to the signature verification on the PAR, which makes our scheme secure against DoS attacks. 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 [5].

6. Conclusion

In this paper, we propose an efficient biometric IBE scheme secure against DoS attacks by integrating an IBS scheme into the BIO-IBE scheme. Despite the additional bilinear pairing computation, we obtain a more efficient scheme compared to the schemes in [2, 4] due to the structure of the decryption algorithm and the removal of the MapToPoint hash function. Finally, an open problem is to prove the security of [4] and our scheme in the standard model.

Table I. 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
New Scheme	Computational k-BDHI	Regular	ROM

Table II. Abbreviations

$\|S\|$	bit size of an element in the set S
n	number of features of a user
d	error tolerance parameter
T_e	time for a single exponentiation in $\mathbb{G}$
T'_e	time for a single exponentiation in $\mathbb{F}$
T_H	time for MaptoPoint hash function
T_m	time for a single multiplication in $\mathbb{G}$
T'_m	time for a single multiplication in $\mathbb{F}$
T_i	time for a single inverse operation in $\mathbb{Z}_p$
T'_i	time for a single inverse operation in $\mathbb{F}$
T_p	time for a single pairing operation
FE	time for the fuzzy extraction process
k_1	output size of the hash function

Acknowledgement

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

References

1. Sarier ND. A new biometric identity based encryption scheme. *The 2008 International Symposium on Trusted Computing - TrustCom 2008*, IEEE Computer Society, 2008.
2. Pirretti M, Traynor P, McDaniel P, Waters B. Secure attribute-based systems. *ACM Conference on Computer and Communications Security*, 2006; 99–112.
3. Sahai A, Waters B. Fuzzy identity-based encryption. *Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science*, vol. 3494, Springer, 2005; 457–473.
4. Baek J, Susilo W, Zhou J. New constructions of fuzzy identity-based encryption. *ACM Symposium on Information, Computer*

Fig. 2. Computational Costs of Various Fuzzy IBE Schemes

	SW-RO [2]	EFIBE-I [4]	EFIBE-II [4]	Modifed BIO-IBE
Size of D_{ID}	$2n\|\mathbb{G}\|$	$2n\|\mathbb{G}\|$	$2n\|\mathbb{G}\|$	$(n+1)\|\mathbb{G}\|$
Size of C	$(n+1)\|\mathbb{G}\|+\|\mathbb{F}\|$	$(n+1)\|\mathbb{G}\|+\|\mathbb{F}\|$	$(n+1)\|\mathbb{G}\|+\|\mathbb{F}\|$	$n\|\mathbb{G}\|+k_1$
Cost of Key Generation	$n(T_H+T_m+3T_e)$	$n(T_H+2T_e)$	$n(T_H+T_m+2T_e)$	$(n+1)(T_e+T_i)$ $+FE+T_e+T'_e$
Cost of Encrypt	$n(T_e+T_H)$ $+2T_e+T_p+T'_m$	$n(T_e+T_m+T_H)$ $+2T_e+T_p+T'_m$	$n(T_e+T_H)$ $+2T_e+T_p+T'_m$	$n(2T_e+T_m)+T'_m+$ $2T_p+FE+T'_e+T_e$
Cost of Decrypt	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(2T_e+T_m+T_p)$ $+T_p+T'_i+T'_m$	$d(T_e+T_p)$

and Communications Security, ASIACCS 2007, 2007; 368–370.

5. Burnett A, Byrne F, Dowling T, Duffy A. A Biometric Identity Based Signature Scheme. *International Journal of Network Security* 2007; **5**(3):317–326.
6. Dodis Y, Ostrovsky R, Reyzin L, Smith A. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *CoRR* 2006; **abs/cs/0602007**.
7. Bellare M, Namprempre C, Neven G. Security Proofs for Identity-Based Identification and Signature Schemes. *Advances in Cryptology - EUROCRYPT 2004, Lecture Notes in Computer Science*, vol. 3027, Springer, 2004; 268–286.
8. Barreto PSLM, Libert B, McCullagh N, Quisquater JJ. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. *ASIACRYPT*, 2005; 515–532.
9. Chen L, Cheng Z. Security Proof of Sakai-Kasahara's Identity-Based Encryption Scheme. *Cryptography and Coding, IMA Int. Conf., Lecture Notes in Computer Science*, vol. 3796, Springer, 2005; 442–459.
10. Okamoto T, Pointcheval D. REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform. *Topics in Cryptology - CT-RSA 2001, Lecture Notes in Computer Science*, vol. 2020, Springer, 2001; 159–175.
11. Chen C, Veldhuis RNJ, Kevenaar TAM, Akkermans AHM. Multi-bits biometric string generation based on the likelyhood ratio. *IEEE conference on Biometrics: Theory, Applications and Systems*, University of Notre Dame, 2007; 1–6.
12. Sakai R, Kasahara M. ID based Cryptosystems with Pairing on Elliptic Curve. Cryptology ePrint Archive, Report 2003/054 2003.
13. Shamir A. How to Share a Secret. *Commun. ACM* 1979; **22**(11):612–613.
14. Boyen X, Dodis Y, Katz J, Ostrovsky R, Smith A. Secure remote authentication using biometric data. *Advances in Cryptology - EUROCRYPT 2005, Lecture Notes in Computer Science*, vol. 3494, Berlin: Springer-Verlag, 2005; 147–163.
15. Liu JK, Au MH, Susilo W. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: extended abstract. *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, 2007; 273–283.
16. Chen L, Cheng Z, Malone-Lee J, Smart N. Efficient ID-KEM based on the Sakai-Kasahara key construction. *IEE Proceedings Information Security* 2006; **153**(1):19–26.
17. Boneh D, Franklin MK. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.* 2003; **32**(3):586–615.

Author's Biography

Neyire Deniz Sarier received her B.Sc. degree in Mathematics and Industrial Engineering from Technical University of Istanbul, Turkey in 2005. She is currently a Ph.D. candidate at Cosec, B-IT Bonn, where she obtained her master degree on Media Informatics in 2007. Her research interests include Biometric security, in particular, integration of biometrics into cryptographic applications.