An Efficient Biometric Identity Based Signature Scheme

Yang Yang[1,2], Yupu Hu[3] and Leyou Zhang[3]
[1] College of Mathematics and Computer Science, Fuzhou University,
Fuzhou, 350108 - China
[e-mail: yang.yang.research@gmail.com]
[2] Key Lab of Information Security of Network Systems (Fujian Province Universities),
Fuzhou University, Fuzhou, 350108 – China
[3] Key Laboratory of Computer Networks and Information Security, Xidian University,
Xi'an, 710071 – China
[e-mail: xidianzly@163.com]
*Corresponding author: Yang Yang

Received April 23, 2012; revised September 6, 2013; revised October 14, 2013; accepted December 2, 2012; published August 30, 2013

Abstract

The combination of biometrics and cryptography gains a lot of attention from both academic and industry community. The noisy biometric measurement makes traditional identity based cryptosystems unusable. Also the extraction of key from biometric information is difficult. In this paper, we propose an efficient biometric identity based signature scheme (Bio-IBS) that makes use of fuzzy extractor to generate the key from a biometric data of user. The component fuzzy extraction is based on error correction code. We also prove that the security of suggested scheme is reduced to computational Diffie-Hellman (CDH) assumption instead of other strong assumptions. Meanwhile, the comparison with existing schemes shows that efficiency of the system is enhanced.

Keywords: Biometric, Identity Based, Signature, Provable Secure

This work is partially supported by the "973" program of China under Grant 2007CB311201 and the National Natural Science Foundation of China under Grants 60970119, 61072067, 61103175, 61100231, 61202350. This work was also supported by the Technology Innovation Platform Project of Fujian Province (No.2009J1007) and Natural Science Basic Research Plan in Shaanxi Province (No.2012JQ8044).

http://dx.doi.org/10.3837/tiis.2013.08.015

1. Introduction

Biometric technology has been used to ensure a higher level of security. It is adopted in important areas of the national infrastructure, such as electronic passports, visa application and immigration control systems. Biometric keys have many advantages over common cryptographic credentials. They are unforgettable, difficult to copy or share, un-transferable and do not need to be stored, while typical keys can be forgotten, lost, stolen and can not provide non-repudiation [1]. Cryptosystems based on biometric characteristics of persons inherently provide solutions to these problems [2].

Identity based scheme (IBE) [3] is a public key cryptosystem that allows the user to choose his email address or telephone number as public key, instead of generating a random pair of public/private keys. A private key generator (PKG) computes private keys from master secret key and distributes these to the entities participating in the scheme. IBE system has its strengths and weaknesses. The chief disadvantage of such schemes is that they did not allow human biometric characteristics to be used as identities. Since the value of a biometric sample is often disturbed by many noises and has distortion when sampled, we could not utilize available identity based schemes.

In 2005, Sahai and Waters [4] proposed a new concept "fuzzy identity based encryption" in which identities are regarded as a set of descriptive attributes instead of a string of social characters in previous identity based encryption systems [5, 6]. In 2007, Burnett, Duffy and Dowling [7] presented the concept of biometric identity based signature(Bio-IBS), where they used the biometric information to construct the key yet has no concrete scheme. In 2008, Liu et al. [8] proposed a new special Bio-IBS scheme. However, it focuses on the algorithm to generate key string from a biometric measurement of signer rather than the construction of Bio-IBS. A toy Bio-IBS scheme is presented in [8] without any security proof. Up to now, the existing Bio-IBS scheme is very few.

In this paper, we present a new Bio-IBS scheme which possesses low communication overhead and high security simultaneously. In our case, biometric measurements such as fingerprints [9], eye retinas and irises [10], voice patterns [11] and facial patterns [12] are utilized to construct the key. Using biometrics in cryptosystem however arouse a question that how to turn biometric data into key and reproduce the key from noisy biometric information. There are three steps to overcome this problem. First, extract biometric feature from raw biometric information with reader equipment. Second, transform the data into identity utilizing an encoding function of error correcting code [13]. Then, decoding function is used to reproduce the key string from biometric information which may be disturbed by many noises and distortion when is sampled. Thus, our construction has features of strong error tolerance and flexibility. We also present the concrete scheme model and security model of Bio-IBS. Furthermore, under the Computational Diffie-Hellman (CDH) assumption, our scheme is provably secure against existential unforgeable chosen message attack (EU-CMA). This assumption is more natural than the hardness assumptions which have been recently introduced to other schemes. Hence, the proposed scheme is secure.

The rest of the paper is organized as follows. In section 2, we briefly outline the concept of bilinear map, the harness assumption, threshold secret sharing and fuzzy extractor. In section 3, we formally define a Bio-IBS scheme including the security model. A description of our construction is followed in section 4 and in section 5 we discuss the security and efficiency issues. Finally, our conclusion is drawn in section 6.

2. Preliminaries

2.1 Bilinear Map

Let G and G_1 be two (multiplicative) cyclic groups of prime order p and g be a generator of G. A bilinear map $\hat{e}$ is a map $\hat{e}: G \times G \to G_1$ with the following properties:

- Bilinearity: for all $u, v \in G, a, b \in Z_p$, we have $\hat{e}(u^a, v^b) = \hat{e}(u, v)^{ab}$;
- Non-degeneracy: $\hat{e}(g, g) \neq 1$;
- Computability: there is an efficient algorithm to compute $\hat{e}(u, v)$ for all $u, v \in G$.

The modified Weil pairing and the Tate pairing are admissible maps of this kind. The security of our scheme described here relies on the hardness of the following problems.

2.2 Computational Diffie-Hellman Assumption

Security of our Bio-IBS scheme will be reduced to the hardness of the CDH problem in the group in which the scheme is constructed. We briefly recall the definition of the CDH problem:

Definition 1 Given a group G of prime order p with generator g and elements $g^a, g^b \in G$ for some uniformly chosen $a, b \in Z_p$ as input, the CDH problem is to compute g^{ab}.

Definition 2 We say that (t, ε) CDH assumption holds in group G if there is no adversary running in time at most t can solve the CDH problem in G with an advantage at least ε.

2.3 Shamir's Threshold Secret Sharing

In Shamir's (n,t) threshold secret sharing scheme, a secret $s \in GF(p)$ is partitioned into several parts s_i as a share of the secret which are distributed among a set of participants $\{P_1, \cdots, P_n\}$. The secret s could be reconstructed by subsets with at least t participants. Shamir's solution utlizes polynomial interpolation to achieve threshold secret sharing. The dealer confidentially selects a polynomial $f(x)$ of degree $t-1$ with $f(0) = s$, i.e. $f(x) = s + \sum_{i=1}^{t-1} a_i x^i \pmod p$.

If each participant P_i is assigned a unique element α_i, the dealer sends P_i the secret share $s_i = f(\alpha_i)$. A participants' group S with $|S| \geq t$ can recover the secret s by computing:

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

where:

$$\Delta_{\alpha_i, S}(x) = \prod_{P_j \in S, j \neq i} \frac{x - \alpha_j}{\alpha_i - \alpha_j} \mod p$$

On the other hand, a group T of the less than t participants could not obtain the secret s.

2.4 Generating Key Data from Biometrics

Extract cryptographic keys from biometric data is problematic since biometric information is not perfectly reproducible. Recently, Dodis [14] demonstrates how such data can be used to generate strong keys for any kind of cryptographic application. They propose the notion of fuzzy extractor to describe the process of extracting a random string U from a biometric input b. The extraction is error-tolerant in the sense that if the input changes slightly to b' then the extracted U will be the same. Dodis [14] describes three metrics to measure the variation of input data: Hamming Distance, Set Distance and Edit Distance. Hamming Distance is defined to be the number of bit positions that differ between b and b' and is proved to be the most natural and straightforward metric.

(1) Biometric Fuzzy Extraction

The fuzzy extractor construction using the Hamming distance metric is based on previous work on the fuzzy commitment scheme in [15]. A comprehensive description appears in [14,15]. Formally, a fuzzy extractor is defined as follows:

Let M be a finite dimensional metric space consisting of biometric data points with a distance function $dis: M \times M \to Z^+$ which calculates the distance between two points based on the chosen metric. Let n be the number of bits of the extracted output string U and d be the error tolerant parameter. An (M,n,d) fuzzy extractor is constructed with two functions **Gen** and **Rep**. **Gen** is a generation procedure. On input $b \in M$, the function outputs an "extracted" string $U \in \{0,1\}^n$ and public string V. **Rep** is a reproduction procedure allows recovery of U from the corresponding public string V and any b' that satisfying $dis(b,b') \le d$, i.e. $\forall b,b' \in M$ with $dis(b,b') \le d$, if $Gen(b) \to (U,V)$, then $Rep(b',V) \to U$.

(2) Error-correcting Codes

Error-correcting code is an important part of the extraction process which will be mentioned in the next subsection. A code is a subset $C = \{c_1, c_2, \cdots, c_{2^k}\} \subseteq \{0,1\}^n$, $|C| = 2^k$, $n > k$ which is referred to as *codebook* and the elements c_i in codebook are called *codeword*. Given a codebook C, we define a pair of functions $< C_e, C_d >$. The encoding function $C_e : M \to C$ represents a one-to-one mapping of messages to codewords. The decoding function $C_d : \{0,1\}^n \to C$ is used to map the received arbitrary n-bit string to codeword. For instance, the decoding function of $[n,k,2d+1]$ BCH error-correcting code maps a given n-bit string x to the nearest codeword in C with an error tolerant threshold of d. More details about BCH code and other error-correcting codes can be found in [13].

(3) The Process of Extraction

We now describe the construction of a fuzzy extractor for the space $M = \{0,1\}^N$ under the Hamming Distance metric.

- **Gen** function takes the biometrics b as input, then returns ω and public parameter $V = b \oplus C_e(\omega)$, in which ω represents the identity of user corresponding to biometrics b. Identity ω is used for private key extraction and V is used to recover ω when any other b' is given.
- **Rep** function takes the biometrics b' and V as input and computes:

$$\omega' = C_d(b' \oplus V) = C_d(b' \oplus b \oplus C_e(\omega) = C_d(e' \oplus C_e(\omega))$$

where $e' = b \oplus b'$. Identity $\omega' = \omega$ if and only if $dis(b,b') \le d$.

(4) Fuzzy Extractor from Sketches

A fuzzy extractor [14] extracts nearly uniform randomness R from its biometric input; the extraction is error-tolerant in the sense that R will be the same even if the input changes, as long as it remains reasonably close to the original.

Assume SS is a (M, m, m', t)-secure sketch with recovery procedure Rec, and let Ext be the (n, m', l, ε) -strong extractor based on pairwise-independent hashing (in particular, $l = m' - 2\log(1/\varepsilon)$). Then for uniformly distributed randomization strings X_1, X_2 the following algorithms (**Gen** , **Rep**) is a (M, m, m', t)-fuzzy extractor:

- $Gen(W; X_1, X_2)$: set $P = \langle SS(W; X_1), X_2 \rangle$, $R = Ext(W; X_2)$, output $\langle R, P \rangle$.
- $Rep(W', \langle V, X_2 \rangle)$: recover $W = Rec(W', V)$ and output $R = Ext(W; X_2)$.

Theorem 1. [21] Let $M_1, \cdots, M_m$ be $n \times n$-matrices over $GF(2)$ such that for every non-empty subset $I \subset [m]$ the matrix $\sum_{i \in I} M_i$ is invertible. Then the function $Ext: (\{0,1\}^n)^N \to \{0,1\}^m$ defined by

$$Ext(x_1, \cdots, x_n) = \left(\sum_{s<t} \langle x_s, M_1 x_t \rangle, \cdots, \sum_{s<t} \langle x_s, M_m x_t \rangle \right)$$

is a $(T^N_{\{0,1\}^n}(k), \varepsilon)$-strong extractor, where $\log(1/\varepsilon) = \frac{k-n}{2} - m + 1$.

Note: The efficient construction of suitable matrices $M_1, \ldots, M_m$ in the theorem is discussed in [22].

Comment: The construction of a secure fuzzy extractor to resist various kinds of attacks is an important research topic in biometric information and cryptography. For different biometric characteristics and metrics, there are distinct designs of fuzzy extractors [23-34] to be chosen according to the practical usage.

2.5 Formal Definition of Bio-IBS

2.5.1 Bio-IBS Scheme

A biometric identity based signature scheme consists of the following four algorithms Setup, Extract, Sign and Verify. They are specified as follows:

- **Setup** : Given a security parameter k and error tolerant parameter d, the algorithm generates the master secret key MK and the public parameters PK of the system.
- **Extract** : Given a biometric string b (identity ω is obtained using a fuzzy extractor) and master secret key MK, the algorithm returns the corresponding private key K_ω.
- **Sign** : Given the public parameters PK, private key K_ω corresponding to identity ω and a message M, the algorithm outputs signature σ.

- **Verify**: Given the public parameters PK, a biometric string b', the message M and corresponding signature σ, the algorithm accepts σ if it is valid and outputs $\perp$ otherwise.

2.5.2 Security Model

Definition 3: A Bio-IBS is existentially unforgeable against chosen message attack (EU-sID-CMA) if no attacker has a non-negligible advantage in the following game.

- **Init**: Adversary A outputs a challenge biometric data b^*. Challenger C extract the challenge identity ω^* (corresponding to b^*) through fuzzy extractor.
- **Setup**: Challenger C runs the setup algorithm and sends adversary A the public parameters PK.
- **Query Phase**: Adversary A issues private key extract queries and signature queries.
  a) **Extract queries**: A issues private key extract queries for biometric string b, where $b \neq b^*$. In response, C obtains the corresponding identity γ using fuzzy extraction algorithm and then runs Extract algorithm to get the private key K_γ and sends it to A.
  b) **Signing queries**: A issues signature queries of identity ω^* and any message M. In response, C runs the Extract algorithm to obtain the private key K_{ω^*} and then runs Sign algorithm to obtain a signature σ, which is forwarded to A.
- **Challenge**: Adversary A outputs a tuple $(\omega^*, M^*, \sigma^*)$ where $M^* \neq M$ for all M got from signing query phase. If σ^* is a valid signature of (ω^*, M^*), then A wins.

Definition 4: We say that a Bio-IBS is $(t, \varepsilon, q_E, q_S)$-EU-sID-CMA secure if all t time adversaries making at most q_E private key extract queries, q_S signing queries have advantage at most ε in winning the above game.

Note: The extract and sign algorithms in security model are identical to those in Bio-IBS scheme. The extract and sign queries are used to simulate that the adversary has the ability to obtain signature of any message that he wants, i.e., the process to choose message. Then, adversary's probability ε to win the game means the probability that an adversary could forge a new signature in a chosen message attack (CMA). When ε is negligible, the adversary could not succeed in CMA attack. Then, the signature is existentially unforgeable (EU) against chosen message attack (CMA).

3. An Efficient Bio-IBS Scheme

In this section, we define some notations for this paper and propose a secure and efficient biometric identity based signature scheme. The proposed scheme involves three roles: a system authority (AU), signer (SG) and a verifier (VF). We assume that AU is responsible for a private key generation center. Due to the noisy nature of biometrics, the proposed Bio-IBS allows for error tolerant in the verification phase, where a signature signed with the identity ω (extracted from biometric data b) could be verified by the identity ω' that is extracted from biometric data b', provided that ω and ω' are within a certain distance of each other.

3.1 Notations

- $E(F_{3^m})$: a supersingular elliptic curve $E: y^2 = x^3 - x + 1 (\mathrm{mod} 3^k)$
- G : a multiplicative group of the elliptic curve E whose order is a large prime p
- g : a generator of G whose order is p
- G_1 : a multiplicative group of the elliptic curve E whose order is p
- $\hat{e}$: a bilinear pair map, $\hat{e}: G \times G \to G_1$
- M : the content of a message
- C_e : encoding function of error-correcting code
- C_d :decoding function of error-correcting code
- d : the error tolerant parameter, which represents the distance that is allowed between two identities for successful verification
- H : a one-way hash function, $H: \{0,1\}^* \to G$

3.2 Proposed Scheme

3.2.1 Setup phase

AU selects a random $g_1 \in G$. Next, AU chooses a master-key $s \in Z_p^*$ and computes $g_2 = g^s$, $A = \hat{e}(g_1, g_2)$. Randomly choose $z', z_1, \cdots, z_{n_m} \in Z_p$ and compute $v' = g^{z'}, v_1 = g^{z_1}$, $\cdots, v_{n_m} = g^{z_{n_m}}$. Then SG publishes the system's public parameters

$$PK = \{g, g_1, g_2, v', v_1, \cdots, v_{n_m}, A\},$$

the master key $MSK = s$ is kept secret.

3.2.2 Extract phase

In this phase, signer SG performs the following steps to register to AU and obtain his private key.

- SG sends his biometric b to AU.
- AU extracts identity $\omega = (\mu_1, \cdots, \mu_n), \mu_i \in \{0,1\}$ from b through fuzzy extractor.
- AU generates SG's private key as follows:
  a) Choose a random $d-1$ degree polynomial $p(x) = a_0 + a_1 x + \ldots + a_{d-1} x^{d-1}$ such that $p(0) = a_0 = s$.
  b) For each $\mu_i \in \omega$, compute $d_{i,1} = (g_1 \cdot g^{H(\omega, \mu_i)})^{p(\mu_i)}, d_{i,2} = g^{-p(\mu_i)}$.
  c) AU sends $K_\omega = \{d_{i,1}, d_{i,2}\}_{\mu_i \in \omega}$ to SG confidentially.

Thus, SG obtains his private key K_ω that is corresponding to his biometric b.

3.2.3 Signature phase

To sign a message represented as a bit string $M = (m_1, \cdots, m_{n_m}) \in \{0,1\}^{n_m}$ for identity ω using private key $K_\omega = \{d_{i,1}, d_{i,2}\}_{\mu_i \in \omega}$, SG calculates $V = b \oplus C_e(\omega)$ as fuzzy commitment [15] used for verification. Then, SG selects a random $s_i \in Z_p$ for each $\mu_i \in \omega$ and outputs

signature

$$\sigma = (\sigma_1^{(i)}, \sigma_2^{(i)}, \sigma_3^{(i)})_{\mu_i \in \omega} = (d_{i,1} \cdot (v' \prod_{j=1}^{n_m} v_j^{m_j})^{s_i}, d_{i,2}, g^{-s_i}).$$

3.2.4 Verification phase

Given a signature σ on a message M for identity ω, VF performs the following steps:

- Obtain user's biometric information b' and calculate $\omega' = C_d(b' \oplus V)$ in order to obtain $\omega' = (\mu_1', \cdots, \mu_n')$.
- If $|\omega \cap \omega'| < d$, VF rejects the signature; if $|\omega \cap \omega'| \geq d$, go to the next step.
- VF chooses an arbitrary set $S \subseteq \omega \cap \omega'$ such that $|S| = d$. VF accepts the signature if and only if the following equation holds, otherwise rejects it.

$$\prod_S [\hat{e}(\sigma_1^{(i)}, g) \cdot \hat{e}(\sigma_2^{(i)}, g^{H(\omega,\mu_i)}) \cdot \hat{e}(\sigma_3^{(i)}, v' \prod_{j=1}^{n_m} v_j^{m_j})]^{\Delta_{i,S}(0)} = A \quad (1)$$

- If there is a dispute between SG and VF, VF can passes $(M, \sigma, \omega, \omega')$ to a third party (the message M has no need to be secret). The third party can verify the validity of the signature by Eq.(1).

3.3 Correctness

For all $\mu_i \in S$, we have $\mu_i = \mu_i'$. Then, correctness of the scheme is justified as follow.

$$\begin{aligned}
&\prod_S [\hat{e}(\sigma_1^{(i)}, g) \cdot \hat{e}(\sigma_2^{(i)}, g^{H(\omega,\mu_i)}) \cdot \hat{e}(\sigma_3^{(i)}, (v' \prod_{j=1}^{n_m} v_j^{m_j}))]^{\Delta_{i,S}(0)} \\
&= \prod_S [\hat{e}(d_{i,1}(v' \prod_{j=1}^{n_m} v_j^{m_j})^{s_i}, g) \cdot \hat{e}(d_{i,2}, g^{H(\omega,\mu_i)}) \cdot \hat{e}(g^{-s_i}, (v' \prod_{j=1}^{n_m} v_j^{m_j}))]^{\Delta_{i,S}(0)} \\
&= \prod_S [\hat{e}((g_1 g^{H(\omega,\mu_i)})^{p(\mu_i)} (v' \prod_{j=1}^{n_m} v_j^{m_j})^{s_i}, g) \cdot \hat{e}(g^{-p(\mu_i)}, g^{H(\omega,\mu_i)}) \cdot \hat{e}(g^{-s_i}, (v' \prod_{j=1}^{n_m} v_j^{m_j}))]^{\Delta_{i,S}(0)} \\
&= \prod_S [\hat{e}(g_1^{p(\mu_i)}, g) \cdot \hat{e}(g^{H(\omega,\mu_i)p(\mu_i)}, g) \cdot \hat{e}((v' \prod_{j=1}^{n_m} v_j^{m_j})^{s_i}, g)]^{\Delta_{i,S}(0)} \\
&\quad \cdot \prod_S [\hat{e}(g^{-p(\mu_i)}, g^{H(\omega,\mu_i)}) \cdot \hat{e}(g^{-s_i}, (v' \prod_{j=1}^{n_m} v_j^{m_j}))]^{\Delta_{i,S}(0)} \\
&= \prod_S \hat{e}(g_1^{p(\mu_i)}, g)^{\Delta_{i,S}(0)} = \hat{e}(g_1, g)^{\sum_S \Delta_{i,S}(0) p(\mu_i)} \\
&= \hat{e}(g_1, g)^s = \mathrm{A}
\end{aligned}$$

3.4 Efficiency Analysis

The number of group elements in the public parameters grows linearly with the length of message, i.e. $n_m + 4$ elements from group G and one element from group G_1. The number of group elements that compose a signer's private key and resulting signature σ grows linearly with the number of identities associated with the signer.

The number of scalar multiplications in group G for a signer to sign a message will be linear with the length of signer's identity. The procedure of signing does not need any bilinear

pairing computations. The cost of verification is dominated by $3d$ bilinear pairing operations.

4. Comparison of Existing Schemes

4.1 Notations

We first define some notations for the comparison.

- size of PP: size of public parameters
- n: length of identity
- n_m: length of message
- $|G|$: bit-length of an element in G
- $|G_1|$: bit-length of an element in G_1
- $|Z_p|$: bit-length of an element in Z_p
- ρ: time of one exponentiation in G_1
- τ: time of one scalar multiplication in G
- t_{Pair}: time of one pairing operation in G
- $(k+1)$-EP: $(k+1)$ Exponential Problem

4.2 Comparison

(1) By comparing the features of our scheme with other signature schemes [7, 8, 16-20] in **Table 1**, we can see that our scheme not only satisfies the security properties for signature scheme but also eliminates the certificate problem. Furthermore, biometric data is utilized to derive user's public key and private key.

(2) **Table 2** shows the performance comparison between the Burnett et al.'s Bio-IBS scheme [7], Liu et al.'s Bio-IBS scheme [8] and ours in terms of system parameter size, private key size, signature size, private key extraction cost, signing cost, verification cost, hardness assumption and security proof.

a) In [7], Burnett's scheme has no concrete construction of Bio-IBS, let alone security proof.

b) Liu's scheme [8] focuses on how to extract identity from biometric data and presents a toy scheme without any security proof.

c) To the author's knowledge, our scheme is the first Bio-IBS scheme with concrete construction and detailed security proof.

(3) Since fuzzy IBS possesses similar error-tolerance property as Bio-IBS, we compare the classical fuzzy IBS schemes [16, 17] and our Bio-IBS scheme in **Table 3**. We can see that our scheme achieves higher efficiency and stronger security.

a) The security of our Bio-IBS scheme is reduced to computational Diffie-Hellman(CDH) assumption, as well as the scheme in [16]. While in [17], the scheme is secure if $(k+1)$-EP assumption holds. Since the hardness of CDH problem is stronger than $(k+1)$-EP problem, the security of [16] and ours are stronger than [17].

b) Compared with [16], our scheme has shorter sizes of public parameters. Hence, communication overhead is decreased in our scheme. Moreover, [16] requires more computation in the private key extraction. Thus, our scheme has better performance than [16].

c) The chief drawback of [17] is that large amount of bilinear pairing operation is required in the private key extraction process. As well known, pairing operation is the most time

consuming operation in group G. It means that a user has to spend long time to get a valid private key. Moreover, high security could not be achieved in [17] which is mentioned in (a).

To sum up, our scheme achieves higher efficiency and stronger security compared with the existing schemes. As a result, the communication overhead of the network is decreased and the computation at the users and system authority is reduced.

Table 1. Features comparison of different signature schemes

	[7]	[8]	[16]	[17]	[18]	[19]	[20]	**Ours**
Unforgeability	×	×	○	○	×	○	○	**○**
Non-repudiatioin	○	○	○	○	○	○	○	**○**
Biometric identity	○	○	×	×	×	×	×	**○**
Without certificate	○	○	○	○	○	×	×	**○**
Security proof	×	×	○	○	×	○	○	**○**

Table 2. Comparison of existing Bio-IBS schemes

	[7]	[8]	**Ours**
Security proof	No	No	**Yes**
Size of PP	--	$2\|Z_p\|$	$\mathbf{(n_m+4)\|G\|+\|G_1\|}$
Size of Private Key	--	$\|Z_p\|$	$\mathbf{2n\|G\|}$
Size of Signature	--	$2\|Z_p\|$	$\mathbf{3n\|G\|}$
Cost of Extract	--	ρ	$\mathbf{n(2\rho+\tau)}$
Cost of Sign	--	$2\rho+\tau$	$\mathbf{n_m(2\rho+\tau)}$
Cost of Verify	--	$2\rho+\tau$	$\mathbf{3d\cdot t_{Pair}+d\cdot\rho}$
Hardness Assumption	--	--	**CDH**

Table 3. Comparison of our scheme with different fuzzy IBS schemes

	[16]	[17]	**Ours**
Biometric identity	No	No	**Yes**
Hardness Assumption	CDH	$(k+1)$-EP	**CDH**
Size of PP	$(n_m+n+4)\|G\|+\|G_1\|$	$(2n+2)\|G\|$	$\mathbf{(n_m+4)\|G\|+\|G_1\|}$
Size of Private Key	$2n\|G\|$	$n\|G\|$	$\mathbf{2n\|G\|}$
Size of Signature	$3n\|G\|$	$(n+1)\|G\|$	$\mathbf{3n\|G\|}$
Cost of Extract	$n(3\rho+2\tau)$	$n(t_{Pair}+\rho+\tau)$	$\mathbf{n(2\rho+\tau)}$
Cost of Sign	$n(2\rho+\tau)$	$2n\cdot\tau$	$\mathbf{n(2\rho+\tau)}$
Cost of Verify	$3d\cdot t_{Pair}+d\cdot\rho$	$d\cdot t_{Pair}+d\cdot\rho$	$\mathbf{3d\cdot t_{Pair}+d\cdot\rho}$

5. Security Analysis

5.1 Non-repudiation

Any third party can be convinced of the message's origin by step 4 in Section 3.2.

5.2 Unforgeability

Theorem 2. Suppose the (t',ε') CDH assumption holds in G, then the constructed Bio-IBS scheme is (t,ε,q_E,q_S) UF-sID-CMA secure, where

$$\varepsilon' = \varepsilon / (q_E + q_S), t' = t + O(d(\rho+\tau)q_E + (\rho+\tau)q_S))$$

ρ is the time for an exponentiation, τ is the time for a multiplication and d is the error tolerant parameter.

***Proof*:** Suppose there exists a $(t, \varepsilon, q_E, q_S)$ adversary A against our scheme, then we construct an algorithm C that solves the CDH problem with probability at least ε' and in time at most t'. The challenger C is given a tuple (g, g^a, g^b) of the CDH problem. The game between A and C proceeds as follows.

- ***Init***. Adversary A outputs a challenge biometric data b^*, C can extract the challenge identity $\omega^* = (\mu_1^*, \cdots, \mu_n^*)$ through fuzzy extractor.
- ***Setup***.

  1) Challenger C sets $l_m = q_E + q_S$ and randomly chooses integer $k \in Z_p$. Select at random $x', x_1, \cdots, x_{n_m}, z', z_1, \cdots, z_{n_m} \in Z_{l_m}$.

  2) Define functions for message M as follows:

$$F(M) = -kl_m + x' + \sum_{j=1}^{n_m} x_j m_j, \quad J(M) = z' + \sum_{j=1}^{n_m} z_j m_j,$$

$$K(M) = \begin{cases} 0, & x' + \sum_{j=1}^{n_m} x_j m_j \equiv 0 \ (mod\ l_m) \\ 1, & \text{otherwise.} \end{cases}$$

  3) Then challenger C calculates a set of public parameters as follows:

$$g_1 = g^a,\ g_2 = g^b,\ A = \hat{e}(g_1, g_2), v' = g_1^{-kl_m + x'} g^{z'},\ v_j = g_1^{x_j} g^{z_j}$$

  where $1 \le j \le n_m$.

  4) We can also obtain

$$v' \prod_{j=1}^{n_m} v_j^{m_j} = (g_1^{-kl_m + x'} g^{z'}) \prod_{j=1}^{n_m} (g_1^{x_j} g^{z_j})^{m_j} = g_1^{-kl_m + x' + \sum_{j=1}^{n_m} x_j m_j} g^{z' + \sum_{j=1}^{n_m} z_j m_j} = g_1^{F(M)} g^{J(M)}.$$

  5) Challenger C outputs the public parameters $\{g, g_1, g_2, v', v_1, \cdots, v_{n_m}, A\}$.

- ***Hash Queries***. Adversary A is allowed to issue hash query in any phase. Upon receiving a query on ω_i, if there exists (ω_i, l_i, g^{h_i}) in H-list, return h_i. Otherwise, do the following.

  1) If $\omega_i = \omega^*$, choose $l^* \in Z_p$ at random and compute $g^{h^*} = g^{l^*}$.

  2) Else, randomly select $l_i \in Z_p$ and compute $g^{h_i} = g^{l_i} / g_1$.

  3) Add (ω_i, l_i, g^{h_i}) to H-list and return g^{h_i} as answer.
- ***Phase 1***.

  Extract queries. Upon receiving a biometric b for private key extract query, challenger C do the following to simulate the private key.

  1. Challenger C extracts identity γ of b with fuzzy extractor, where $\gamma = (\mu_1, \cdots, \mu_n)$.

  2. C judges the relationship between γ and ω^*:

     - If $|\gamma \cap \omega^*| < d$, challenger C sets $\Gamma = \gamma \cap \omega^*$ and let Γ' be any set such that $\Gamma \subseteq \Gamma' \subseteq \gamma$, $|\Gamma'| = d - 1$. Then, let $S = \Gamma' \cup \{0\}$.
     - If $|\gamma \cap \omega^*| \ge d$, challenger C sets $\Gamma = \gamma \cap \omega^*$ and let Γ' be any set such that $\Gamma' \subseteq \Gamma \subseteq \gamma$, $|\Gamma'| = d - 1$. Then, let $S = \Gamma' \cup \{0\}$.

3. Challenger C constructs the private key.
   - For every $\mu_i \in \Gamma'$, run the above hash query to get (γ, l_i, g^{h_i}) in H-list. Then, pick $\lambda_i \in Z_p$ at random and compute $(d_{i,1}, d_{i,2}) = ((g_1 g^{h_i})^{\lambda_i}, g^{\lambda_i})$.

     Now define $\lambda_i = p(\mu_i)$ for a random polynomial $p(\cdot)$ of degree $d-1$ such that $p(0) = b$. Thus challenger C has successfully constructed $(d_{i,1}, d_{i,2})$ for $\mu_i \in \Gamma'$.
   - For every $\mu_i \in \gamma \setminus \Gamma'$, run the above hash query to get (γ, l_i, g^{h_i}) in H-list and compute:

$$d_{i,1} = (\prod_{\mu_j \in \Gamma'} (g_1 g^{h_i})^{\Delta_{\mu_j,S}(\mu_i)\lambda_j}) g_2^{l_i \Delta_{0,S}(\mu_i)}, \quad d_{i,2} = (\prod_{\mu_j \in \Gamma'} g^{\Delta_{\mu_j,S}(\mu_i)\lambda_j}) g_2^{\Delta_{0,S}(\mu_i)}.$$

   Note that $g_1 g^{h_i} = g^{l_i}$ for $\mu_i \in \gamma \setminus \Gamma'$, then we have

$$d_{i,1} = (g^{l_i(\sum_{\mu_j \in \Gamma'} \Delta_{\mu_j,S}(\mu_i) p(\mu_j))}) g^{l_i \Delta_{0,S}(\mu_i) b} = g^{l_i(\sum_{\mu_j \in \Gamma'} \Delta_{\mu_j,S}(\mu_i) p(\mu_j) + \Delta_{0,S}(\mu_i) p(0))}$$
$$= (g^{l_i})^{p(\mu_i)} = (g_1 g^{h_i})^{p(\mu_i)} = (g_1 g^{H(\gamma,\mu_i)})^{p(\mu_i)}$$
$$d_{i,2} = (g^{\sum_{\mu_j \in \Gamma'} \Delta_{\mu_j,S}(\mu_i) p(\mu_j)}) g^{\Delta_{0,S}(\mu_i) b} = g^{\sum_{\mu_j \in \Gamma'} \Delta_{\mu_j,S}(\mu_i) p(\mu_j) + \Delta_{0,S}(\mu_i) p(0)} = g^{p(\mu_i)}$$

   Thus, challenger C has successfully simulated the private key $K_\gamma = (d_{i,1}, d_{i,2})_{\mu_i \in \gamma}$ of identity γ.

- ***Signing queries***. To answer the signing query on ω^* for $M = (m_1, \cdots, m_{n_m})$, if $F(M) \equiv 0 \ (mod\ l_m)$, the challenger C aborts. Otherwise,

1. C selects a random set Γ such that $\Gamma \in \omega^*$ and $|\Gamma| = d-1$. Let $S = \Gamma \bigcup \{0\}$.
   - For $\mu_i^* \in \Gamma$, randomly pick $r_i \in Z_p$ and define $q(i) = r_i$ for a random polynomial $q(\cdot)$ of degree $d-1$ over Z_p such that $q(0) = b$.
   - For $\mu_i^* \in \omega^* \setminus \Gamma$, challenger C computes:

$$(\prod_{j=1}^{d-1} g^{r_j \Delta_{j,S}(i)}) g^{\Delta_{0,S}(i) b} = g^{\sum_{j=1}^{d-1} \Delta_{j,S}(i) q(j) + \Delta_{0,S}(i) q(0)} = g^{q(i)}.$$

2. Challenger C chooses random $s_i \in Z_p$ for every $\mu_i^* \in \omega^*$ and calculates:

$$\sigma_1^{(i)} = (g^{q(i)})^{-\frac{J(M)}{F(M)}} \cdot (g^{q(i)})^{l^*} \cdot (g^{J(M)} g_1^{F(M)})^{s_i}, \quad \sigma_2^{(i)} = g^{-q(i)}, \quad \sigma_3^{(i)} = (g^{q(i)})^{1/F(M)} g^{-s_i}$$

3. Set $\tilde{s}_i = s_i - q(i)/F(M)$. Since $g^{h^*} = g^{l^*}$ for identity ω^*, we have that

$$\begin{aligned}
\sigma_1^{(i)} &= (g^{q(i)})^{-\frac{J(M)}{F(M)}} \cdot (g^{q(i)})^{l^*} \cdot (g^{J(M)} g_1^{F(M)})^{s_i} \\
&= (g^{q(i)})^{-\frac{J(M)}{F(M)}} \cdot (g^{q(i)})^{l^*} \cdot (g^{J(M)} g_1^{F(M)})^{\frac{q(i)}{F(M)}} \cdot (g^{J(M)} g_1^{F(M)})^{s_i - \frac{q(i)}{F(M)}} \\
&= (g^{q(i)})^{-\frac{J(M)}{F(M)}} \cdot (g^{q(i)})^{l^*} \cdot (g^{q(i)})^{\frac{J(M)}{F(M)}} \cdot g_1^{q(i)} \cdot (g^{J(M)} g_1^{F(M)})^{s_i - \frac{q(i)}{F(M)}} \\
&= (g^{l^*})^{q(i)} \cdot g_1^{q(i)} \cdot (g^{J(M)} g_1^{F(M)})^{\tilde{s}_i} \\
&= (g^{h^*})^{q(i)} \cdot g_1^{q(i)} \cdot (v' \prod_{i=1}^{n_m} v_i^{m_i})^{\tilde{s}_i} \\
&= (g_1 g^{H(\omega^*, \mu_i)})^{q(i)} \cdot (v' \prod_{i=1}^{n_m} v_i^{m_i})^{\tilde{s}_i} \\
\sigma_2^{(i)} &= g^{-q(i)} \\
\sigma_3^{(i)} &= (g^{q(i)})^{\frac{1}{F(M)}} g^{-s_i} = (g^{q(i)})^{\frac{1}{F(M)}} g^{-\frac{q(i)}{F(M)}} g^{-\tilde{s}_i} = g^{-\tilde{s}_i}.
\end{aligned}$$

It shows that $\sigma_1^{(i)}, \sigma_2^{(i)}, \sigma_3^{(i)}$ are correctly simulated.

- ***Challenge***. Adversary A generates a valid forgery $\sigma^* = (\sigma_1^{(i,*)}, \sigma_2^{(i,*)}, \sigma_3^{(i,*)})_{\mu_i^* \in \omega^*}$ for identity ω^* on message $M^* = (m_1^*, \cdots, m_{n_m}{}^*)$, where $M^* \neq M$ for all M got from signing query phase.

1. Challenger C define:

$$F(M^*) = -2l_m k + x' + \sum_{j=1}^{n_m} x_j m_j^*, \quad J(M^*) = z' + \sum_{j=1}^{n_m} z_j m_j^*,$$

$$K(M^*) = \begin{cases} 0, & x' + \sum_{j=1}^{n_m} x_j m_j^* \equiv 0 \ (mod\ l_m) \\ 1, & \text{otherwise.} \end{cases}$$

2. If $F(M^*) \neq 0 (mod\ p)$, challenger C aborts. Otherwise, the signature must be the following form:

$$\sigma_1^{(i,*)} = g_1^{q^*(i)} (g^{l^*})^{q^*(i)} g^{J(M^*) s_i^*}, \quad \sigma_2^{(i,*)} = g^{-q^*(i)}, \quad \sigma_3^{(i,*)} = g^{-s_i^*}.$$

for some $s_i^* \in Z_p$. Since $h^* = g^{l^*}$, then:

$$\begin{aligned}
\sigma_1^{(i,*)} &= g_1^{q^*(i)} \cdot (g^{l^*})^{q^*(i)} \cdot g^{J(M^*) s_i^*} \\
&= g_1^{q^*(i)} \cdot (g^{h^*})^{q^*(i)} \cdot (g^{J(M^*)} g_1^{F(M^*)})^{s_i^*} \\
&= g_1^{q^*(i)} \cdot (g^{H(\omega^*, \mu_i)})^{q^*(i)} \cdot (v' \prod_{i=1}^{n_m} v_i^{m_i^*})^{s_i^*}
\end{aligned}$$

3. Challenger C selects a random set Λ such that $\Lambda \subseteq \omega^*$ and $|\Lambda| = d$ and calculates:

$$\begin{aligned}
\sigma_1^* &= \prod_{i\in\Lambda}(\sigma_1^{(i,*)})^{\Delta_{i,\omega^*}(i)} \\
&= \prod_{i\in\Lambda} W\cdot(g^{l^*})^{\Delta_{i,\omega^*}(i)q^*(i)}\cdot g^{\Delta_{i,\omega^*}(i)J(M^*)s_i^*} \\
&= \prod_{i\in\Lambda} W\prod_{i\in\Lambda}(g^{l^*\Delta_{i,\omega^*}(i)q^*(i)}g^{\Delta_{i,\omega^*}(i)J(M^*)s_i^*}) \\
&= g_1^b\prod_{i\in\Lambda}(g^{l^*\Delta_{i,\omega^*}(i)q^*(i)}g^{\Delta_{i,\omega^*}(i)J(M^*)s_i^*}) \\
\sigma_2^* &= \prod_{i\in\Lambda}(\sigma_2^{(i,*)})^{\Delta_{i,\omega^*}(i)l^*} = \prod_{i\in\Lambda} g^{-l^*\Delta_{i,\omega^*}(i)q^*(i)} \\
\sigma_3^* &= \prod_{i\in\Lambda}(\sigma_3^{(i,*)})^{\Delta_{i,\omega^*}(i)} = \prod_{i\in\Lambda} g^{-\Delta_{i,\omega^*}(i)s_i^*}
\end{aligned}$$

where $W = g_1^{\Delta_{i,\omega^*}(i)q^*(i)}$.

4. Challenger C could solve the CDH problem by computing

$$\sigma_1^*\cdot\sigma_2^*\cdot(\sigma_3^*)^{J(M^*)} = g_1^b = g^{ab}.$$

- **Probability Analysis**: Let *abort* be the event that the simulated game aborts.

1. We require $F(M)\neq 0\,(mod\ l_m)$ in signing phase which means that $K(M)=1\,(mod\ l_m)$ and occurs with probability $(1-1/l_m)^{q_S}$.

2. We require $F(M^*)=0\,(mod\ l_m)$ in challenge phase which means that $K(M^*)=0\,(mod\ l_m)$ and occurs with probability $1/l_m$.

3. Then:

$$Pr[\overline{abort}] = (1-\frac{1}{l_m})^{q_S}(\frac{1}{l_m}) = (1-\frac{1}{q_E+q_S})^{q_S}\cdot\frac{1}{q_E+q_S} \square \frac{1}{q_E+q_S}$$

$$\varepsilon' = Pr[\overline{abort}]\varepsilon = \varepsilon/(q_E+q_S)$$

- **Time Analysis**: The running time of the simulation is dominated by the multiplication and exponent operation in the query phase. Then we have

$$t' = t + O(d(\rho+\tau)q_E + (\rho+\tau)q_S)$$

5. Conclusion

Biometric technology has been attracting considerable attention in recent years and mainly been for highly secretive environments. In this paper, we have proposed an efficient biometric identity based signature scheme. With the adoption of Shamir's threshold secret sharing and error correction code, the suggested scheme is error tolerant and flexible. Moreover, this scheme is proved unforgeable against adaptive chosen message attack. Compared with the previous works, the proposed scheme is more secure and efficient. Meanwhile, the scheme will decrease the computational costs and improve communication efficiency of the system. An open problem is to construct efficient biometric identity based signature scheme in standard model.

References

[1] Tang Q, Bringer J, Chabanne H, and Pointcheval D, "A formal study of the privacy concerns in biometric-based remote authentication schemes," in *Proc. of 4th Int. Conf. on Information Security Practice and Experience*, vol. 4991, pp. 56-70, April 21-23, 2008. Article (CrossRef Link)

[2] Uludag U, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, 2004. Article (CrossRef Link)

[3] Boneh D, and Boyen X, "Secure identity based encryption without random oracles," in *Proc. of 24th Annual Int. Cryptology Conf.*, vol. 3152, pp. 443-459, August 15-19, 2004. Article (CrossRef Link)

[4] Sahai A, and Waters B, "Fuzzy identity-based encryption," in *Proc. of 24th Annual Int. Conf. on the Theory and Applications of Cryptographic Techniques*, vol. 3494, pp.457-473, May 22-26, 2005. Article (CrossRef Link)

[5] Kancharla PK, Gummadidala S, and Saxena A, "Identity based strong designated verifier signature scheme," *Informatica*, vol. 18, no. 2, pp. 239-252, 2007. Article (CrossRef Link)

[6] Sun X, Li J, Yin H, and Chen G, "Delegatability of an identity based strong designated verifier signature scheme," *Informatica*, vol. 21, no. 1, pp. 117-122, 2010. Article (CrossRef Link)

[7] Burnett A, Byrne F, Dowling T, and Duffy A, "A biometric identity based signature scheme," *International Journal of Network Security*, vol. 5, no. 3, pp. 317-326, 2007. Article (CrossRef Link)

[8] Liu X, Miao Q, and Li D, "A new special biometric identity based signature scheme," *International Journal of Security and its Applications*, vol. 2, no.1, pp. 13-18, 2008. Article (CrossRef Link)

[9] Maltoni D, Maio D, Jain AK, and Prabhakar S, *Handbook of Fingerprint Recognition*, Springer Publishing Company, New York, 2009. Article (CrossRef Link)

[10] Sanjay K, Dijana P, and Bernadette D, "Obtaining cryptographic keys using feature level fusion of iris and face biometrics for secure user authentication," in *Proc. of IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, pp. 138-145, June 13-18, 2010. Article (CrossRef Link)

[11] Rashid RA, Mahalin NH, Sarijari MA, "Security system using biometric technology: design and implementation of voice recognition systems," in *Proc. of Int. Conf. on Computer and Communication Engineering*, pp. 898-902, May 13-15, 2008. Article (CrossRef Link)

[12] Koelstra S, Pantic M, Dynamic A, "A dynamic texture-based approach to recognition of facial actions and their temporal models," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 11, pp. 1-15, 2010. Article (CrossRef Link)

[13] Huffman WC, Pless V, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003. Article (CrossRef Link)

[14] Y. Dodis, L. Reyzin, A. Smith. "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97-139, 2008. Article (CrossRef Link)

[15] Juels A, Wattenberg M, "A fuzzy commitment scheme," in *Proc. of the 6th ACM Conf. on Computer and Communications Security*, pp. 28-36, November 1-4, 1999. Article (CrossRef Link)

[16] Yang P, Cao Z, and Dong X. "Fuzzy identity based signature." *Available in Cryptology ePrint Archive*. Article (CrossRef Link)

[17] Wang C, Wei C, Yang L. "A fuzzy identity based signature scheme," in *Proc. of Int. Conf. on E-Business and Information System Security*, pp. 1-5, October 17-19, 2009. Article (CrossRef Link)

[18] Wang C, Kim JH, "Two constructions of fuzzy identity based signature," in *Proc. of 2nd Int. Conf. on Biomedical Engineering and Informatics*, pp. 1-5, October 17-19, 2009. Article (CrossRef Link)

[19] Li J, Huang X, Mu Y, Susilo W, Wu Q, "Certificate-based signature: security model and efficient construction." in *Proc. of European Public Key Infrastructure Workshop*, vol. 4582, pp. 110-125, June 28-30, 2007. Article (CrossRef Link)

[20] Liu J, Baek J, Susilo W, Zhou J, "Certificate-based signature schemes without pairings or random oracles," in *Proc. of Information Security Conf.*, pp. 285-297, September 15-18, 2008. Article (CrossRef Link)
[21] Konig R, and Maurer U, "Generalized strong extractors and deterministic privacy amplification," in *Proc. of Int. Workshop on Cryptography and Coding*, vol. 3796, pp. 322–339, March 14-18, 2005. Article (CrossRef Link)
[22] Dodis Y, Elbaz A, Oliveira R, and Raz R, "Improved randomness extraction from two independent sources," in *Proc. of Int. Workshop on Randomization and Approximation Techniques in Computer Science*, pp 334-344, August 22-24, 2004. Article (CrossRef Link)
[23] Kanukurthi B, L. Reyzin, "An improved robust fuzzy extractor," in *Proc. of 6th Conf. on Security and Cryptography for Networks*, vol. 5229, pp. 156-171, September 10-12, 2008. Article (CrossRef Link)
[24] Yang B, Sun A, and Zhang W, "A Fuzzy Extractor Based on Smooth Entropy," in *Proc. of 2nd Int. Conf. on Computer Science and its Applications*, pp. 1-6, December 10-12, 2009. Article (CrossRef Link)
[25] Skoric B, Tuyls P, Guajardo J, and Preneel B, "An efficient fuzzy extractor for limited noise," *Available in Cryptology ePrint Archive*. Article (CrossRef Link)
[26] Yang B, Sun A, and Zhang W, "A fully robust fuzzy extractor," in *Proc. of IEEE Int. Conf. on Network Infrastructure and Digital Content*, pp. 552-556, October 10-11, 2009. Article (CrossRef Link)
[27] Buhan I, Doumen J, Hartel P, and Veldhuis R, "Constructing practical fuzzy extractors using QIM," Tech. Rep. TR-CTIT-07-52, Centre for Telematics and Information Technology, University of Twente, 2007. Article (CrossRef Link)
[28] Škorić B, "Security with Noisy Data I," in *Proc. of Int. Conf. on Information Hiding*, pp. 79-99, May 15-18, 2007. Article (CrossRef Link)
[29] Škorić B, "Security with Noisy Data II," in *Proc. of Int. Conf. on Information Hiding*, pp. 101-112, May 15-18, 2007. Article (CrossRef Link)
[30] Ong TS, "Fuzzy key extraction from fingerprint biometrics based on dynamic quantization mechanism," in *Proc. of Third Int. Symposium on Information Assurance and Security*, pp. 71-76, August 29-31, 2007. Article (CrossRef Link)
[31] Álvarez FH, and Encinas LH, "Biometric fuzzy extractor scheme for iris templates," in *Proc. of the 2009 World Congress in Computer Science, Computer Engineering, and Applied Computing*, pp. 563-569, July 13-16, 2009. Article (CrossRef Link)
[32] Arakala A, Jeffers J, and Horadam K, "Fuzzy extractors for minutiae-based fingerprint authentication," in *Proc. of Advances in Biometrics*, vol. 4642, pp. 760-769, August 27-29, 2007. Article (CrossRef Link)
[33] Li Q, Guo M, and Chang E, "Fuzzy extractors for asymmetric biometric representations," in *Proc. of IEEE Conf. on Computer Vision and Pattern Recognition Workshops*, pp. 1-6, June 23-28, 2008. Article (CrossRef Link)
[34] Sutcu Y, Li Q, and Memon N, "Design and analysis of fuzzy extractors for faces," in *Proc. of the SPIE Optics and Photonics in Global Homeland Security V and Biometric Technology for Human Identification VI*, vol. 7306, pp. 71-76, April 13-16, 2009. Article (CrossRef Link)

Yang Yang received the Ph.D degree in school of communication engineering from Xidian University of China in 2011. Now she is a faculty in School of Math. & Computer Science of Fuzhou University. Her main research interests include network security and security protocol.

Yupu Hu received the Ph.D degrees in school of communication engineering from Xidian University of China in 2008. Now he is a professor in School of Telecommunication Engineering of Xidian University. His main research interests include information security and cryptography.

Leyou Zhang received the Ph.D degrees in applied mathematics from Xidian University of China in 2009. Now he is an associate professor in Department of Mathematical Sciences of Xidian University. His main research interests include security protocol and public key cryptography.