Multibiometric Based Secure Encryption and Authentication Scheme with Fuzzy Extractor

Mingwu Zhang[1,3], Bo Yang[1], Wenzheng Zhang[2], Tsuyoshi Takagi[3]
(Corresponding author: Mingwu Zhang)

College of Informatics, South China Agricultural University[1]
No.383, Wushan Rd., Tianhe District, Guangzhou 510642, China
(Email: csmwzhang@gmail.com)

National Laboratory for Modern Communications, Chengdu 610041, China[2]
Graduate School of Mathematics, Kyushu University[3]
744, Motooka, Nishi-ku, Fukuoka, 819-0395, Japan
(Received Dec. 17, 2009; revised and accepted Apr. 13, 2010)

Abstract

Encryption and authentication schemes suffice for the security of information stored or exchanged by different parties, but secure key generation and distribution is a highly non-trivial matter in cryptography. Fuzzy extractor is a security primitive, which can be used to encrypt and authenticate a message using his biometric b' to reproduce extraction of an almost uniformly key from non-uniform source such as fingerprint and iris, voice sample etc, is allowed to decrypt ciphertexts created by biometric b, if and only if the two sets b and b' are close to a measured set-overlap-distance metric. Biometric security systems are being widely used for the maximum level of security requirements because of the unique of participant's biometric characteristic. In this paper, it proposes a novel multiple biometric based encryption and authentication scheme that provides confidentiality, undeniability, unforgeability and verifiability. It employs multiple biometrics to encrypt the message, and with the help of public value produced by fuzzy extractor it can reproduce the secure key from distinction biometric to decrypt the ciphertext. It also gives the security analysis including semantic secure and unforgeable in the random oracle model.

Keywords: Authentication, biometric cryptographic, encryption, semantic secure

1 Introduction

Biometric system, which has a unique identification of human being based on the principle of measurable characteristics such as fingerprint, iris and voice sample, is being widely used for providing maximum level of security requirements [3, 7, 11, 12, 18]. It has fine-grained source of information entropy which makes them an excellent candidate for distributed security requirement, and is hard to be forged and be stolen. In biometric system, neither the data is uniformly distributed, nor can it be reproduced precisely. It cannot be used directly as password or secret key [12]. Fuzzy extractor [7, 8] can overcome the obstacles of biometric secret key by introducing auxiliary public information to be reliably sent on insecure public network channel.

Biometric authentication [3, 5, 8], which is concerned with recognizing individuals by physiological or behavioral characteristics, has been widely used. Several literatures introduce the biometrics to cryptography technology [3, 9, 11, 16].Sahai and Waters proposed an encryption scheme based on fuzzy identities and attribute(FIBE or ABE) [16], which views an identity as a set of descriptive attributes that allows for a private key of a identity w to decrypt a ciphertext with an identity w' iff the identities w and w' are close to each other. The ABE scheme consider the fuzzy identity is uniformly distributed, which cannot employ in biometric systems. In [4, 10, 14, 15], authors proposed an encryption based on logic expression access structure that improved the fuzzy identity based FIBE. Dodis et al. first proposed the concept of fuzzy extractor that generates the nearly uniformly string from non-uniformly biometric data [7, 8]. Based on fuzzy extractor, Boyen et al. proposed a secure remote mutual authentication scheme with biometric data that tolerates the errors in insecure channel.

Much work has focused on addressing on the signcryption [1, 2, 6, 13, 17, 20] that provided the functions of both digital signature and encryption simultaneously. Multisigncryption is an extension of signcryption scheme for multisigners performing the signcryption operation on messages [19].

In this paper, we propose an encryption and authentication scheme called mSEAS that uses multiple biomet-

ric data to sign and encrypt the message in order to hold the confidentiality, unforgeability, verifiability etc. The mSEAS extends the multisigncryption scheme that introduces a fuzzy extractor algorithm to construct biometric key. On received the ciphertext, receiver decrypts and extracts the plaintext by multiple biometric with the hand of helper parameters $\mathcal{V}_i$. To the best knowledge of us, mSEAS is the first fuzzy extract based scheme that provides confidentiality and undeniability with multiple biometric data such as fingerprint, iris, voice etc. We provide the security proofs about confidentiality and unforgeability in the random oracle model.

The paper proceeds as follows: In Section 2 we give the basic notions such as fuzzy extractor, bilinear maps and security assumptions. The formal of biometric based encryption and authentication scheme(mSEAS) and security definitions are described in Section 3. We detail the construction of the mSEAS scheme in Section 4 and provide the security proofs in Section 5. We make a conclusion in Section 6.

2 Preliminaries

2.1 Fuzzy Extractor

Let $\mathcal{M} = \{0,1\}^n$ be a finite dimensional metric space consisting of biometric data points, with a distance function $dis : \mathcal{M} \times \mathcal{M} \rightarrow Z^+$, which calculates the distance between two points based on the metric chosen. Let l be the number of bits of the extracted output string $\mathcal{U}$ from biometric b, and t be the error threshold value(i.e for two point $b, b' \in \mathcal{M}$ has $dis(b,b') \leq t$).

Definition 1. (Fuzzy extractor) *An (m,l,t,ε)-fuzzy extractor is a pair of efficient randomized procedures* Gen,Rep *such that the following hold:*

1) Gen. *Given $b \in \mathcal{M}$, outputs an extracted string $\mathcal{U} \in \{0,1\}^l$ and a helper string $\mathcal{V} \in \{0,1\}^*$;*

2) Rep. *Takes an elements $b' \in \mathcal{M}$ and the helper string $\mathcal{V} \in \{0,1\}^*$, it reproduces the $\mathcal{U}$ if b and b' is closer enough.*

3) *Correctness. If $dis(b,b') \leq t$ and $(\mathcal{U},\mathcal{V}) \leftarrow \text{Gen}(b)$, then $\text{Rep}(b',\mathcal{V}) = \mathcal{U}$.*

4) *Security. For all m-sources W over $\mathcal{M}$, the string $\mathcal{U}$ is nearly uniform even given $\mathcal{V}$.*

The fuzzy extractor has the following property:

Property 1. *If $\text{Gen}(b) \rightarrow (\mathcal{U},\mathcal{V})$, then $\text{Rep}(b',\mathcal{V}) \rightarrow \mathcal{U}$ when $dis(b,b') \leq t$).*

If the input changes to some b' but remains close, the string $\mathcal{U}$ can be reproduced exactly. We can use $\mathcal{U}$ as an encryption/authentication key and store $\mathcal{V}$ in order to recover $\mathcal{U}$ from the biometric whenever the record needs to be accessed. The encryption scheme with biometric based fuzzy extractor shows in Figure 1.

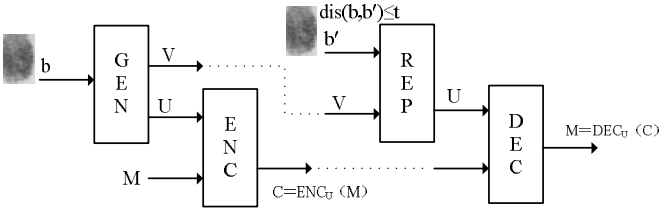

Figure 1: Secure system with fuzzy extractor

2.2 Bilinear Pairings

Let $\mathbb{G}_1, \mathbb{G}_2$ be groups of the same prime order q, and let P be a generator of $\mathbb{G}_1$. Let $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a map with the following properties:

1) Bilinearity: $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$ for all $P,Q \in \mathbb{G}_1$, and $a,b \in_R \mathbb{Z}_p$;

2) Non-degeneracy: $\hat{e}(P,Q) \neq 1$ for some $P,Q \in \mathbb{G}_1$, in other words, the bilinear map doesn't send all pairs in $\mathbb{G}_1 \times \mathbb{G}_1$ to the identity in $\mathbb{G}_2$.

3) Computable: There is an efficient algorithm to compute $\hat{e}(P,Q)$ for any $P,Q \in \mathbb{G}_1$.

2.3 Computational Assumptions

Definition 2. (Bilinear DH Problem) *Given $(P,aP,bP,cP) \in G_1$ for $a,b,c \in Z_q^*$, to compute $\hat{e}(P,P)^{abc} \in G_2$.*

Definition 3. (Decisive Bilinear DH Problem) *Given (P,aP,bP,cP,h) for $a,b,c \in Z_q$, and an element $h \in \mathbb{G}_2$, to decide whether $h = \hat{e}(P,P)^{abc}$ holds.*

Let Ω be a DBDH parameter generator. We say that an algorithm $\mathcal{B}$ has the advantage $Adv_{\Omega,\mathcal{B}}(k)$ in solving the DBDH problem for Ω in time at most $t(k)$ if for sufficiently large parameter k:

$$Adv_{\Omega,B}(k) = \Big|P_{a,b,c\in_R Z_q, h\in G_2}[1 \leftarrow \mathcal{B}(aP,bP,cP,h)] - P_{a,b,c\in_R Z_q}[1 \leftarrow \mathcal{B}(aP,bP,cP,\hat{e}(P,P)^{abc})]\Big|.$$

3 Formal Model and Security Requirements

3.1 mSEAS Scheme

We propose an multi-biometric string based encryption and authentication scheme (mSEAS) which motivated by signcryption and multisigncryption scheme [6, 19]. The mSEAS scheme consists of four algorithms as follow:

- Setup: The Public Key Generator (PKG) generates public parameters and master key.

- BioKeyExt: Take public parameters, master key, and a user's list of biometric information as input, and outputs a list of user's private keys corresponding with his multi-biometrics. In this algorithm, the fuzzy extractor function Gen should be used to construct user's public value $\mathcal{V}$.
- BioSignEnc: Takes message m, possibly some public information, and a list of biometric string $b_1, .., b_n$, and receiver public key Q_R as input, and outputs an ciphertext.
- BioDecVeri: Takes ciphertext and public parameter as input, outputs plaintext m and flag $\top$ if and only if the ciphertext could be a valid output, otherwise outputs $\perp$ as failure.

3.2 Security Notions

We formalize the mSEAS model that has two security requirements: unforgeability for adaptive message attack adversaries (UNF-mSEAS-CMA2) and indistinguish for adaptive chosen ciphertext adversaries (IND-mSEAS-CCA2).

3.2.1 Semantic Secure

The recipient of a message learns nothing about the encryption message. The game $mSEAS$ for semantic security in our scheme is described as:

Initial. The distinguisher $\mathcal{B}$ runs the Setup algorithm with a security parameter k and sends the public parameters *params* to adversary $\mathcal{A}$.

Query-I adaptively. Adversary $\mathcal{A}$ performs key extract algorithm BioKeyExt queries, BioSignEnc queries, BioDecVeri queries adaptively. These queries are the same as ID-based multisigncryption [19].

Challenge. $\mathcal{A}$ chooses two plaintext m_0, m_1 and sender biometric string $b_{S1}, ..., b_{Sn}$ and receiver PK Q_R on which he wants to be challenged. In this stage $\mathcal{A}$ cannot perform the key extract query corresponding to Q_R. $\mathcal{B}$ picks a random b from $\{0, 1\}$ and computes $\sigma = \text{BioSignEnc}(m_b, D_{s_1,s_n}, Q_R)$ and sends σ to $\mathcal{A}$.

Query-II adaptively. The adversary $\mathcal{A}$ can ask a polynomially bounded number of queries adaptively again as in the first stage with the restriction that he cannot make the key extraction BioKeyExt query on Q_R and BioDecVeri query on σ.

Response. Finally, adversary $\mathcal{A}$ returns a bit b' and wins the game if $b' = b$.

The mSEAS scheme is semantic security (IND-mSEAS-CCA2) if adversary $\mathcal{A}$ obtains the advantage $Adv(\mathcal{A})$ is negligible in mSEAS game.

$$Adv^{IND-mSEAS-CCA2}(\mathcal{A}) = |2Pr[b' = b] - 1|.$$

Note that the scheme about confidentiality is insider security since the adversary has the ability to query the private of the sender of a biometric string key extract algorithm BioKeyExt. It ensures the forward security that the confidentiality is preserved even if the sender's private key is compromised.

3.2.2 Unforgeability

The adversary's goal is to forge a valid ciphertext under the existential forgery ability of a multisigncryption scheme. We give the adversary the power to choose the multibiometric string on which wishes to forge a ciphertext, the power to request the BioKeyExt algorithm adaptively. The adversary is also given access to a BioSignEnc and BioDecVeri oracle on any desired biometric strings.

An mSEAS scheme based on multiple biometric identity strings is existentially unforgeable against chosen-message insider attack (EUF-mSEAS-CMA2) if no PPT forger $\mathcal{F}$ has a non-negligible advantage in the following game:

- Challenger runs Setup just like in mSEAS game.
- Forger $\mathcal{F}$ adaptively performs a number of queries just like in mSEAS game.
- $\mathcal{F}$ produces a ciphertext $(\sigma, ID_{s1}, ..., ID_{sn}, Q_R)$ in the sense that the key is the range of the BioKeyExt algorithm, and wins the game iff:
  (a) Ciphertext σ is not produced by BioSignEnc oracle, and
  (b) $\text{BioDecVeri}(\sigma, b_1, ..., b_n, Q_R)) \neq \perp$.

4 Construction of mSEAS

Let $\mathbb{G}_1$ be bilinear group of prime order q, and let P be a generator of $\mathbb{G}_1$. Additionally, $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow G_2$ denote the bilinear map. The proposed mSEAS scheme consists of four algorithms: Setup, BioKeyExt, BioSignEnc, and BioDecVeri. The details of the scheme are as follows:

Setup: (Input: k; Output: *params*).

The PKG generates system parameters and master key as follows:

1) On input system security parameter 1^k, generates a group $\mathbb{G}_1$ of prime order q. Constructs a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_2$ is a group of the same order q.
2) Picks a generator $P \in \mathbb{G}_1$ at random.
3) Picks a random $s \in \mathbb{Z}/q\mathbb{Z}$, computes $P_{pkg} = sP$.
4) Chooses four cryptographic hash functions H_1: $\{0, 1\}^n \rightarrow G_1$, H_2: $G_2 \rightarrow \{0, 1\}^n$, H_3: $\{0, 1\}^n \rightarrow \mathbb{Z}/q\mathbb{Z}$, H_4: $G_1 \rightarrow Z/qZ$.

5) Picks a fuzzy extractor algorithm $FE(\cdot)$ with threshold t satisfying $(\mathcal{U}, \mathcal{V}) \leftarrow FE.\textsc{Gen}(b)$, and $\mathcal{U} \leftarrow FE.\textsc{Rep}(b', \mathcal{V})$ if $dis(b, b') \leq t$.
6) Selects a symmetric cryptography (E, D). The PKG's public parameter $params = (\mathbb{G}_1, \mathbb{G}_2, q, P, P_{pkg}, \hat{e}, t, FE, E, D, H_1, H_2, H_3, H_4)$, and the system master key is s.

BioKeyExt: (Input: user with biometric string $\{b_i\}$ $(1 \leq i \leq n)$, Output: secret key $\{D_i\}(1 \leq i \leq n)$).

A user U with a list biometric strings $\{b_1, b_2, ..., b_n\}$ $\in \mathcal{M}$ generated from biometric reader.

PKG generates the U's private key set as follows:

For $i = 1$ to n, it does

1) Generates biometric parameters $(\mathcal{U}_i, \mathcal{V}_i)$ as $(\mathcal{U}_i, \mathcal{V}_i) \leftarrow \textsc{Gen}(b_i)$ using fuzzy extractor, where $\mathcal{U}_i$ is a nearly uniformly string that can only identify the biometric string b_i. $\mathcal{V}_i$ is a public value that generated by fuzzy extractor function FE.Gen, and with the help of $\mathcal{V}_i$, it can recover the $\mathcal{U}_i$ when the fuzzy biometric satisfying $dis(b_i, b_i') \leq t$.
2) Computes $Q_i = H_1(\mathcal{U}_i) \in G_1$.
3) Computes $D_i = sQ_i$. The user u_i's private key is D_i and its public key is Q_i. PKG sends U's multi-biometric private key set $\{D_i\}_{1 \leq i \leq n}$ to U via a secret channel.

BioSignEnc: (Input: plaintext m, sender U's biometric $b_1, ..., b_n$ with secret key $D_1, ..., D_n$, and receiver public key Q_R; Output: ciphertext σ).

To encrypt a plaintext m to receiver Q_R and provide the biometric authenticity, user U who has the multiple biometric string $b_1, ..., b_n$ with corresponding private key $D_1, ..., D_n$, does the following:

For $i = 1$ to n, it does

1) Picks $x_i \in_R \mathbb{Z}/q\mathbb{Z}$ at random, and computes $W_i = x_i P \in G_1$.
2) Computes $\omega_i = \hat{e}(P_{pkg}, Q_R)^{x_i} \in G_2$.
3) Computes

$$\begin{aligned} W &= \sum_{j=1}^{n} W_i, \\ \omega &= \prod_{j=1}^{n} \omega_i, \\ c &= E_{H_2(\omega)}(m), \\ S_i &= x_i H_3(c) P_{pkg} + H_4(W) D_i \in G_1, \\ S &= \sum_{j=1}^{n} S_i. \end{aligned}$$

Finally, user U outputs the ciphertext $\sigma = (c, W, S)$ as multi-biometric encryption ciphertext.

BioDecVeri: (Input: $\sigma = (c, W, S)$, decryptor Q_R with secret key D_R, and sender biometric $b_1, ..., b_n$; Output: plaintext m if success, or $\perp$ as failure).

To decrypt and verify the ciphertext $\sigma = (c, W, S)$ on message m encrypted by n biometric strings $b_1, ..., b_n$, the receiver Q_R who has the secret key D_R does the following:

1) Requests multi-biometric strings $b_i'(1 \leq i \leq n)$ by biometric reader.
2) Generates the identities by $\mathcal{U}_i \leftarrow \textsc{Rep}(b_i', \mathcal{V}_i)$, $(1 \leq i \leq n)$, with biometric fuzzy extractors such that $dis(b_i, b_i') \leq t$ for the help of public value $\mathcal{V}_i$ because the same user's two extracted biometric data error tolerant threshold is t. If $dis(b_i, b_i') > t$, extracts its biometric data again, otherwise it fails for decryption.
3) For $i = 1$ to n, computes $Q_i = H_1(\mathcal{U}_i)$.
4) Computes $\omega = \hat{e}(W, D_R)$ and $m = D_{H_2(\omega)}(c)$.
5) Checks the equation:

$$\begin{aligned} & \hat{e}(S, P) \\ = \; & \hat{e}(W, P_{pkg})^{H_3(c)} \hat{e}(P_{pkg}, \sum_{j=1}^{n} Q_i)^{H_4(W)}). \end{aligned}$$

If the above equation holds, it accepts plaintext m and outputs $\top$ as success; Otherwise, it outputs $\perp$ as reject invalid ciphertext.

5 Consistent

Clearly, the correction and consistent can be easily verified by the following two equations as

$$\begin{aligned} \hat{e}(W, D_R) &= \hat{e}(\sum_{i=1}^{n} W_i, sQ_R) \\ &= \prod_{i=1}^{n} \hat{e}(W_i, sQ_R) \\ &= \prod_{i=1}^{n} \hat{e}(x_i P, sQ_R) \\ &= \prod_{i=1}^{n} \hat{e}(P_{pkg}, Q_R)^{x_i} \\ &= \omega, \end{aligned}$$

and,

$$\begin{aligned}\hat{e}(S,P) &= \hat{e}(\sum_{i=1}^{n}(x_iH_3(c)\cdot P_{pkg}+H_4(W)\cdot D_i),P)\\ &= \hat{e}(\sum_{i=1}^{n}x_iH_3(c)P_{pkg},P)\hat{e}(\sum_{i=1}^{n}H_4(W)D_i,P)\\ &= \hat{e}(\sum_{i=1}^{n}x_iP,P_{pkg})^{H_3(m)}\hat{e}(\sum_{i=1}^{n}D_i,P)^{H_4(W)}\\ &= \hat{e}(W,P_{pkg})^{H_3(c)}\hat{e}(\sum_{i=1}^{n}sQ_i,P)^{H_4(W)}\\ &= \hat{e}(W,P_{pkg})^{H_3(c)}\hat{e}(P_{pkg},\sum_{i=1}^{n}Q_i)^{H_4(W)}.\end{aligned}$$

It is clear that anyone can verify the origin of the ciphertext $\sigma=(c,W,S)$ using public verification equation:

$$\hat{e}(S,P)=\hat{e}(W,P_{pkg})^{H_3(c)}\hat{e}(P_{pkg},\sum_{i=1}^{n}Q_j)^{H_4(W)}.$$

6 Security Results

6.1 Confidentiality

Theorem 1. *(Confidentiality) Assuming the fuzzy extractor is secure in PPT against biometric identity attacks, the mSEAS scheme is* $(t,q_e,q_S,q_U,q_{H2},q_{H3},q_{H4},\epsilon)$*-IND-mSEAS-CCA2 secure in the random oracle model assuming that the DBDH problem is* ϵ*'-intractable, where* $\epsilon'\geq(\epsilon-2^{1-k}q_U)/2q_e^2$.

Proof. We assume the distinguisher $\mathcal{B}$ receives a random instance $(P,aP,bP,\ cP,h)$ of the DBDH problem, where $h\in\mathbb{G}_1$. Our goal is to decide whether $h=\hat{e}(P,P)^{abc}$ or not. We use the attacker $\mathcal{A}$ as a subroutine for answer the IND-mSEAS-CCA2 in order to distinguish whether $\hat{e}(P,P)^{abc}$ holds or not. In the whole game, $\mathcal{A}$ will consult $\mathcal{B}$ for answers to the random oracles H_1,H_2,H_3,H_4. $\mathcal{B}$ needs to maintain hash lists L_1,L_2,L_3,L_4 that are initially empty and are used to keep track of answers to queries asked by $\mathcal{A}$ to oracle $H_i(1\leq i\leq 4)$.

At the beginning of the game, $\mathcal{B}$ sets system public key with $P_{pkg}=aP$ and sends P_{pkg} to $\mathcal{A}$. Note that value a is unknown to $\mathcal{B}$ and plays the roles of the PKG's master key in the game. The identities of n biometric strings are denoted by $b_1,...,b_n$. chooses a random number $i\in\{1,...,n\}$ as challenged identity index.

Query-I: $\mathcal{A}$ performs a series of queries of the following kinds that are handled by as explained below:

H_1-Oracles: When $\mathcal{A}$ asks H_1 queries with b_j, $\mathcal{B}$ answers as: if $j=i$, then $\mathcal{B}$ answers by $H_1(b_i)=bP$, else if $j\neq i$ then $\mathcal{B}$ picks $t_i\in Z_q^*$ randomly, and set $H_1(b_i)=t_iP$ and and records the pair (b_j,t_j) in list L_1.

H_2,H_3,H_4-Oracles: When $\mathcal{A}$ asks queries on these hash values, $\mathcal{B}$ checks the corresponding lists. If an entry for the query is found, the same answer will be given to $\mathcal{A}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{A}$, the query and the answer will then be recorded in the lists.

BioKeyExt-Oracle: When $\mathcal{A}$ makes a key extract query with b_j. If $j=i$ $\mathcal{B}$ fails and stops it; otherwise, $\mathcal{B}$ first searches L_1. If the pairs $\{b_j,t_j\}$ exists, then $\mathcal{B}$ answers the private key as $D_j=t_jP_{pkg}$, otherwise it randomly picks $t_j\in Z_q^*$ and answers $D_j=t_jP_{pkg}$ as answer and records it in L_1. The private key corresponding to b_j is $D_j=t_jP_{pkg}=at_jP$.

BioSignEnc-Oracle: For a given query of a ciphertext on the list of encryptor identities $L=\{b_1,b_2,...,b_n\}$, the receiver Q_R and a plaintext m, $\mathcal{B}$ response as follows:

- If $Q_R\neq Q_i$, he performs the following steps: (1)Randomly picks $x\in Z_q^*$ to compute $W=x\sum_{j=1}^{n}Q_i$ where $Q_i=H_1(\text{REP}(b_i,\mathcal{V}_i))$; (2)Computes $\alpha=H_4(W)$,$\omega=\hat{e}(R,D_R)$, $k=H_2(\omega)$, $c=E_k(m)$; (3)Checks if a pair $(c,*)$ exist in list L_3. If so, it aborts, otherwise it randomly selects β to set $H_3(c)=\beta P-x^{-1}\alpha P_{pkg}$; (4)Computes $S=\beta xP$; (5)$\mathcal{B}$ responds the ciphertext (c,W,S) to $\mathcal{A}$(Notes that $\mathcal{B}$ can obtain the private key D_R by BioKeyExt oracle).
- If $Q_R=Q_i$, $\mathcal{B}$ answers the queries as: (1)Picks $x\in Z_q^*$ randomly, computes $W=xP_{pkg}$, $\omega=\hat{e}(P_{pkg},xQ_R)$; (2)Computes $k=H_2(\omega)$, $c=E_k(m)$, $\alpha=H_4(W)$; (3)Checks whether the pair $(c,*)$ in L_3. If so, it aborts it, else it randomly selects β to set $H_3(c)=\beta P-x^{-1}\alpha\sum_{j=1}^{n}Q_i$, $S=x\beta P_{pkg}$. Responds the ciphertext as (c,W,S).

BioDecVeri-Oracle: For a BioDecVeri query on a ciphertext $\sigma=\{c,W,S\}$ from $\{b_1,...,b_n\}$ to Q_R, if $Q_R=Q_i$ then $\mathcal{B}$ always answers $\mathcal{A}$ that the ciphertext is invalid. If $Q_R\neq Q_i$, $\mathcal{B}$ computes $\omega=\hat{e}(W,D_R)$ and $m=D_{H_2(\omega)}(c)$. Finally, $\mathcal{B}$ computes $\alpha=H_4(W)$ and checks whether $\hat{e}(P,S)=\hat{e}(W,P_{pkg})^{H_3(c)}\hat{e}(P_{pkg},\sum_{j=1}^{n}Q_i)^{\alpha}$ holds or not. It easy to see that the probability to reject a valid ciphertext does not exceed $q_U/2^k$.

Challenge: Finally, $\mathcal{A}$ outputs two plaintext m_0^*,m_1^* together with the receiver's private key D_R on which he wishes to be challenged. $\mathcal{B}$ randomly chooses $b\in\{0,1\}$ and plaintext m_b as: (1)Set $R^*=cP$; (2)Computes $k'=H_2(h)$(where h is $\mathcal{B}$ candidate for DBDH problem); (3)Computes $c_b^*=E_h(m_b^*)$; (4)Finally, $\mathcal{B}$ returns the ciphertext $\sigma=(c_b^*,R^*,W^*)$ to $\mathcal{A}$.

Query-II: $\mathcal{A}$ performs a second series of queries in the same way of Query-I. At the end of this phrase, $\mathcal{A}$

outputs a bit b' for its guess. If $b' = b$, then it denotes that $\mathcal{B}$ can output $h = \hat{e}(R^*, D_R) = \hat{e}(cP, abP) = \hat{e}(P,P)^{abc}$ as a solution of the DBDH problem, otherwise it stops and outputs failure.

Success probability analysis: It can see that $\mathcal{B}$ fails if $\mathcal{A}$ asks the private key associated to ID_j during the first stage. With a probability greater than $1/q_{H_1}$, $\mathcal{A}$ cannot ask the query BioExtKey oracle. Furthermore, with a probability $1/q_{H_1}$, $\mathcal{A}$ chooses to be challenged on the b_j and this must allow $\mathcal{B}$ to solve his DBDH problem if $\mathcal{A}$ wins the IND-mSEAS-CCA2 game. It has,

$$\begin{aligned} p_1 &= Pr[b' = b | \omega = BioSignEnc(m_b^*, b_j, D_R)] \\ &= (\epsilon + 1)/2 - q_U/2^k. \\ p_2 &= Pr[b' = i | h \in G_2] = 1/2 \text{ for } i = 1, 2. \\ Adv(\mathcal{B}) &= |P_1 - p_2|/q_e^2 \\ &= ((\epsilon + 1)/2 - q_U/2^k - 1/2)1/q_e^2 \\ &= (\epsilon - 2^{1-k} q_U)/2q_e^2. \end{aligned}$$

□

6.2 Unforgeability

Theorem 2. *(Unforgeability) Assuming the fuzzy extractor is secure in PPT under biometric string forgery, the mSEAS scheme is $(t, q_e, q_S, q_U, q_{H_1}, q_{H_2}, q_{H_3}, q_{H_4}, \epsilon)$-UNF-mSEAS-CMA2 secure in the random oracle model assuming that the CDH problem is ϵ'-intractable, where $\epsilon' \geq \epsilon(1 - 1/q_e)^{q_e}/q_e^n$.*

Proof. We suppose that is a forger $\mathcal{F}$ who can break the mSEAS scheme in negligible advantage ϵ. Given a CDH instance $(P, xP, yP) \in G_1^3 (x, y \in_R Z_q)$, we will construct an algorithm to solve the CDH solution xyP in G_1 by using $\mathcal{F}$ as subroutine. To do so, it performs the following simulation by interacting with the forger $\mathcal{F}$.

Setup: Algorithm sets the system public key $P_{pkg} = xP$ and sends it to the forger $\mathcal{F}$.

H_1-Oracle: To respond H_1-queries with b_j, it first call FE.Gen(b_j) to generate $(\mathcal{U}_j, \mathcal{V}_j)$ and it maintains a list of tuples (b_j, w_j, t_j, c_j) as explained below. We refer to this list as L_1-list which is initially empty. When $\mathcal{F}$ makes a H_1-query with b_j, the algorithm responses as follows: If the query b_j already appears on the L_1-list in a tuple (b_j, w_j, t_j, c_j), then it responds with $H_1(b_j) = w_j \in G_1$. Otherwise, it chooses a random coin $c_j \in \{0, 1\}$ with $Pr[c_j = 0] = 1/q_e$. If $c_j = 0$, it picks $t_j \in_R Z_q$ to compute $w_j = t_j yP$. If $c_j = 1$, it picks $t_j \in_R Z_q$ to compute $w_j = t_j P$. Finally, records the tuple (b_j, w_j, t_j, c_j) in the L_1-list and answers with $w_j = H_1(b_j)$.

H_2, H_3, H_4-Oracles: When $\mathcal{F}$ asks queries on these hash values, it first checks the corresponding lists. If an entry for the query is found, the same answer will be given to $\mathcal{F}$; otherwise, a randomly generated value will be used as an answer to $\mathcal{F}$, the query and the answer will then be recorded in the lists.

BioKeyExt-Oracle: When $\mathcal{F}$ queries the private key corresponding to b_j, it first searches the tuple (b_j, w_j, b_j, c_j) in L_1-list. If $c_j = 0$, it fails and aborts. Otherwise, it computes $D_{b_j} = b_j P_{pkg}$ and responds the private key with D_{b_j}.

BioSignEnc-Oracle: For a given query of a ciphertext on the list of encryptor identities $L = \{b_1, b_2, ..., b_n\}$, the receiver Q_R and a plaintext m, it response as follows:

- If for $i = 1$ to n, it means that $H_1(b_i) = t_i P (1 \leq i \leq n)$ was previously queried. Thus, it can compute ciphertext σ by using the algorithm BioSignEnc. Otherwise, it fails and aborts it.
- If it aborts as a result of $\mathcal{F}$'s BioKeyExt queries and BioSignEnc queries, then $\mathcal{F}$'s view is identical to its view in the real attack.

Output: $\mathcal{F}$ outputs a forgery $\sigma^* = (c^*, S^*, W^*)$ on a plaintext m^* for sender $b_1^*, ..., b_n^*$ and receiver Q_R^*. By previous assumption, for $i = 1$ to n, b_i has been queried to H_1-oracle and c^* been queried to H_3-oracle. If the coins flipped for the query with all b_k^*, where $1 \leq k \leq n$, did not show 0 then declares "failure". Otherwise, if the coin flipped by $c_m^* = 1$ for c^*, then it aborts it. If $c_m^* = 0 (H_3(c^*) = b_m^* P)$, it can response as follows: (Note that we allow the adversary $\mathcal{F}$ to corrupt at most $n - 1$ signers.)

We assume the adversary has corrupted $n - 1$ signer. Without loss of generality, b_i^* is the honest signer, then $c_i^* = 1$. We have:

$$\begin{aligned} S^* &= \sum_{j=1}^{n} x_i H_3(c^*) P_{pkg} + H_4(W^*) \sum_{j=1}^{n} D_i^* \\ &= W^* H_3(c^*) + H_4(W) \sum_{j=1, j \neq i}^{n} t_j^* P_{pkg} \\ &\quad + H_4(W) t_i^* xyP. \end{aligned}$$

It means that it can solve the instance of CDH problem as:

$$\begin{aligned} xyP &= (H_4(W^*) t_i^*)^{-1} (S^* - W^* H_3(c^*) \\ &\quad + H_4(W^*) \sum_{j=1, j \neq i}^{n} t_j^* P_{pkg}). \end{aligned}$$

The success advantage ϵ' is:

$$\epsilon' \geq \epsilon(1 - 1/q_e)^{q_e}/q_e^n.$$

□

7 Conclusion

In this paper, we proposed a multibiometric encryption and authentication scheme that provides provably secure in the random oracle model. In the proposed scheme, secret key is generated by fuzzy extractor after multibiometric data is first extracted by biometric string reader. The proposed scheme can be used in biometric based authentication and data secure requirement environments. The next work is how to construct an efficient scheme without reveal any biometric data for privacy considerations.

Acknowledgement

This work is supported by the National Natural Science Foundation of China under Grant 60773175 and 60973134, the Foundation of National Laboratory for Modern Communications under Grant 9140c1108020906, the Natural Science Foundation of Guangdong Province under Grants 10151064201000028 and 10351806001000000, the Foundation for Distinguished Young Talents in Higher Education of Guangdong(wym09066), and the Support of JSPS Postdoctoral Fellowship, Japan.

References

[1] J. Baek, R. Steinfeld, Y. Zheng, "Formal proofs for the security of signcryption," *Journal of Cryptology*, vol. 20, pp. 203-235, 2007.

[2] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. J. Quisquater, "Efficient and provably-secure identity based signatures and signcryption from bilinear maps," *Advance in Cryptology (AsiaCrypt'05)*, LNCS 3788, pp. 515-532, Springer-Verlag, 2005.

[3] X. Boyen, Y. Dodis, J. Kata, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometric data," *Advances in Cryptology (Eurocrypt'05)*, LNCS 3494, Springer-Verlag, pp.147-163, 2005.

[4] X. Boyen, B. Waters, "Anonymous hierarchical identity-based encryption without random oracles," *Advances in Cryptology (Crypto'06)*, LNCS 4117, pp. 290-307, 2006.

[5] A. Broemme, "A risk analysis approach for biometric authentication technology," *International Journal of Network Security*, vol. 2, no. 1, pp. 290-307, 2006.

[6] S. S. M. Chow, S. M. Yiu, L. C. K. Hui, and K. P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," *Information Security and Cryptology (ICISC 2003)*, LNCS 2971, pp. 352-369, Springer-Verlag, 2004.

[7] Y. Dodis, J. Katz, L. reyzin, A Smith, "Robust fuzzy extractors and authenticated key aggreement from close secrets," *Advances in Cryptology (Crypto'06)*, pp. 232-250, Springer-Verlag, 2006.

[8] Y. Dodis, R. Osrovsky, L. Reyzin, A Smith, "Fuzzy extractor: How to generate strong keys from biometrics and other noisy data," *Advances in Cryptology'04*, pp. 523-540, Springer-Verlag, 2004.

[9] S. V. K. Gaddam and M. Lal, "Efficient gancelable biometric key generation scheme for cryptography," *International Journal of Network Security*, vol. 11, no. 2, pp. 61-69, 2010.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *In Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS'06)*, pp. 89-98, 2006.

[11] F. Hao, R. Anderson, J. Daugman, "Combining cryptography with biometrics effectively," *University of Cambridge, UK*, Technical report, No. 640, 2005.

[12] A. Juels, M. Wattenberg, "A fuzzy commitment scheme," *Proceeding of the 6th ACM conference on computer and communication security (CCS99),* pp.28-36, 1999.

[13] C. K. Li, G. Yang, D. S. Wong, X. Deng, and S. S. M.Chow, "An efficient signcryption scheme with key privacy," *EuroPKI 2007*, LNCS 4582, pp.78-93, Springer-Verlag, 2007.

[14] R. Ostrovsky, A. Sahai, B. Waters, "Attribute-based encryption with nonmonotonic access structures," *Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS'07)*, pp. 195-203, 2007.

[15] Y. Ren, and D. Gu, "Efficient hierarchical identity-based encryptio scheme in the standard model," *Informatica*, vol. 32, no. 2, pp. 207-211, 2008.

[16] A. Sahai, B. Waters, "Fuzzy identities and attributed-based encryption," *Proceedings of the Security with Noisy Data*, pp.113-125, Springer London, 2007.

[17] M. Toorani and A. A.B. Shirazi, "Cryptanalysis of an elliptic curve-based signcryption scheme," *International Journal of Network Security*, vol. 10, no. 1, pp. 51-56, 2010.

[18] D. Yang, B. Yang, "A new password authentication scheme using fuzzy extractor with smart card," *International Conference on Computational Intelligence and Security (CIS 2009)*, IEEE-CS, pp. 278-282, 2009.

[19] J. Zhang, J. Mao, "A novel identity-based multisigncryption scheme," *Computer Communication*, vol. 32, no. 1, pp. 14-18, 2008.

[20] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost(signature) + cost(encryption)," *Advances in Crypto'97*, LNCS 1294, pp. 165-179, Springer-Verlag, 1997.

Mingwu Zhang is an associate professor at South China Agricultural University, and current a Postdoctoral fellow at Kyushu University in Japan supported by JSPS. He received his M.S. in computer science and engineering from Hubei Polytechnic University in 2000, and the Ph.D degree in South China Agricultural

University in 2009, respectively. He is a senior member of Chinese Computer Federation (CCF), a senior member of Chinese Association for Cryptologic Research(CACR), and a member of IEEE Computer Society. He now serves for the organization committee chair for JWIS2010. His research interests include network and information security, trusted and secure computing (E-mail: csmwzhng@mail.com).

Bo Yang received his B. S. degree from Peking University in 1986, and the M. S. and Ph. D. degrees from Xidian University in 1993 and 1999, respectively. From July 1986 to July 2005, he had been at Xidian University, from 2002, he had been a professor of National Key Lab. of ISN in Xidian University, supervisor of Ph.D. He had served as a Program Chair for the CCICS2005, and ChinaCrypt2009. He severed the co-Chair of JWIS2010. He is currently a professor and supervisor of Ph.D. at College of Information, South China Agricultural University. He is a senior member of Chinese Institute of Electronics (CIE), a member of specialist group on information security in Ministry of Information Industry of China and a member of specialist group on computer network and information security in Shanxi Province. His research interests include information theory and cryptography (E-mail: byang@scau.edu.cn)

Wenzheng Zhang is a senior research fellow in National Laboratory for Modern Communications, China. He is a senior member of Chinese Computer Federation (CCF). His research interests include distributed network, information security, and trusted computing (E-mail: scausoft@tom.com).

Tsuyoshi Takagi received his B.Sc. and M.Sc. degrees in mathematics from Nagoya University in 1993 and 1995, respectively. He had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He received the Dr.rer.nat degree from Technische University Darmstadt in 2001. He was an Assistant Professor in the Department of Computer Science at Technische University Darmstadt until 2005, and a Professor at the School of Systems Information Science in Future University-Hakodate, Japan until 2009. He is currently a Professor in Graduate School of Mathematics, Kyushu University. His current research interests are information security and cryptography. Dr. Takagi is a memeber of International Association for Cryptologic Research(IACR).