An Efficient Biometric Certificateless Signcryption Scheme

Ming Luo
School of Software, Nanchang University, Nanchang 330047, P. R. China
Email: lmhappy21@163.com

Donghua Huang and Jun Hu
School of Software, Nanchang University, Nanchang 330047, P. R. China
Email: eighteenth18@163.com, jx_hujun@163.com

***Abstract*—Biometric signcryption, which enables a user using his biometric information as the identity to fulfills both the functions of encryption and digital signature simultaneously, and it provides better overall security and performance. However, almost all biometric signcryption schemes that have been proposed in the literature do not satisfy forward secrecy, known session-specific temporary information security and public verifiability with confidentiality, also have the certificate management complexity or key escrow issues which are inherent in traditional public key and identity-based cryptography respectively. In order to solve these problems, a novel biometric signcryption using certificateless public key cryptography is introduced, the formal definition and security notion of the biometric certificateless signcryption (BCSC) are presented, and a concrete BCSC scheme is also proposed in this paper. The proposed scheme eliminates the above security shortcomings and it does not have the certificate management complexity and key escrow issue by exploiting the certificateless public key cryptography. Moreover, the proposed scheme only requires one bilinear pairing operation, which makes it applicable to the resource-constrained communication devices and the communication networks with high security requirements.**

***Index Terms*—cryptography; biometric certificateless signcryption; forward secrecy; random oracle**

I. Introduction

Signcryption is a high performance cryptographic primitive first proposed by Zheng in 1997 as an approach to perform both the functionality of encryption and signature in a single operation, and is more efficient than the sign-then-encrypt approach. In the early decades, many signcryption schemes [1, 2] have been presented using the conventional public key infrastructure (PKI). In PKI, certificate issued by certification authority (CA) is used to bind user's identity and their public keys. This brings the complex problems associated all users certificate management including certificate generation, distribution, revocation and storage, as well as the communication and computation overheads of certificate verification. To mitigate the burden of conventional PKI, Shamir introduced the notion of Identity-Based Cryptography (IBC). In the IBC system, the user's public key is replaced by any binary strings that uniquely represent the user and the user's private key is generated and distributed by a trusted authority called private key generator (PKG), which gets rid of the certificates. The concept of identity-based signcryption (IBSC) was first presented by Malone-Lee in [3]. Subsequently, many IBSC schemes are proposed [4, 5]. However, in IBC all users' private keys are not selected by the users but rather issued by the PKG, which unfortunately introduces the key distribution and escrow problems, and also has the security risk since the PKG can decrypt and forge any signcryption in an IBSC scheme.

A new cryptographic primitive called certificateless cryptography was introduced by Al-Ryiami and Paterson [6] in 2003 in order to address the key distribution and escrow problems while avoiding the use of certificate which are inherent in identity-based and traditional public key cryptography respectively. In the certificateless cryptography system, the user's private key is divided into two parts. A trusted third party called key generation center (KGC) is also used to generate all users' private keys, but he only help users generate a partial private key. The other part of private key named secret value is selected by the users themselves and the KGC cannot obtain this secret value. In 2008, Barbosa and Farshim [7] proposed the first certificateless signcryption (CLSC) scheme along with a security model, where the model dealt with security notions of confidentiality and unforgeability for CLSC. Recently, a number of efficient CLSC schemes [8, 9] have been proposed in certificateless cryptography.

Nowadays, many security schemes use the user's biometric information as his identity instead of arbitrary strings like an IP address since the biometric data is unique and inherent for a user. Some work [10, 11] in applying biometric data to cryptography has focused on the extraction of a secret from biometrics. Sahai and Waters [12] pointed out in above biometric security schemes [10, 11] simply capturing a digital reading of

Corresponding author: Ming Luo (lmhappy21@163.com).
Ming Luo is supported by the National Natural Science Foundation of China under grant no. 11226042, the Science and Technology Supporting Program of Jiangxi Province under grant no. 2012ZBBE50036 and the Science and Technology Project of Jiangxi Provincial Department of Education under grant no. GJJ12147.

doi:10.4304/jcp.8.7.1853-1860

someone else's biometric would (forever) invalidate approaches where symmetric keys are systematically derived from biometric readings, and they proposed a new type of identity-based encryption called fuzzy identity-based encryption (Fuzzy-IBE) that uses biometric attributes. But the public parameters grow linearly with the number of attributes in Sahai and Waters's Fuzzy-IBE. In 2007, Baek, et al. [13] presented two new Fuzzy-IBE schemes, in which the public parameters size is independent of the number of attributes. Later, Sarier [14] introduced a new and efficient biometric IBE (Bio-IBE) scheme and achieved better efficiency in terms of the decryption and key generation algorithms compared to [13]. In 2011, Sarier [15] proposed generic constructions for Bio-IBE that require no bilinear pairings. Recently, Qing [16] proposed a new Bio-IBE scheme in the standard model. In 2007, Burnett et al. [17] presented a biometric identity-based signature scheme in which the public key is constructed by a fuzzy extractor [18]. However, Sarier [19] showed that their scheme [17] cannot resist a type of denial of service attack and they proposed an improved scheme. In 2012, Li et al. [20] formalize the concept of biometric identity-based signcryption (Bio-IBSC) and proposed a Bio-IBSC scheme in the random oracle model. Recently, Wang and Tang [21] proposed a novel biometric signcryption scheme that is identity-based and group-oriented.

All the above biometric signcryption schemes [20, 21] do not adopt the certificateless cryptography, and have the key escrow issue. In this paper, we extend the notion of biometric signcryption to the certificateless setting, and define the formal definition and security notion of the biometric certificateless signcryption (BCSC). We also proposed a concrete scheme of BCSC and formally prove its security in the random oracle model. Our BCSC scheme has the following advantages: (1) The scheme achieves forward secrecy, known session-specific temporary information security and public verifiability with confidentiality (PVC) security attributes; (2) The scheme only requires one bilinear pairing operation, and if there exits a proxy server between the sender and receiver, the users require no bilinear pairing operation since our scheme achieves PVC; (3) The scheme eliminates the certificate management complexity and key escrow issues.

The paper is organized as follows. Some background on bilinear pairings and hard problems are introduced in the next section. The formal models of BCSC are proposed in Section 3. Then, we propose a concrete BCSC scheme and provide a security proof for it in Section 4 and Section 5 respectively. In Section 6, a comparison is discussed with existing schemes. Finally, this paper ends with some concluding remarks.

II. Preliminaries

In order to introduce the new biometric certificateless signcryption scheme, firstly, we review the required mathematical preliminaries and definitions. Then we describe the fuzzy extractor method.

A. Mathematical Preliminaries

Let $(G_1, +)$ and $(G_2, \cdot)$ be an additive and multiplicative group respectively of the same prime order q. The bilinear pairing is a map $\hat{e}$ from $G_1\times G_1$ to G_2, which has the following properties.

1) Bilinear: $\hat{e}(R, S)^{xy}=\hat{e}(xR, yS)$ for all $R, S\in G_1$ and $x, y\in Z_q^*$
2) Non-degenerate: There exists R and $S\in G_1$ such that $\hat{e}(R, S)\neq 1_{G2}$
3) Computable: There exists an efficient algorithm to compute $\hat{e}(R, S)$ for all $R, S\in G_1$

The security of our biometric certificateless signcryption scheme is reduced to the well-exploited complexity assumptions, which are described as follows.

***Definition* 1.** *Elliptic Curve Discrete Logarithm Problem (ECDLP): For an integer* $k\in Z_q^*$ *and* $R, S\in G_1$, *given* $(R, S=kR)$, *computing* k *is hard.*

***Definition* 2.** *Computational Diffie-Hellman Problem (CDHP) in* G_1*: For two integers* $x, y\in Z_q^*$ *and a generator* P *of* G_1, *given* (P, xP,yP), *computing* xyP *is hard.*

***Definition* 3.** *Modified Inverse Computational Diffie-Hellman Problem (MInv-CDHP) in* G_1*: For two integers* $x, y\in Z_q^*$ *and a generator* P *of* G_1, *given* (P, xP,yP), *computing* $x^{-1}y^2P$ *is hard.*

B. Fuzzy Extractor Method

Nowadays, many security systems use the user's biometric information as his identity, such as fingerprint, voice command, retina scan, and so on. However, two biometric inputs are rarely identical. In order to solve this problem, Dodis et al. [18] showed how to generate cryptographic keys from biometric data, and proposed a new approach called fuzzy extractor, which can extract a unique string ID_U from biometric input w in a noise-tolerant way. In other words, suppose the biometric input changes to be $\hat{w}$ such that dis$(w, \hat{w})\leqq t$, the string ID_U can be reproduced exactly even if the approach is applied on a different $\hat{w}$, where dis() is the distance metric used to measure the variation in the biometric reading and t is the noise tolerance parameter of the fuzzy extractor. Three following metrics were used in the fuzzy extractor approach.

1). Hamming metric: the number of symbol positions in which the biometric input w and $\hat{w}$ differ.

2). Set difference metric: size of the symmetric difference of two biometric input sets between w and $\hat{w}$.

3). Edit metric: the number of character insertions and deletions needed to convert w into $\hat{w}$.

Hamming metric is the most convenient metric and the other two are auxiliary. Based on the hamming metric, a cryptographic hash function H and a $[n, k, 2t+1]$ BCH (Bose-Chaudhuri-Hocquenghem) error correction code, Burnett et al. [17] proposed a concrete fuzzy extractor. The definition of the fuzzy extractor is as follows:

Let $M=\{0,1\}^n$ be a metric space with finite dimensions, a distance function dis() is defined as $M\times M^{\,n}\rightarrow Z^*$ and a hash function H: $\{0,1\}^n \rightarrow \{0,1\}^l$, where l is the length of the extracted output string ID_U. The fuzzy extractor consists of two functions Gen and Rep.

Gen: The probabilistic generation procedure Gen on a biometric input $w \in M$ returns an extracted identity $ID_U = H(w)$ and a publicly reproduction parameter PAR=$w \oplus C_e(ID_U)$, where is a one-to-one encoding function.

Rep: The deterministic reproduction procedure Rep on a biometric input $\hat{w}$ and the reproduction parameter PAR outputs $ID'_U = C_d(\hat{w} \oplus \text{PAR}) = C_d(\hat{w} \oplus w \oplus C_e(ID_U))$, where C_d is a decoding function that has an error threshold of t (can correct up to t-bit errors). If dis$(w,\hat{w}) \leqq t$, then $ID'_U = ID_U$.

III. Formal Models of biometric certificateless signcryption

In this section, we present the generic model and security model of biometric certificateless signcryption.

A. Generic Model

The model of biometric certificateless signcryption is constructed using the following five algorithms:

Setup: On input of a security parameter k the KGC uses this algorithm to output master secret key and some public parameters *prms* for the system.

PartialKeyGen: On input of a user U's biometric data w, public parameters *prms* and the master secret key, the KGC uses this algorithm to output the private key D_U corresponding to w.

KeyGen: Upon input of the user U's biometric data w and public parameters *prms*, the user U uses this algorithm to output the secret value x_U and the public key PK_U for the user U.

Signcrypt: To send a message m to the receiver with biometric data w_r , secret value x_r and private key D_r, the sender with biometric data w_s , secret value x_s and private key D_s runs this algorithm along with input (m, w'_r, w_s, x_s, D_s) to compute the signcryption message σ, where dis$(w'_r, w_r) \leqq t$.

UnSigncrypt: When the receiver obtains the signcryption message σ, he uses this algorithm with input $(\sigma, w'_s, w_r, x_r, D_r)$ to outputs either the plaintext message m or the symbol $\perp$ according as whether σ is a valid signcryption or not, where dis$(w'_s, w_s) \leqq t$.

The Signcrypt and UnSigncrypt algorithms have the following consistency constraint. If dis$(w'_r, w_r) \leqq t$, dis$(w'_s, w_s) \leqq t$ and σ =signcrypt(m, w'_r, w_s, x_s, D_s),then we must have m=Unsigncrypt$(\sigma, w'_s, w_r, x_r, D_r)$.

B. Security Model

In this section, we define the security notions of BCSC. A BCSC scheme should satisfy message confidentiality and unforgeability. There are two types of adversaries in our security model as follows:

Adversary A_1: This type of adversary is not allowed to obtain the KGC's master secret key, but he can replace public key PK_U with values of his choice.

Adversary A_2: This type of adversary is allowed to obtain the master secret key but can not replace user's public key PK_U.

Definition* 4 *(Confidentiality). *A biometric certificateless signcryption (BCSC) scheme is said to have the indistinguishability against adaptive chosen ciphertext attacks (IND-BCSC-CCA2) if no polynomially bounded adversary $A_{i(i=1,2)}$ has a non-negligible advantage in the following game.*

Game

– Initial: The challenger C runs the *Setup*(k) algorithm, sends the system parameters to the adversary A_i and sends the master secret key to the adversary A_2.

– Phase1: The adversary A_i can make a polynomially bounded number of the following queries, where A_2 does not need to perform the PartialKeyGen and Replace Public Key query:

- **PartialKeyGen query:** On a PartialKeyGen(w) query for a user U, C runs the PartialKeyGen algorithm to output the private key D_U corresponding to w and returns D_U to A_1.
- **KeyGen query:** On a KeyGen(w) query for a user U, C runs the KeyGen algorithm to output the secret value x_U and the public key PK_U, adds (w, x_U, PK_U) to the list L_u. Finally, PK_U is returned.
- **Replace Public Key query:** On input of a biometric data w and a valid public key PK_U, C replaces the public key corresponding to the w with PK_U.
- **Corruption query:** On a Corruption(w) query for a user U, C checks the list L_u and returns the secret value x_U to A_i. Note that if C cannot answer the secret value of any biometric data w for which corresponding public key has been replaced.
- **Signcrypt query:** A_i produces a sender's biometric data w_s, a receiver's biometric data w_r and a plaintext message m. C computes σ =Signcrypt(m, w_r, w_s, x_s, D_s), then sends σ to A_i.
- **Unsigncrypt query:** A_i produces a sender's biometric data w_s, a receiver's biometric data w_r and a signcryption σ. C sends the result of UnSigncrypt$(\sigma, w_s, w_r, x_r, D_r)$ to A_i.

Note it is possible that the public key PK_s or PK_r has been replaced earlier by A_1 in Signcrypt or Unsigncrypt queries. If so, A_1 has to submit the corresponding secret value to C for the consistency constraint.

At the end of Phase1, A_i generates a sender's biometric data w_A, a receiver's biometric data w_B and two plaintext messages (m_0, m_1) on which he wishes to be challenged. He cannot make Corruption query on w_B in Phase 1.

– Challenge: The challenger selects a random bit b from $\{0,1\}$and computes σ^* =Signcrypt$(m_b, w_A, w_B, x_A, D_A)$, then sends σ to A_i.

– Phase 2: A_i can continue to ask the same queries that he made in the first phase. He is not allowed to make a Corruption query on w such that dis$(w, w_B) \leqq t$, also he is not allowed to make an UnSigncrypt query on σ^* with biometric data w_A and w_B unless the public key PK_A and PK_B has been replaced after the challenge phase.

– Response: A_i produces a bit b'. The adversary A_i wins the game if $b' = b$.

Definition* 5 *(Unforgeability). *A BCSC scheme is existential unforgeable under adaptive chosen messages attacks (EUF-BCSC-CMA) if no polynomially bounded time adversary $A_{i(i=1,2)}$ has a non-negligible advantage in the following game.*

Game

– Initial: The challenger C runs the *Setup*(k) algorithm, sends the system parameters to the adversary A_i and sends the master secret key to the adversary A_2.

–Probing: A_i performs a polynomially bounded number of the queries just like in the Definition 1.

–Forge: A_i produces a forgery (σ^*, w_A, w_B), where the signcryption σ^* is not generated by the signcryptiom oracle. A_i is not allowed to make a Corruption query on w such that dis(w, w_A) $\leqq t$, he wins the game if the result of UnSigncrypt(σ^*, w_A, w_B, x_B, D_B) is not the symbol $\perp$.

IV. Proposed Scheme

Our biometric certificateless signcryption scheme is constructed using the following concrete algorithms:

Setup: On input of a security parameter k the KGC chooses a bilinear pairing $\hat{e}$: $G_1 \times G_1 \rightarrow G_2$ and four cryptographic hash functions H_1: $\{0,1\}^n \rightarrow \{0,1\}^l$, H_2: $\{0,1\}^l \rightarrow Z_q^*$, H_3: $(G_1)^2 \times G_2 \rightarrow \{0,1\}^n$ and H_4: $\{0,1\}^n \times G_1 \rightarrow Z_q^*$. The KGC randomly selects a master secret key $s \in Z_q^*$ and computes the corresponding key $P_{pub} = sP$. The KGC also chooses a biometric feature extractor function B_f, a one-to-one encoding function C_e and decoding function C_d. The KGC secretly keeps the master secret key and publishes the public parameters of the system $<G_1, G_2, \hat{e}, q, P, P_{pub}, H_1, H_2, H_3, H_4, C_e, C_d, B_f>$.

PartialKeyGen: A communication user U obtains his biometric data w_U using the feature extractor function B_f and submits w_U to the KGC. The KGC computes $ID_U = H_1(w_U)$ and $D_U = s^{-1}H_2(ID_U)P$ as the private key of the user.

KeyGen: A communication user U first picks randomly a number $x_U \in Z_q^*$, computes the public key $PK_U = x_U P_{pub}$ and sets x_U as the secret value.

Signcrypt: When the sender with biometric data w_A, public key PK_A, secret value x_A and private key D_A needs to send a plaintext message m to the receiver with public parameter PAR$_B$ and public key PK_B, he performs the following steps.

1). Obtain a biometric data w'_B of the receiver together with PAR$_B$

2). Compute $ID'_B = Rep(w'_B$, PAR$_B)$

3). Compute $ID_A = H_1(w_A)$ and PAR$_A = w_A \oplus C_e(ID_A)$

4). Choose a random number $x \in Z_q^*$

5). Compute $R = xP_{pub}$ and $v = \hat{e}(D_A, P)^{H_2(ID'_B)}$

6). Compute $k_{AB} = H_3(xPK_B, x_A PK_B, v)$

7). Compute $c = m \oplus k_{AB}$ and $h = H_4(c, R)$

8). Compute $S = x^{-1}(D_A + h\, x_A H_2(ID_U) PK_A)$

9). Send the signcryption message $\sigma = (c, R, S,$ PAR$_A)$.

Unsigncrypt: When receiving $\sigma = (c, R, S,$ PAR$_A)$, the receiver with secret value x_B and private key D_B does the following steps.

1). Obtain a biometric data w'_A of the sender together with PAR$_A$

2). Compute $ID'_A = Rep(w'_A$, PAR$_A)$

3). Compute $h = H_4(c, R)$

4). Check if $\hat{e}(\frac{1}{H_2(ID'_A)} R, S) \overset{?}{=} \hat{e}(P, P)\hat{e}(PK_A, PK_A)^h$

5). If the check fails, return $\perp$. Else, perform following steps.

6). Compute $v = \hat{e}(D_B, P)^{H_2(ID'_A)}$

7). Compute $k_{AB} = H_3(x_B R, x_B PK_A, v)$

8). Recover $m = c \oplus k_{AB}$

Next, we show that our biometric certificateless signcryption scheme satisfies the consistency.

If dis(w'_A, w_A) $\leqq t$ and dis(w'_B, w_B) $\leqq t$, we have $ID_A = ID'_A$ and $ID_B = ID'_B$, so

$$\hat{e}(\frac{1}{H_2(ID'_A)} R, S)$$

$$= \hat{e}(\frac{1}{H_2(ID'_A)} xP_{pub}, x^{-1}\left(D_A + h\, x_A H_2\left(ID_U\right) PK_A\right))$$

$$= \hat{e}(\frac{1}{H_2(ID'_A)} P_{pub}, \left(s^{-1} H_2\left(ID_U\right) P + h\, x_A H_2\left(ID_U\right) PK_A\right))$$

$$= \hat{e}(P_{pub}, \left(s^{-1} P + h\, x_A P\right)) = \hat{e}(P, P)\hat{e}(PK_A, PK_A)^h$$

V. Security Analysis

In this section, we use the random oracle model to analyze the confidentiality and unforgeability security attributes of our BCSC scheme based on the Computational Diffie-Hellman Problem and Modified Inverse Computational Diffie-Hellman Problem.

A. Basic Security

***Theorem* 1.** *Assuming that the CDHP is hard, the advantage of any IND-BCSC-CCA2 adversary A_i against our biometric certificateless signcryption scheme is negligible in the random oracle model.*

Proof. On receiving the CDHP challenge tuple (P, aP, bP), where P is the generator of G_1, the goal of the distinguisher C is to compute abP. The challenger C chooses a random number $s \in Z_q^*$ as the master secret key, sets $P_{pub} = sP$, sends the system parameters to A_i and sends the master secret key to A_2. The C answers a polynomially bounded number of queries as follows.

***H_1* queries:** A_i picks the biometric data w. C sets $ID_w = H_1(w)$, adds the tuple (w, ID_w) to a list L_1 which is initially empty and answers h_1.

***H_2* queries:** A_i picks the biometric data w. We will assume that A_i makes the query $H_1(w)$ before it makes the $H_2(w)$ query. C searches an element (w, ID_w) in the list L_1 and sets $h_2 = H_2(ID_w)$. It then adds the tuple (w, h_2) to a list L_2 which is initially empty and answers h_2.

***H_3* queries:** C checks if there exists (K_1, K_2, K_3, h_3) in a list L_3 which is initially empty. If such a tuple is found, C

returns h_3, otherwise he returns A_i by a random binary sequence $h_3 \in \{0,1\}^n$ and puts the (K_1, K_2, K_3, h_3) into L_3.

***H*₄ queries:** C checks if there exists (c, R, h_4) in a list L_4 which is initially empty. If such a tuple is found, C returns h_4, otherwise he returns A_i by a random number $h_4 \in Z_q^*$ and puts the (c, R, h_4) into L_4.

PartialKeyGen queries: A_1 picks the biometric data w. C checks if there exists (w,u,D_i) in a list L_d which is initially empty. If such a tuple is found, C returns D_i, otherwise, C selects a number $u \in Z_p^*$ at random and computes $D_i = uP$, then returns D_i and adds the (w,u,D_i) into L_d.

KeyGen queries: A_i picks the biometric data w. C chooses an index $l \in \{1,2,\ldots,q_k\}$ first (suppose that C can answer at most q_k KeyGen queries). On the i-th query, if $i=l$, C sets $w_l=w$, $x_i=\perp$ and $PK_i = bP_{pub}$. Otherwise, C chooses a number $x_i \in Z_q^*$ at random and sets $PK_i=x_iP_{pub}$. In these two cases above, C adds the tuple (w, x_i, PK_i) to a list L_u which is initially empty and answers PK_i.

Replace Public Key query: A_1 picks the biometric data w and a valid corresponding public key $PK_i^{'}$, C updates L_u with the tuple $(w, \perp, PK_i^{'})$.

Corruption queries: A_i picks the biometric data w. We will assume that A_i makes the query KeyGen(w) before it makes the Corruption(w) query. If $w=w_l$, then C aborts the simulation. Otherwise, C searches the list L_u for the entry (w, x_i, PK_i) and answers x_i.

Signcrypt queries: A_i picks the sender's biometric information w_s, the receiver's biometric information w_r and a plaintext message m. We will assume that A_i makes the query Corruption(w_s) before he makes a Signcrypt query. If $w_s=w_l$, C aborts. Otherwise, C knows the secret value x_s and the private key D_s by making the PartialKeyGen(w_s) query, then answers the query according to the specification of the Signcrypt algorithm.

Unsigncrypt queries: A_i picks the sender's biometric information w_s, the receiver's biometric information w_r and a signcryption message $\sigma =(c, R, S, \mathrm{PAR}_s)$. If $w_r=w_l$, C returns $\perp$. Otherwise, C obtains the secret value x_r and private key D_r by making the Corruption(w_r) and PartialKeyGen(w_r) queries respectively, then answers the query according to the specification of the Unsigncrypt algorithm.

After the first stage, A_i generates a sender's biometric data w_s^*, a receiver's biometric data w_r^* and two plaintext messages (m_0, m_1) on which he wishes to be challenged. If $w_r^* \neq w_l$, C aborts. Otherwise, if $w_r=w_l$ and hence $w_s \neq w_l$ by the irreflexivity assumption, C first computes $ID_r^* = Rep(w_r^*, PAR_r^*)$, $ID_s^* = H_1(w_s^*)$ and $PAR_s^* = w_s^* \oplus C_e(ID_s^*)$, then randomly chooses $S^* \in G_1$, $b \in \{0,1\}$ and sets $R^*=aP$, computes $v^* = \hat{e}(D_s^*, P)^{H_2(ID_r^*)}$ and obtains $k_{AB}=H_2(\xi, x_s^* bP_{pub}, v^*)$ (where $\xi=abP$ is the candidate for the CDHP). Finally, C computes $c^*=m_b \oplus k_{AB}$ and sends the signcryption message $\sigma^* =(c^*, R^*, S^*, PAR_s^*)$ to A_i.

In the phase 2, A_i performs a series of queries as in the phase 2, At the end of the simulation, he selects a bit b' for which he believes the relation $\sigma^* =(c^*, R^*, S^*, PAR_s^*)$ holds. If $b \neq b'$, C fails the game. If $b=b'$, C will win the game due to he can recognize which message was signcrypted by seeing the signcryption alone with the session key $k_{AB}=H_2(\xi, x_s^* bP_{pub}, v^*)$, where $\xi=abP$.

So, if the adversary A_i can defeat our BCSC scheme by learning something about the signcryption message, that means there exists an efficient algorithm to solve the CDHP with non-negligible advantage. However, so far, the probability of any polynomial-time algorithm to solve CDHP is negligible. Hence, our BCSC scheme is secure against any *IND-BCSC-CCA2* adversary A_i attack.

***Theorem* 2 (Unforgeability).** *Assuming that the MInv-CDHP is hard, the advantage of any EUF-BCSC-CMA adversary A_i against our biometric certificateless signcryption scheme is negligible in the random oracle model.*

Proof. On receiving the MInv-CDHP challenge tuple (P, aP, bP), where P is the generator of G_1, the goal of the distinguisher C is to compute $a^{-1}b^2P$. The challenger C chooses a random number $s \in Z_q^*$ as the master secret key, sets $P_{pub}= sP$, sends the system parameters to A_i and sends the master secret key to A_2. The C answers a polynomially bounded number of queries as follows.

KeyGen queries: A_i picks the biometric data w. C chooses an index $l \in \{1,2,\ldots,q_k\}$ first (suppose that C can answer at most q_k KeyGen queries). On the i-th query, if $i=l$, C sets $w_l=w$, $x_i=\perp$ and $PK_i = bP$. Otherwise, C chooses a number $x_i \in Z_q^*$ at random and sets $PK_i=x_iP$. In these two cases above, C adds the tuple (w, x_i, PK_i) to a list L_u which is initially empty and answers PK_i.

***H*₁, *H*₂, *H*₃, *H*₄, PartialKeyGen, Replace Public Key, Corruption, Signcrypt, Unsigncrypt queries:** these queries are the same as the Theorem 1.

Eventually, A_i chooses a valid forgery signcryption message $\sigma^* =(c^*, R^*, S^*, PAR_s^*)$ on some message m^* from the sender w_s^* to the receiver w_r^*. C calls the KeyGen query on w_s^* and checks if $w_s^*=w_l$ and if this is not the case he aborts; otherwise he obtains D_s^* by calling the PartialKeyGen oracle on w_s^* and retrieves $H_2(ID_s^*)$ and $h=H_4(c^*, R^*)$ from the lists L_2 and L_4 respectively. If σ^* is a valid signcryption message from the sender w_s^* to the receiver w_r^*, that is, a plaintext m^* is returned by the unsigncrypt algorithm, then C applies the oracle replay technique to produce two valid signcryptions $\sigma' =(c', R', S', PAR_s^{'})$ and $\sigma'' =(c'', R'', S'', PAR_s^{''})$ on some message m from the sender w_s^* to the receiver w_r^*, where $R' = R''=aP$. C unsigncrypts σ' and σ'' to obtain the signatures $S' =x^{-1}(D_s^* + h' x_s^* H_2(ID_s^*)PK_s^*)$ and $S'' = x^{-1}(D_s^* + h'' x_s^* H_2(ID_s^*)PK_s^*)$. Now we can apply standard arguments for the outputs of the forking lemma since both S' and S'' are valid signatures for the same message m and same random tape of the adversary. Finally, C obtains the solution to the MInv-CDHP instance as $H_2(ID_s^*)^{-1}(h'-h'')^{-1}(S' - S'')$. We have

$H_2(ID_s^*)^{-1}(h'-h'')^{-1}(V' - V'')$

$$= H_2(ID_s^*)^{-1}\ (h^{'}\text{-}h^{''})^{-1}(h^{'}\text{-}h^{''})\ x^{-1}\ x_s^* H_2(ID_s^*)PK_s^*$$

$$=x^{-1}\ x_s^* PK_s^*\ P=a^{-1}b^2P$$

So, if the adversary A_i can forge a valid signcryption message of our BCSC scheme by learning something about the signcryption message, that means there exists an efficient algorithm to solve the MInv-CDHP with non-negligible advantage. However, so far, the probability of any polynomial-time algorithm to solve MInv-CDHP is negligible. Hence, our BCSC scheme is secure against any *EUF-BCSC-CMA* adversary A_i attack.

B. Further Security Considerations

In this subsection we will heuristically argue that our biometric certificateless signcryption scheme achieves the following two security properties and show that Li et al's scheme [20] does not satisfy these security properties.

1). Forward Secrecy (FS): In our BCSC scheme, compromise of the i-th decryption key $(k_{AB})_i$=$H_3(x_iPK_B$, x_APK_B, $v)$ =$H_3(x_BR_i$, x_BPK_A, $v)$ will not affect the secrecy of the later j-th decryption key $(k_{AB})_j$. Further, suppose the adversary obtains the sender's private key D_A or receiver's private key D_B does not affect the secrecy of the j-th signcryption message and cannot recover the plaintext m_j. For the adversary, he can compute the value v, but he can't compute x_jPK_B or x_BR_j. Given (R_j, PK_B), it is hard to compute x_jPK_B or x_BR_j under the assumption of CDHP and it is hard to compute x_j or x_B under the assumption of ECDLP. Hence, our BCSC scheme satisfies the forward secrecy. But in Li et al's scheme [20] if the receiver's private key S_{ID_B} is compromised by the adversary, then the adversary can compute the decryption key r= $\hat{e}(T, S_{ID_B})$ and can recover the plaintext m=$c \oplus H_3(r)$.

2). Known session-specific temporary information security (KSSTIS): Compromising the sender's ephemeral key does not enable the adversary to obtain the decryption key. Specifically, for our BCSC scheme, obtaining the sender's ephemeral key x, allows the adversary A_i to compute x_iPK_B and the adversary A_2 can compute the value v. However, the adversary A_i still cannot compute the encryption key k_{AB}=$H_3(xPK_B$, x_APK_B, $v)$=$H_3(x_BR$, x_BPK_A, $v)$, since it is hard to obtain the value x_APK_B or x_BPK_A. Given (PK_A, PK_B), it is hard to compute x_APK_B or x_BPK_A under the assumption of CDHP and it is hard to compute x_A or x_B under the assumption of ECDLP. Hence, our BCSC scheme satisfies the KSSTIS security property. But in Li et al's scheme [20] if the sender's ephemeral key x is compromised by the adversary, then the adversary can compute the decryption key r=g^x and can recover the plaintext m=$c \oplus H_3(r)$.

3). **Public verifiability with confidentiality (PVC):** Whenever necessary, the sender may submit the signcryption message σ =$(c, R, S,$ PAR$_A)$ to any verifier, who can be convinced that the signcryption σ originally came from the sender by obtaining a biometric data w'_A of the sender together with PAR$_A$, computing ID'_A=$Rep(w'_A$, PAR$_A)$ and h=$H_4(c, R)$, verifying $\hat{e}(\frac{1}{H_2(ID'_A)}R, S) \overset{?}{=} \hat{e}(P,P)\hat{e}(PK_A, PK_A)^h$. From the above analysis it is quite evident that the verifier without the knowledge of the plaintext message m can check the validity of the signcryption message in our BCSC scheme, which achieves public verifiability with confidentiality. Moreover, in our BCSC scheme, the receiver recovers the plaintext message m after he verifies the validity of the signcryption message, which improves the efficiency of Unsigncryption algorithm. But in Li et al's scheme [20], the verifier without the knowledge of the plaintext message m cannot check the validity of the signcryption message and the receiver recovers the plaintext message m before he verifies the validity of the signcryption message.

VI. Performance analysis

In this section, we compare our BCSC scheme with the Li et al's biometric identity-based signcryption scheme in Table 1. We assume that two schemes use the same parameters <G_1,G_2, $\hat{e}$,q> as defined in Section 2.

In the "security" column, the notations FS, KSSTIS and PVC refer to the forward secrecy, known session-specific temporary information security and public verifiability with confidentiality security properties respectively. Y denotes that the scheme provably achieves the security and N denotes that it does not satisfy this security.

In the "Computation Cost" column, the notations "Signcryption" and "Unsigncryption" refer to the overall computation costs not including precomputation overheads required in the Signcrypt and Unsigncrypt algorithms respectively, and we let MUL be the number of point scalar multiplications in the group G_1, EXP be the number of exponentiations in the group G_2 and PAI be the number of bilinear pairing computations.

From the Table 1, we can see that our BCSC scheme only requires one bilinear pairing operation, and if there exits a proxy server between the sender and receiver, the user requires no bilinear pairing operation since our scheme achieves PVC. As we all know, bilinear pairing

TABLE I.
A comparison of efficiency

Scheme	Security			Computation Cost	
-	FS	KSSTIS	PVC	Signcryption	Unsigncryption
Li's scheme[12]	N	N	N	3MUL+EXP	MUL+EXP+2PAI
Our scheme	Y	Y	Y	4MUL+EXP	2MUL+2EXP+PAI

computation in general is the most expensive operation in a signcryption scheme from bilinear pairing, although Li et al's scheme [20] has less multiplications and exponentiations computations, the computation time of our BCSC scheme is better since the time for 2MUL+2EXP is more than the time for one bilinear pairing operation. Moreover, our BCSC scheme satisfies the forward secrecy, known session-specific temporary information security and public verifiability with confidentiality security properties.

VII. Conclusions

In this paper, we define the formal notion of biometric certificateless signcryption and propose a concrete BCSC scheme from bilinear pairing. Our scheme admits a security analysis in the random oracle model. Moreover, The scheme only requires one bilinear pairing operation, and if there exits a proxy server between the sender and receiver, the users require no bilinear pairing operation since our scheme achieves public verifiability with confidentiality. Considering the resource-constrained communication devices and the communication networks with high security requirements, it may be that our biometric certificateless signcryption scheme is more applicable.

Acknowledgment

The authors would like to thank the reviewers for giving valuable suggestions and comments. This work is supported by the National Natural Science Foundation of China under grant no. 11226042, the Science and Technology Supporting Program of Jiangxi Province under grant no. 2012ZBBE50036 and the Science and Technology Project of Jiangxi Provincial Department of Education under grant no. GJJ12147.

References

[1] J. H. An, Y. Dodis, T. Rabin, "On the security of joint signature and encryption", in: *Proceedings of Cryptology-EUROCRYPT 2002*, Amsterdam, Netherlands, pp. 83-107, 2002.

[2] B. Libert, J. J. Quisquater, "Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups", in: *Proceedings of Public Key Cryptography-PKC 2004*, Singapore, pp. 187-200, 2004.

[3] J. Malone-Lee, "Identity-based signcryption", in: *Cryptology ePrint Archive*, Report 2002/098, pp 1-8, 2002.

[4] M. Luo, C. Zou, J. Xu, "An Efficient Identity-based Broadcast Signcryption Scheme", *Journal of Software*, vol.7, no.2, pp.366-373, 2012.

[5] W. Yuan, L. Hu, H. Li, et al, "Cryptanalysis and Improvement of an ID-Based Threshold Signcryption Scheme", *Journal of Computers*, vol.7, no.6, pp. 1345-1352, 2012.

[6] S. S. Al-Riyami, K. G. Paterson, "Certificateless Public Key Cryptography", in: *Proceedings of Cryptography-Asiacrypt 2003*, Taipei, Taiwan, pp. 452–473, 2003.

[7] M. Barbosa, P. Farshim, "Certificateless Signcryption", in: *Cryptology ePrint Archive*, Report 2008/143, pp 1-24, 2008.

[8] C. Zhou, W. Zhou, X. Dong, "Provable certificateless generalized signcryption scheme", *Designs, Codes and Cryptography*, doi.10.1007/s10623-012-9734-y, pp. 1-16, 2012.

[9] F. Li, M. Shirase, T. Takagi, "Certificateless hybrid signcryption", *Mathematical and Computer Modelling*, vol.57, pp. 324-343, 2013.

[10] F. Monrose, M. Reiter, Q. Li, et al, "Towards voice generated cryptographic keys on resource constrained device", in: *Proceedings of the 11th USENIX Security Symposium*, San Francisco, CA, USA, pp. 1-14, 2002.

[11] X. Boyen, "Reusable cryptographic fuzzy extractors", in: *Proceedings of ACM Conference on Computer and Communications Security-CCS 2004*, Washington, DC, USA, pp. 82-91, 2004.

[12] A. Sahai, B. Waters, "Fuzzy identity-based encryption", in: *Proceedings of Cryptology-Eurocrypt 2005*, Aarhus, Denmark, pp. 457-473, 2005.

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

[14] N. D. Sarier, "A new biometric identity based encryption scheme", in: *Proceedings of the 9th International Conference for Young Computer Scientists*, Zhangjiajie, China, pp. 2061–2066, 2008.

[15] N. D. Sarier, "A new biometric identity based encryption scheme secure against DoS attacks", *Security and Communication Networks*, Vol.4, no.1, pp. 23–32, 2011.

[16] Q. Wu, "Fuzzy Techniques in Biometric IBE without Random Oracles", *Applied Mechanics and Materials*, vol.148-149, pp.112-115, 2012.

[17] A. Burnett, F. Byrne, T. Dowling, et al, "A biometric identity based signature scheme", *International Journal of Network Security*, vol. 5, no.3, pp. 317–326, 2007.

[18] Y. Dodis, L. Reyzin, A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data", in: *Proceedings of Cryptology-Eurocrypt 2004*, Interlaken, Switzerland, pp. 523–540, 2004.

[19] N. D. Sarier, "Biometric identity based signature revisited", in: *Proceedings of EuroPKI 2009*, Pisa, Italy, pp. 271–285, 2010.

[20] F. Li, M K. Khan, "A biometric identity-based signcryption scheme", *Future Generation Computer Systems*, vol. 28, pp. 306–310, 2012.

[21] M. Wang, D. Tang, "A Novel Biometric Signcryption Scheme that Is Identity-based and Group-oriented", *Applied Mathematics & Information Sciences*, vol.6-3S, pp. 849-854, 2012.

Ming Luo received the B.E. and Ph.D degree from Northeastern University, Shenyang, China in 2004 and 2010, respectively. Now he is an associate professor in the School of Software, Nanchang University, Nanchang, China. He has won lots of scholarships in China and was supported by the National Natural Science Foundation of China under grant no. 60602061, 60803131 and 11226042, the National High-Tech Research and Development Plan of China under grant no. 2006AA01Z413 and the Science and Technology Supporting Program of Jiangxi Province under grant no. 2012ZBBE50036. His research interests are information security, networks security and cryptography.

Donghua Huang received the B.E. degree form the College of software, Nanchang University in July 2012. He is currently pursuing his M.E degree from the College of software, Nanchang University. His current research interests include networks security and cryptography.

Jun Hu received his PhD degree from Beijing Institute of Technology, Beijing, China in 2003. He is currently a professor in the School of Software, Nanchang University, Nanchang, China. He is a director of Chinese Association for Artificial Intelligence and a senior member of China Computer Federation. He has participated in a number of in the computer area, such as: the National High-Tech Research and Development Plan of China, National Natural Science Foundation of China, Ten Five-Year Plan of General Armament Department of China, and so on. His research interests include network security, electronic commerce and artificial intelligence.