Identity based signcryption schemes without random oracles

Prashant Kushwah[1] and Sunder Lal[2]

[1]Department of Mathematics and Statistics, Banasthali University, Rajasthan, India.
[2] Vice Chancellor, Veer Bahadur Singh Purvanchal University, Jaunpur (UP), India
Email:- [1]pra.ibs@gmail.com, [2]sunder_lal2@rediffmail.com

Abstract: Signcryption is a cryptographic primitive which performs encryption and signature in a single logical step with the cost lower than signature-then-encryption approach.. In this paper we gave attacks on confidentiality and unforgeability of two identity based signcryption schemes without random oracles. Further we proposed an improved identity based signcryption scheme without random oracles. We also proposed an identity based public verifiable signcryption scheme with third party verification without random oracles.

Keywords: Signcryption, public verifiable signcryption, identity based cryptography, provable security, standard model.

1. Introduction: The main advantages of public key cryptography are encryption and digital signature, used to achieve confidentiality and authenticity of a message respectively. There are scenarios where both primitives are needed (for example secure e-mailing). Earlier signature-then-encryption approach was followed to achieve both primitives. However, this approach has high computational cost and communication overhead. In 1997, Zheng [31] proposed a novel cryptographic primitive "Signcryption" which achieves both confidentiality and authenticity in a single logical step with the cost significantly lower than 'signature-then-encryption' approach. In 2002, Beak et al. [1] first formalize and define security notions for signcryption via semantic security against adaptive chosen cipher text attack and existential unforgeability against adaptive chosen message attack. Many public key signcryption schemes have been proposed after [31]. Some of them are [2, 13, 15, 32].

Identity based cryptography was introduced by Shamir [21] in 1984. In the identity based cryptosystem public key of users are their identities (e.g. email address, PAN number etc.) and secret keys of users are created by a trusted third party called private key generator (PKG). First identity based signature (IBS) scheme was given by Shamir [21] in 1984, but the first identity based encryption (IBE) scheme was given by Boneh and Franklin [6] in 2001. The first identity based signcryption (IBSC) scheme was proposed by Malone Lee [17] in 2002. They also gave the security model for signcryption in identity based setting. Since then, many IBSC schemes have been proposed in literature [3, 8, 11, 12, 16, 18, 20]. Their main objective is to reduce the computational complexity and to design the more efficient identity based signcryption scheme.

However, most IBSC schemes were proven secure in the random oracle model [4]. Although the random oracle methodology leads to the construction of efficient and provable secure schemes but a proof in the random oracle model can only serve as heuristic argument. It has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [10]. Many cryptographic schemes are proposed which are provably secure without random oracles (or in the standard model). Some of them are [5, 9, 14, 19, 23, 25, 26, 29, 30]. In 2009 Yu et. al. [25] proposed an IBSC scheme in the standard model based on Water et al.'s [23] encryption scheme. Many authors proved that their scheme is not secure [14, 22, 24, 27, 28]. Among them Zhang [27] and Jin et al. [14] gave improvement on Yu et al. scheme. In this paper we show that still their schemes are not secure and propose a new IBSC scheme with insider security in the standard model.

In conventional signcryption the sender signs the message which is hidden under the receiver's public key. Thus only the receiver can decrypt the message using his/her private key and can verify the authenticity of the cipher text. In the case when receiver wants to prove that indeed the sender has signed the message to a third party then he/she has to reveal his/her private key. In public verifiable signcryption scheme a third party who is unaware of the receiver's private key is able to verify whether a cipher text is valid or not. Public verifiable signcryption schemes have applications in filtering out the spam in a secure email system and private contract signing [20]. In third party verifiable signcryption schemes, a third party is able to verify the integrity and origin of the message using some additional information along with the signcryption provided by the receiver other than his/her private key. In this paper we also propose an identity based public verifiable signcryption (IBPSC) scheme with third party verification without random oracle.

This paper is organized as follows: In section 2, we give the formal definitions of IBSC and IBPSC schemes and their security model. Section 3 contains the preliminaries for the proposed scheme. In section 4, we review the Zhang [27] IBSC scheme without random oracle and give the attack on the confidentiality. In section 5, we review the Jin et al. [14] scheme and show that their scheme is not insider secure. Section 6 contains the proposed new IBSC without random oracle. In section 7, we propose the identity based public verifiable signcryption scheme with third party verification without random oracle. We conclude this paper in section 8.

2. Formal model of IBSC and IBPSC schemes:

An **identity based signcryption (IBSC) scheme** consists of the following four algorithms:

1. **Setup:** This algorithm takes input a security parameter k and outputs the system parameters **params** and a master secret key.
2. **Key Generation:** Given input params, master secret key and a user's identity ID_U, it outputs a partial private key D_U corresponding to ID_U.
3. **IBSC:** To send a message m from a user A to B, this algorithm takes input (D_A, m, ID_A, ID_B) and outputs a $\sigma = IBSC(D_A, m, ID_A, ID_B)$.
4. **IBUSC:** This algorithm takes input $(\sigma, D_B, ID_B, ID_A)$ and outputs m if σ is a valid signcryption of m done by A for B, otherwise outputs "invalid".

An **identity based public verifiable signcryption (IBPSC) scheme** consists of the following five algorithms:

1. **Setup:** This algorithm takes input a security parameter k and outputs the system parameters **params** and a master secret key.
2. **Key Generation:** Given input params, master secret key and a user's identity ID_U, it outputs a partial private key D_U corresponding to ID_U.
3. **IBPSC:** To send a message m from a user A to B, this algorithm takes input (D_A, m, ID_A, ID_B) and outputs a $\sigma = IBPSC(D_A, m, ID_A, ID_B)$.
4. **IBPUSC:** This algorithm takes input $(\sigma, D_B, ID_B, ID_A)$ and outputs m and ϕ if σ is a valid signcryption of m done by A for B, otherwise outputs "invalid".
5. **TP-Verify:** This algorithm takes input (ϕ, ID_A, ID_B) and outputs "Valid", if σ is a valid signcryption of m done by A for B, otherwise outputs "invalid".

Security model for IBSC and IBPSC schemes:

2.1. Message Confidentiality:

The notion of security with respect to confidentiality is indistinguishability of encryptions under adaptive chosen cipher text attack (IND-CCA2). For IBSC (IBPSC) this notion is captured by the following game played between challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

GAME 1 (IND-CCA2):

Initialization: $\mathcal{C}$ runs the setup algorithm on input a security parameter *k*, gives public parameters params to the adversary $\mathcal{A}$. $\mathcal{C}$ keeps the master key secret.

Queries (Find Stage): The adversary $\mathcal{A}$ makes the following queries adaptively.

- **Hash Queries:** $\mathcal{A}$ can request the hash values of any input and $\mathcal{C}$ responds with appropriate hash values.
- **Key generation Queries:** $\mathcal{A}$ submits an identity ID_U and $\mathcal{C}$ computes the private key D_U corresponding to ID_U and returns to $\mathcal{A}$.
- **IBSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B and a message *m*. Challenger $\mathcal{C}$ runs IBSC algorithm with message *m* and identities ID_A and ID_B and returns the output σ to the adversary $\mathcal{A}$.
- **IBUSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B along with σ to the challenger $\mathcal{C}$. $\mathcal{C}$ runs the IBUSC algorithm with input σ , ID_A and ID_B and returns the output *m* and ϕ if σ is a valid signcryption of m done by *A* for *B*, otherwise outputs "invalid".

No queries with $ID_A = ID_B$ is allowed.

Challenge: At the end of find stage, $\mathcal{A}$ submits two distinct messages m_0 and m_1 of equal length, a sender's identity ID_A^* and a receiver's identity ID_B^* on which $\mathcal{A}$ wishes to be challenged. The adversary $\mathcal{A}$ must have made no key generation query on ID_B^*. $\mathcal{C}$ picks randomly a bit $b \in \{0,1\}$, runs the IBSC algorithm with message m_b under ID_A^* and ID_B^* and returns the output $\sigma *$ to the adversary $\mathcal{A}$.

Queries (Guess stage): $\mathcal{A}$ queries adaptively again as in the find stage. It is not allowed to extract the private key corresponding to ID_B^* and also it is not allowed to make an IBUSC query on $\sigma *$ with sender ID_A^* and receiver ID_B^*.

Eventually, $\mathcal{A}$ outputs a bit $b'$and wins the game if $b = b'$.

$\mathcal{A}$'s advantage is defined as $Adv_{\mathcal{A}}^{IND-CCA2} = 2\Pr[b = b'] - 1$.

Definition 1: An IBSC (IBPSC) scheme is said to IND-CCA2 secure if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

Note that the confidentiality game described above deals with the insider security since the adversary is given access to the private key of sender ID_A^* in the challenge phase.

2.2. Signature (Cipher text) unforgeability:

The notion of security with respect to authenticity is existential unforgeability against chosen message attacks (EUF-CMA). For IBSC (IBPSC) this notion is captured by the following game played between challenger $\mathcal{C}$ and adversary $\mathcal{A}$.

GAME 2 (EUF-CMA):

Initialization: Same as in GAME 1.

Queries: The adversary $\mathcal{A}$ asks a polynomially bounded number of queries adaptively as in GAME 1.

Forgery: Finally, $\mathcal{A}$ produces a triplet $(ID_A^*, ID_B^*, \sigma^*)$ that was not obtained from IBSC query during the game and for which private key of ID_A^* was not exposed. The forger wins if σ^* is valid signcrypted text from ID_A^* to ID_B^*.

The adversary $\mathcal{A}$'s advantage is its probability of winning the above game.

Definition 3: An IBSC (IBPSC) scheme is said to EUF-CMA secure if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

Note that in the cipher text unforgeability game described above deals with the insider security since the adversary is given access to the private key of receiver ID_B^* in the forgery.

3. Preliminaries:

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be multiplicative groups of the prime order p and g be a generator of $\mathbb{G}_1$. A function $e:\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is called a **bilinear pairing** if it satisfies the following properties:

1. Bilinearity: for all $a,b \in \mathbb{Z}_p, e(g^a, g^b) = e(g,g)^{ab}$
2. Non-degeneracy: $e(g,g) \neq 1_{\mathbb{G}_2}$
3. Computability: e is efficiently computable.

Given $g, g^a, g^b, g^c \in \mathbb{G}_1$ for some unknown $a,b,c \in \mathbb{Z}_p$ and an element $Z \in \mathbb{G}_2$, decide whether $Z = e(g,g)^{abc}$ or not is known as **Decisional Bilinear Diffie-Hellman (DBDH) Problem**.

Given $g, g^a, g^b \in \mathbb{G}_1$ for some unknown $a,b \in \mathbb{Z}_p$ to compute g^{ab} is known as **Computational Diffie-Hellman (CDH) Problem**.

4. Review of Zhang's IBSC scheme [27]:

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e:\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha \in_R \mathbb{Z}_p$, compute $g_1 = g^\alpha$ and pick $g_2 \in_R \mathbb{G}_1$. Furthermore, pick elements $u', m', h \in_R \mathbb{G}_1$ randomly and vectors $\vec{\boldsymbol{u}} = (u_i)$, $\vec{\boldsymbol{m}} = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Let H_1, H_2 be two hash functions where $H_1 : \mathbb{G}_2 \times \mathbb{G}_2 \to \mathbb{Z}_p^*$, $H_2 : \mathbb{G}_1 \to \{0,1\}^{n_m}$. The public parameters are params = $\langle \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, u', \vec{\boldsymbol{u}}, m', \vec{\boldsymbol{m}}, h, H_1, H_2 \rangle$ and the master secret key is g_2^α.

Key Generation: Let *u* be a bit string of length n_u representing an identity and let $u[i]$ be the *i*-th bit of *u*. Define $U' \subset \{1,...,n_u\}$ to be the set of indices *i* such that $u[i] = 1$.

To construct the private key d_u of identity *u*, pick $r_u \in_R \mathbb{Z}_p^*$ and compute: $d_u = (g_2^\alpha (u' \prod_{j \in U'} u_j)^{r_u}, g^{r_u})$. Therefore, $d_A = (d_{A1}, d_{A2}) = (g_2^\alpha (u' \prod_{j \in U'_A} u_j)^{r_A}, g^{r_A})$ and

$d_B = (d_{B1}, d_{B2}) =$ $(g_2^{\alpha}(u' \prod_{j \in U'_B} u_j)^{r_B}, g^{r_B})$ are the private keys of the sender (Alice) with identity u_A and the receiver (Bob) with identity u_B respectively.

IBSC: To send a message $m \in \mathbb{G}_2$ to Bob, Alice picks $r, s \in_R \mathbb{Z}_p$ randomly and computes $R = e(g_1, g_2)^r$, $\sigma_1 = R \cdot m$, $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $t = H_1(m \,\|\, R)$, $M = H_2(g^t h^s)$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$ where $M' \subset \{1, ..., n_m\}$ is the set of indices *j* such that $m[j] = 1$ ($m[j]$ is the *j*-th bit of *M*). Next Alice sets $\sigma_5 = d_{A2}$ and $\sigma_6 = s$. The cipher text is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$.

IBUSC: On receiving the cipher text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$, Bob computes $R = e(d_{B2}, \sigma_3)^{-1} e(d_{B1}, \sigma_2)$, $m = \sigma_1 R^{-1}$, $\hat{t} = H_1(m \,\|\, R)$, $\hat{M} = H_2(g^{\hat{t}} h^{\sigma_6})$. Bob generates the corresponding set $M' \subset \{1, ..., n_m\}$ of indices *j* such that $m[j] = 1$, where $m[j]$ is the *j*-th bit of $\hat{M}$. Accept the message if and only if

$$e(\sigma_4, g) = e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2).$$

CPA attack on confidentiality: At the challenge phase of the CPA game adversary issues two messages m_0 and m_1 with a sender identity u_A^* and a receiver identity u_B^*. The challenger chooses the random bit $b \in_R \{0,1\}$ and signcrypts the message m_b to produce the challenge cipher text $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*)$. The challenger sends the σ^* to the adversary. Now adversary can guess correctly which message is signcrypted as follows:

1. She computes $R_0 = \sigma_1^* / m_0$, $\hat{t}_0 = H_1(m_0 \,\|\, R_0)$ and $\hat{M}_0 = H_2(g^{\hat{t}_0} h^{\sigma_6^*})$.
2. She generates the corresponding set $M'_0 \subset \{1, ..., n_m\}$ of indices *j* such that $m[j] = 1$, where $m[j]$ is the *j*-th bit of $\hat{M}_0$.
3. If $e(\sigma_4^*, g) = e(g_1, g_2) e(u' \prod_{j \in U'^*_A} u_j, \sigma_5^*) e(m' \prod_{j \in M'_0} m_j, \sigma_2^*)$, She returns m_0 as her guess, otherwise returns m_1.

5. Review of Jin et al.'s IBSC scheme [14]:

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha \in \mathbb{Z}_p$, compute $g_1 = g^{\alpha}$ and pick $g_2 \in_R \mathbb{G}_1$. Furthermore, pick elements $u', m' \in_R \mathbb{G}_1$ randomly and vectors $\vec{\boldsymbol{u}} = (u_i)$, $\vec{\boldsymbol{m}} = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Here public parameters are params = $\left\langle \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, u', \vec{\boldsymbol{u}}, m', \vec{\boldsymbol{m}}, H, \varphi, \varphi^{-1} \right\rangle$ and the master secret key is g_2^{α}. Cryptographic hash function *H* is defined as $H : \{0,1\}^{\ell} \to \{0,1\}^{n_m}$. $\varphi : \mathcal{R} \to \mathbb{G}_2$ is a bijection while φ^{-1} is its inverse, $\mathcal{R}$ is a subset of $\{0,1\}^{\ell + n_m}$ with *p* elements. Here ℓ is the length of the plaintext.

Key Generation: Similar to the previous scheme.

IBSC: To send a message $m \in \{0,1\}^{\ell}$ to Bob, Alice randomly picks $r \in_R \mathbb{Z}_p$ and $R \in \{0,1\}^{n_m}$ such that $m \| R \in \mathcal{R}$ and computes $\sigma_1 = e(g_1, g_2)^r \varphi(m \| R)$, $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$ where $M' \subset \{1, ..., n_m\}$ denotes the set of indices j for which the j-th bit of $H(m)$ is different from that of *R*, i.e. $M' = \{j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1\}$. Next Alice sets $\sigma_5 = d_{A2}$. The cipher text is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

IBUSC: On receiving the cipher text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, Bob

1. computes $\varphi^{-1}(\sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}) \to m \| R$
2. generates the corresponding set $M' = \{j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1\}$
3. accepts the message *m* if

$$e(\sigma_4, g) = e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2)$$

Insider CCA2 attack on confidentiality: Jin et al. [14] consider the security model which deals with the insider security [8] since the adversary is assumed to have the access to the private key of the sender of the challenged signcrypted text. Next we will show that Jin et al. [14] scheme does not have insider security.

At the challenge phase of the CCA2 game, adversary issues two messages m_0 and m_1 with a sender identity u_A^* and a receiver identity u_B^*. Note that adversary has access to the private key $d_A^* = (d_{A1}^*, d_{A2}^*) = (g_2^{\alpha}(u' \prod_{j \in U_A'^*} u_j)^{r_A^*}, g^{r_A^*})$ of sender u_A^* and does not ask any key generation query for the private key of u_B^* at any time. The challenger chooses the random bit $b \in_R \{0,1\}$ and signcrypts the message m_b to produce the challenge cipher text $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*)$. The challenger sends the σ^* to the adversary.

Adversary converts σ^* to a new valid signcrypted text σ' for receiver u_B^* from a sender u'_A and asks the IBUSC query on σ'. She returns the output of σ' as her guess of the challenge signcrypted text. Details are as follow:

1. She computes $\sigma'_4 = (d_{A1}^*)^{-1} \sigma_4^* d'_{A1}$
2. Sets $\sigma'_1 = \sigma_1^*$, $\sigma'_2 = \sigma_2^*$, $\sigma'_3 = \sigma_3^*$ $\sigma'_5 = d'_{A2}$ and $\sigma' = (\sigma'_1, \sigma'_2, \sigma'_3, \sigma'_4, \sigma'_5)$

Note that the decryption of σ' is equal to the decryption of σ^*, since

$$\varphi^{-1}(\sigma'_1 e(d_{B2}^*, \sigma'_3) e(d_{B1}^*, \sigma'_2)^{-1}) = \varphi^{-1}(\sigma_1^* e(d_{B2}^*, \sigma_3^*) e(d_{B1}^*, \sigma_2^*)^{-1}) \to m_b \| R.$$

Also σ' is valid as

$$e(\sigma'_4, g) = e((d_{A1}^*)^{-1} \sigma_4^* d'_{A1}, g)$$

$$= e((d^{*}_{A1})^{-1} d^{*}_{A1} (m' \prod_{j \in M'} m_j)^{r} d'_{A1}, g)$$

$$= e(d'_{A1}, g) e((m' \prod_{j \in M'} m_j)^{r}, g)$$

$$= e(g_2^{\alpha} (u' \prod_{j \in U''_A} u_j)^{r'_A}, g) e((m' \prod_{j \in M'} m_j), g^{r})$$

$$= e(g_1, g_2) e((u' \prod_{j \in U''_A} u_j), \sigma'_5) e((m' \prod_{j \in M'} m_j), \sigma^{*}_2)$$

Here $M' = \{ j \in \mathbb{Z} : H(m_b)[j] \oplus R[j] = 1 \}$.

Note that Zhang's [27] scheme is also not insider secure. A similar kind of attack (defined above) can be launch on [27].

Insider attack on the strongly existentially unforgeability: A signature scheme is called strongly existentially unforgeable [7] if the adversary can't forge any signatures different from those generated by the challenger. It also include that given a signature on some message *m* it is hard to derive other signatures on the message. Zhang [27] gave the attack on the strong existential unforgeability on the Yu et al. scheme [25]. We give the similar kind of attack on strong existential unforgeabiliy on the Jin el al. [14] scheme. But our attack is based on insider security [8] i.e. adversary has the access to the private key of the receiver of the alleged forgery for the unforgeability game. Details of the attack are as follow:

During the EUF-CMA game, the adversary submits a message *m* with a sender identity u_A and a receiver identity u_B to the IBSC oracle. Note that adversary has access to the private key $d_B = (d_{B1}, d_{B2}) = (g_2^{\alpha} (u' \prod_{j \in U'_B} u_j)^{r_B}, g^{r_B})$ of the receiver u_B and does not ask any key generation query for the private key of u_A at any time. The challenger returns $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ as the signcrypted text of message m with sender u_A and receiver u_B. Here $\sigma_1 = e(g_1, g_2)^{r} \varphi(m \,||\, R)$, $\sigma_2 = g^{r}$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^{r}$, $\sigma_4 = d_{A1} (m' \prod_{j \in M'} m_j)^{r}$, $\sigma_5 = d_{A2}$ ($M' = \{ j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1 \}$).
Now adversary does the following to generate a forgery on the message *m*.

1. Computes $\varphi^{-1}(\sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}) \rightarrow m \,||\, R$
2. Selects $s \in_R \mathbb{Z}_p$ randomly
3. Generates the corresponding set $M' = \{ j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1 \}$
4. Computes $\sigma'_1 = \sigma_1 \cdot e(g_1, g_2)^{s}$, $\sigma'_2 = \sigma_2 \cdot g^{s}$, $\sigma'_3 = \sigma_3 \cdot (u' \prod_{j \in U'_B} u_j)^{s}$, $\sigma'_4 = \sigma_4 \cdot (m' \prod_{j \in M'} m_j)^{s}$
5. Sets $\sigma'_5 = \sigma_5$.

It is easy to cheek that $\sigma' = (\sigma'_1, \sigma'_2, \sigma'_3, \sigma'_4, \sigma'_5)$ is a valid signcrypted cipher text of *m*.

Insider attack on the existentially unforgeability: Next we will show an insider attacker can forge a valid signature on any message of her choice. Details are as follows:

During the EUF-CMA game, the adversary submits a message m with a sender identity u_A and a receiver identity u_B to the IBSC oracle. Note that adversary has access to the private key $d_B = (d_{B1}, d_{B2}) = (g_2^{\alpha}(u' \prod_{j \in U'_B} u_j)^{r_B}, g^{r_B})$ of the receiver u_B and does not ask any key generation query for the private key of u_A at any time. The challenger returns $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ as the signcrypted text of message m with sender u_A and receiver u_B. Here $\sigma_1 = e(g_1, g_2)^r \varphi(m \| R)$, $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$, $\sigma_5 = d_{A2}$ ($M' = \{ j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1\}$). Now adversary does the following to generate a forgery on the message m'.

1. Computes $\varphi^{-1}(\sigma_1 e(d_{B2}, \sigma_3) e(d_{B1}, \sigma_2)^{-1}) \to m \| R$
2. Sets $R' \in \{0,1\}^{n_m}$ such that $R'[j] = H(m')[j] \oplus H(m)[j] \oplus R[j]$
3. Computes $\sigma'_1 = \varphi(m \| R)^{-1} \cdot \sigma_1 \cdot \varphi(m' \| R')$, $\sigma'_2 = \sigma_2$, $\sigma'_3 = \sigma_3$, $\sigma'_4 = \sigma_4$
4. Sets $\sigma'_5 = \sigma_5$ and returns the cipher text $\sigma' = (\sigma'_1, \sigma'_2, \sigma'_3, \sigma'_4, \sigma'_5)$.

It is easy to check that σ' is valid forgery since the corresponding set M' generated by *m* and *R* is the same set generated by m' and R'.

$$\begin{aligned} M' &= \{ j \in \mathbb{Z} : H(m')[j] \oplus R'[j] = 1\} \\ &= \{ j \in \mathbb{Z} : H(m')[j] \oplus H(m')[j] \oplus H(m)[j] \oplus R[j] = 1\} \\ &= \{ j \in \mathbb{Z} : H(m)[j] \oplus R[j] = 1\}. \end{aligned}$$

6. Proposed Identity based signcryption (IBSC) scheme without random oracles:

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha \in \mathbb{Z}_p$, compute $g_1 = g^{\alpha}$ and pick $g_2 \in_R \mathbb{G}_1$. Furthermore, pick elements $u', m' \in_R \mathbb{G}_1$ and vectors $\vec{\boldsymbol{u}} = (u_i)$, $\vec{\boldsymbol{m}} = (m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Here public parameters are params = $\langle \mathbb{G}_1, \mathbb{G}_2, e, g, g_1, g_2, u', \vec{\boldsymbol{u}}, m', \vec{\boldsymbol{m}}, H_1, H_2 \rangle$ and the master secret key is g_2^{α}. Cryptographic hash functions H_1 and H_2 are defined as $H_1 : \mathbb{G}_2 \to \{0,1\}^{\ell}$ and $H_2 : \{0,1\}^{\ell} \times \mathbb{G}_2 \times \mathbb{G}_1 \to \{0,1\}^{n_m}$. Here ℓ is the length of the plaintext.

Key Generation: Similar to the previous scheme.

IBSC: To send a message $m \in \{0,1\}^{\ell}$ to Bob, Alice picks $r \in_R \mathbb{Z}_p$ randomly and computes $\omega = e(g_1, g_2)^r$, $\sigma_1 = m \oplus H_1(\omega)$, $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $M = H_2(m, \omega, u' \prod_{j \in U'_A} u_j)$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$ where $M' \subset \{1, ..., n_m\}$ is the set of indices *j* such that $m[j] = 1$ ($m[j]$ is the *j*-th bit of *M*). Next Alice sets $\sigma_5 = d_{A2}$. The cipher text is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

IBUSC: On receiving the cipher text $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$, Bob computes $\omega=e(d_{B2},\sigma_3)^{-1}e(d_{B1},\sigma_2)$, $m=\sigma_1\oplus H_1(\omega)$, $\hat{M}=H_2(m,\ \omega,\ u'\prod_{j\in U'_A}u_j)$. Bob generates the corresponding set $M'\subset\{1,...,n_m\}$ of indices *j* such that $m[j]=1$, where $m[j]$ is the *j*-th bit of $\hat{M}$. Accept the message if and only if

$$e(\sigma_4,g)=e(g_1,g_2)e(u'\prod_{j\in U'_A}u_j,\sigma_5)e(m'\prod_{j\in M'}m_j,\sigma_2).$$

Consistency:

$$\omega=e(d_{B2},\sigma_3)^{-1}e(d_{B1},\sigma_2)=e(g^{r_B},(u'\prod_{j\in U'_B}u_j)^r)^{-1}e(g_2^{\alpha}(u'\prod_{j\in U'_B}u_j)^{r_B},g^r)$$
$$=e(g^r,(u'\prod_{j\in U'_B}u_j)^{r_B})^{-1}e(g_2^{\alpha},g^r)e((u'\prod_{j\in U'_B}u_j)^{r_B},g^r)=e(g_1,g_2)^r$$

and

$$e(\sigma_4,g)=e(d_{A1}(m'\prod_{j\in M'}m_j)^r,g)$$
$$=e(d_{A1},g)e((m'\prod_{j\in M'}m_j)^r,g)$$
$$=e(g_2^{\alpha}(u'\prod_{j\in U'_A}u_j)^{r_A},g)e((m'\prod_{j\in M'}m_j),g^r)$$
$$=e(g_1,g_2)e((u'\prod_{j\in U'_A}u_j),\sigma_5)e((m'\prod_{j\in M'}m_j),\sigma_2)$$

7. Proposed Identity based public verifiable signcryption (IBPSC) scheme without random oracles:

Setup: Choose two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p such that an admissible pairing $e:\mathbb{G}_1\times\mathbb{G}_1\to\mathbb{G}_2$ can be constructed and pick a generator g of $\mathbb{G}_1$.

Now pick a random secret $\alpha\in_R\mathbb{Z}_p$, compute $g_1=g^{\alpha}$ and pick $g_2\in_R\mathbb{G}_1$. Furthermore, pick elements $u',m'\in_R\mathbb{G}_1$ and vectors $\vec{\boldsymbol{u}}=(u_i)$, $\vec{\boldsymbol{m}}=(m_i)$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. Here public parameters are params = $\langle\mathbb{G}_1,\mathbb{G}_2,e,g,g_1,g_2,u',\vec{\boldsymbol{u}}$, m', $\vec{\boldsymbol{m}},H_1,H_2,\varphi,\varphi^{-1}\rangle$ and the master secret key is g_2^{α}. Cryptographic hash functions H_1 and H_2 are defined as $H_1:\{0,1\}^{\ell}\times\mathbb{G}_2\times\mathbb{G}_1^4\to\{0,1\}^k$ and $H_2:\mathbb{G}_2\to\{0,1\}^{n_m}$. $\varphi:\mathcal{R}\to\mathbb{G}_2$ is a bijection while φ^{-1} is its inverse, $\mathcal{R}$ is a subset of $\{0,1\}^{\ell+k}$ with *p* elements. Here ℓ is the length of the plaintext and k is the sufficiently large integer.

Key Generation: Similar to the previous scheme. Also for the convenience we denote $U_A=u'\prod_{j\in U'_A}u_j$ and $U_B=u'\prod_{j\in U'_B}u_j$.

IBPSC: To send a message $m \in \{0,1\}^{\ell}$ to Bob, Alice randomly picks $r \in \mathbb{Z}_p$ and computes $\sigma_2 = g^r$, $\sigma_3 = (u' \prod_{j \in U'_B} u_j)^r$, $\omega = e(g_1, g_2)^r$, $R = H_1(m, \omega, \sigma_2, \sigma_3, U_A, U_B)$, $\sigma_1 = \omega \cdot \varphi(m \,||\, R)$, $M = H_2(\sigma_1)$, $\sigma_4 = d_{A1}(m' \prod_{j \in M'} m_j)^r$ where $M' \subset \{1,...,n_m\}$ denotes the set of indices j such that $m[j] = 1$ ($m[j]$ is the *j*-th bit of *M*). Next Alice sets $\sigma_5 = d_{A2}$. The cipher text is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

IBUSC: On receiving the cipher text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, Bob

1. computes $\hat{M} = H_2(\sigma_1)$
2. generates the corresponding set $M' \subset \{1,...,n_m\}$ of indices *j* such that $m[j] = 1$, where $m[j]$ is the *j*-th bit of $\hat{M}$
3. if $e(\sigma_4, g) \neq e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2)$, returns invalid. Otherwise
4. computes $\omega = e(d_{B2}, \sigma_3)^{-1} e(d_{B1}, \sigma_2)$
5. computes $\varphi^{-1}(\sigma_1 \cdot \omega^{-1}) \rightarrow m \,||\, R$
6. computes $R' = H_1(m, \omega, \sigma_2, \sigma_3, U_A, U_B)$
7. if $R' \neq R$ returns "invalid". Otherwise returns $\phi = (m, R', \omega, \sigma)$.

TP-Verify: On receiving $\phi = (m, R', \omega, \sigma)$, a sender identity u_A and a receiver identity u_B. Trusted third party

1. computes $\hat{M} = H_2(\sigma_1)$
2. generates the corresponding set $M' \subset \{1,...,n_m\}$ of indices *j* such that $m[j] = 1$, where $m[j]$ is the *j*-th bit of $\hat{M}$
3. if $e(\sigma_4, g) \neq e(g_1, g_2) e(u' \prod_{j \in U'_A} u_j, \sigma_5) e(m' \prod_{j \in M'} m_j, \sigma_2)$, returns invalid. Otherwise
4. computes $\varphi^{-1}(\sigma_1 \cdot \omega^{-1}) \rightarrow \hat{m} \,||\, \hat{R}$
5. accepts σ and output valid if $\hat{R} = H_1(\hat{m}, \omega, \sigma_2, \sigma_3, U_A, U_B)$ and $\hat{R} = R'$.

   It is easy to verify that the above scheme is consistent.

Conclusion: In this paper we showed that the improvements given by Zhang [27] and Jin el al. [14] on the Yu et al. [25] identity based signcryption scheme without random oracles are not secure. We gave the CPA attack on the confidentiality of Zhang [27] scheme and showed that the Jin et al. [14] scheme is not insider secure. Further we proposed a new identity based signcryption scheme without random oracles and an identity based public verifiable signcryption scheme with third party verification without random oracles.

References:

1. J. Baek, R. Steinfeld and Y. Zheng: Formal proofs of security of signcryption, PKC 02, LNCS # 2274, pp. 81-98, 2002.
2. F. Bao and R. H. Deng: A signcryption scheme with signature directly verifiable by public key. Proceeding of PKC'98 LNCS # 1431, Springer-Verlag pp. 55-59, 1998.
3. 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, Asicrypto'05, LNCS 3788, pp. 515-532, Springer-Verlag, 2005.
4. M. Bellare and P. Rogaway: Random oracles are practical: a paradigm for designing efficient protocols. D. Denning et al. (Eds.), Proceedings of the First ACM Conference on Computer and Communications Security ACM Press, pp. 62-73, 1993.
5. D. Boneh and X. Boyen: Efficient selective-ID secure identity based encryption without random oracles. In Eurocrypt'04, LNCS # 3027, pp. 223-238, Springer, 2004.
6. D. Boneh and M. Franklin: Identity–based encryption scheme from Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 2001, 213-229.
7. D. Boneh, E. Shen and B. Waters: Strongly unforgeable signatures based on computational Diffie-Hellman problem. PKC'2005, LNCS # 3958, pp. 229-240.
8. X. Boyen: Multipurpose Identity based signcryption: A Swiss army knife for identity based cryptography. CRYPTO 2003, LNCS # 2729, pp. 389-399, Springer-Verlag, 2003.
9. R. Canetti, S. Halevi, J. Katz: A forward secure public key encryption scheme. Advances in Cryptology. EUROCRYPT 2003, LNCS # 2656, pp. 225-271, Springer-Verlag, Berlin 2003.
10. R. Canetti, O. Goldreich and S. Halevi: The random oracle methodology revisited. Journal of the ACM 51 (4) pp. 557-594, 2004.
11. L. Chen and J. Malone-Lee: Improved identity-based signcryption. PKC 2005, LNCS # 3386, pp. 362-379, Springer-Verlag, 2005.
12. 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 cipher text authenticity. ICISC'2003, LNCS # 2971, pp. 352-369, Springer-Verlag, 2003.
13. R. Hwang, C. Lai and F. Su: An efficient signcryption scheme with forward secrecy based on elliptic curve. Applied Mathematics and Comutation 165 pp. 870-881, 2005.
14. Z. Jin, Q. Wen and H. Du: An improved semantically secure identity based signcryption scheme in the standard model. Comput Electr Eng, 2010.
15. H. Y. Jung, K. S. Chang, D. H. Lee, and J. I. Lim, Signcryption schemes with forward secrecy, Proceeding of WISA 2 pp. 403-233, 2001.
16. B. Libert and J. J. Quisquater: New identity based signcryption schemes from pairings, IEEE Information Theory Workshop, Paris, France, *http://eprint.iacr.org/2003/023*, 2003.
17. J. Malone-Lee: Identity-based signcryption, Cryptology ePrint Archive Report 2002/098.
18. N. McCullagh and P.S.L.M. Baarreto: Efficient and forward secure identity based signcryption. Cryptology ePrint Archive Report 2004/117.
19. K. G. Paterson and J. C. Schuldt: Efficient identity based signatures secure in the standard model. Proceedings of the 11th Australasian Conference Information Security and Privacy, LNCS # 4058, pp. 207-222, Springer-Verlag, 2006.
20. S. S. D. Selvi, S. S. Vivek, C. P. Rangan: Identity based public verifiable signcryption scheme. Proc. ProvSec 2010, LNCS # 6402, pp. 244-260, Springer-Verlag, 2010.
21. A. Shamir: Identity-based cryptosystems and signature schemes. CRYPTO 84, LNCS # 196, pp 47-53 Springer-Verlag, 1984.
22. X. Wang and H. Qian: Attacks against two identity based signcryption schemes. 2nd International Conference NSWCTC'2010, Wuhan, Hubei, Vol. 1 pp. 24-27, 2010.
23. B. Waters: Efficient identity based encryption without random oracles. Advances in Cryptology. EUROCRYPT 2005, LNCS # 3494, pp. 114-127, Springer-Verlag, Berlin 2005.
24. Q. Xia and C. Xu: Cryptanalysis of identity based signcryption schemes. 8th IEEE International Conference, DASC'09, pp. 292-294, 2009.

25. Y. Yu, B. Yang, Y. Sun and S. L. Zhu: Identity based signcryption scheme without random oracles. Computer Standard and Interfaces, 31 (1) pp. 56-62, 2009.
26. T. H. Yuen and V. K. Wei: Constant size hierarchical identity based signature/signcryption without random oracles. Cryptology ePrint Archive, *http:eprint.iacr.org/2005/412.pdf,* 2005.
27. B. Zhang: Cryptanalysis of an identity based signcryption scheme without random oracles. Journal of Computational Information Systems 6:6 (2010) pp. 1923-1931, 2010.
28. M. Zhang, P. Li, B. Yang H. Wang and T. Takagi: Towards confidentiality of ID-based signcryption scheme under without random oracle model. PAISI’2010, LNCS # 6122, pp. 98-104, Springer-Verlag, 2010.
29. B. Zhang and Q. Xu: An ID-based anonymous signcryption scheme for multiple receivers. International Journal of Advanced Science and Technology, Vol. 20, pp. 9-24, 2010.
30. B. Zhang and Q. Xu: Identity based multi-sigcryption scheme without random oracles. Chinese Journal of Computers, Issue No. 1, pp. 103-110, 2010.
31. Y. Zheng: Digital signcryption or how to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption), CRYPTO'97, LNCS # 1294, pp. 165-179, Springer-Verlag, 1997.
32. Y. Zheng and H. Imai: How to construct efficient signcryption schemes on elliptic curves. Information Proceeding Letters, Vol. 68 No. 5, pp. 227-233, 1998.