Efficient Generalized Signcryption Schemes

Prashant Kushwah[1] and Sunder Lal[2]

[1]Department of Mathematics and Statistics, Banasthali University, Rajasthan, India.
[2]Department of Mathematics, Dr. B. R. A. (Agra) University, UP, India.
Email:- [1]pra.ibs@gmail.com, [2]sunder_lal2@rediffmail.com

Abstract: Generalized signcryption is a new cryptographic primitive which works as a signcryption scheme, a signature scheme and an encryption scheme as per need. Recently Ji et al. proposed a security model for certificateless generalized signcryption scheme and also proposed a scheme which they claim is secure under the proposed security model. In this paper we show that Ji et al. scheme is not existentially unforgeable against Type-I adversary and propose a simplified certificateless generalized signcryption. We also present an efficient identity based generalized signcryption scheme.

Keywords: signcryption, generalized signcryption, identity based cryptography, certificateless cryptography.

1. Introduction: Confidentiality and authenticity are two logically independent primitives of cryptography. To achieve confidentiality, an encryption scheme is used and authenticity is achieved through a signature scheme. There are scenarios where both the primitives are required. In this situation we use signcryption a primitive proposed by Zheng [13] in 1997. Signcryption performs encryption and signature both in a single logical step. However, in the low bandwidth environment we cannot afford to use three different schemes to achieve confidentiality or authenticity or both. In [6] Han et al. proposed the concept of generalized signcryption which can work as an encryption scheme, a signature scheme and a signcryption scheme as per need. Wang et al. [11] gave the first security model for a generalized signcryption scheme and modified the scheme proposed in [6].

Identity based cryptography was introduced by Shamir [10] in 1984. In the identity based cryptosystem public key of users are their identities and secret keys of user are created by a trusted third party called private key generator (PKG). First identity based signature scheme was given by Shamir [10] in 1984, but the first identity based encryption scheme was given by Boneh and Franklin [4] in 2001. The first identity based signcryption scheme was proposed by Malone Lee [9] in 2002. They also gave the security model for signcryption in identity based setting. Since then, many identity based signcryption schemes have been proposed in literature. The first identity based generalized signcryption along with a security model was proposed by Lal and Kushwah [8] in 2008. However, Yu et al. [12] show that security model for identity based generalized signcryption proposed in [8] is not complete. They modified the security model and proposed a concrete scheme which is secure in this model.

In 2003, Al-Riyami and Paterson [1] proposed a new cryptographic primitive, certificateless public key cryptosystem, which avoid the key escrow problem and the need of certificate in public key cryptography. Barbosa and Frashim [2] in 2008 proposed a signcryption scheme in the certificateless setting. Recently, Ji et al. [7] modeled a security notion of generalized signcryption in certificateless setting and proposed a concrete scheme. However they have not given any security proof of their scheme.

In this paper we first show that Ji et al. [7] scheme is not existentially unforgeable against Type-I adversary. Further we propose a simplified certificateless generalized Signcryption and also an efficient identity based generalized signcryption scheme.

This paper is organized as follows: In section 2, we define identity based generalized Signcryption scheme. In section 3, we proposed a simplified security model for identity based generalized signcryption (IBGSC). In section 4, we proposed an IBGSC scheme which can be shown secure under the new security model. We also discuss the efficiency of this scheme. In section 5, we show that Ji et al. scheme is not existentially unforgeable against Type-I adversary [2]. Finally, in section 7, we give a simplified certificateless generalized signcryption.

2. Identity Based Generalized Signcryption (IBGSC):

Preliminaries:

Bilinear Pairing: Let G_1 be an additive group and G_2be a multiplicative group both of the same prime order q. A function $e: G_1 \times G_1 \rightarrow G_2$ is called a bilinear pairing if it satisfies the following properties:

1. $\forall\, P, Q \in G_1, \forall\, a, b \in Z_q^*, e(aP, bQ) = e(P, Q)^{ab}$
2. For any $O \neq P \in G_1$, there is $Q \in G_1$, such that $e(P, Q) \neq 1$.
3. There exists an efficient algorithm to compute $e(P, Q), \forall\, P, Q \in G_1$.

q-Diffie Hellman inversion problem(q-DHIP): Given a $(q+1)$ tupple $(P, \alpha P, \alpha^2 P, \ldots, \alpha^q P)$ comput $\frac{1}{\alpha} P$.

q-Bilinear Diffie Hellman inversion problem: Given a $(q+1)$ tupple $(P, \alpha P, \alpha^2 P, \ldots, \alpha^q P)$ compute $e(P, P)^{1/\alpha} \in G_2$.

An identity based generalized signcryption (IBGSC) consist the following algorithms:

1. **Setup:** This algorithm takes input a security parameter k and outputs the system parameter **params** and a master secret key.
2. **Private 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. **IBGSC:** If user A wants to send a message m to B. This algorithm takes input $(D_A, m, ID_A$, $ID_B)$ and outputs a $\sigma = IBGSC\ (D_A, m, ID_A, ID_B)$.
4. **UIBGSC:** This is unsigncryption algorithm. It takes input $(\sigma, ID_B, S_B, PK_B, ID_A, PK_A, PK_A)$ and outputs m if σ is valid otherwise $\perp$ if σ is not valid.

There is no specific sender (or receiver) when we only encrypt (or sign) a message m using IBGSC. We denote the absence of sender (or receiver) by $ID_\emptyset$. Thus to only sign or encrypt a message m, use $ID_B = ID_\emptyset$ or $ID_A = ID_\emptyset$.

A security model for IBGSC was given in [8]. This model is recently been modified by Yu et al. [12]. In the next section we provide a new and simplified security model for IBGSC.

3. Security model for IBGSC:

The modified security notion for identity based generalized signcryption by Yu et al. [12] provide 7 oracles to the adversary namely Extraxt, Sign, Verify, Encrypt, Decrypt, GSC and GUC. But the basic nature of generalized signcryption is to use a single algorithm to sign, to encrypt or to signcrypt a message as per need, which can be achieved by giving specific input to generalized signcryption algorithm. Similarly a single algorithm is used to decrypt and verify a message. Therefore the oracles Encrypt, Decrypt, Sign and verify seem redundant. In our simplified security model we provide only IBGSC and UIBGSC oracles to the adversary which he can query with specific inputs. Also Yu et al. gave the security proof of their scheme for confidentiality and unforgeability in different modes viz. encryption only mode, signature only mode and signcryption mode. In our security model, we use a single game for confidentiality in encryption only mode and signcryption mode. Similarly we use a single game for unforgeability in signature only mode and signcryption mode. To do so, in the challenge stage of the game for confidentiality we only impose restriction on receiver's identity i.e. $ID_B^* \neq ID_\emptyset$, also for the unforgeability we only impose restriction on sender's identity i.e. $ID_A \neq ID_\emptyset$.

Message Confidentiality:

The notion of security with respect to confidentiality is indistinguishability of encryptions under adaptive chosen ciphertext attack (IND-CCA2). For IBGSC 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.

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.
- **Private Key Extraction Queries:** $\mathcal{A}$ submits an identity ID_U and $\mathcal{C}$ computes the private key D_U corresponding to ID_U and returns to $\mathcal{A}$.
- **IBGSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B and a message m. Challenger $\mathcal{C}$ runs IBGSC with message m and identities ID_A and ID_B and returns the output σ to the adversary $\mathcal{A}$.
- **UIBGSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B along with σ to the challenger $\mathcal{C}$. $\mathcal{C}$ runs the UIBGSC algorithm with input σ, ID_A and ID_B and returns the output m of UCLGSC.

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 he wishes to be challenged. The adversary $\mathcal{A}$ must have made no private key extraction query on ID_B^*, also $ID_B^* \neq ID_\emptyset$ for the confidentiality game. $\mathcal{C}$ picks randomly a bit $b \in \{0, 1\}$, runs the IBGSC algorithm to with message m_b under ID_A^* and ID_B^* and returns the output σ^* to the adversary $\mathcal{A}$.

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 it is not allow to make an UIBGSC query on σ^* 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 IBGSC scheme is said to IND-CCA2 secure if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

Signature unforgeability:

The notion of security with respect to authenticity is existential unforgeability against chosen message attacks (EUF-CMA). For IBGSC 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, σ) that was not obtained from IBGSC query during the game and for which private key of ID_A was not exposed, also $ID_A \neq ID_{\emptyset}$ for signature unforgeability game. The forger wins the game if the result of $UIBGSC\ (\sigma, ID_B, S_B, ID_A)$ is not the $\perp$ symbol.

The adversary $\mathcal{A}$'s advantage is its probability of victory.

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

4. Proposed IBSC Scheme:

In this section we will propose an efficient identity based generalized signcryption scheme based on identity based signcryption scheme proposed in [3].

Setup: Given a security parameter 1^k, the PKG chooses two groups G_1 and G_2 of prime order p, a random generator P of G_1, and a bilinear map $e: G_1 \times G_1 \rightarrow G_2$. Compute $g = e(P, P)$, define hash functions as $H_1: \{0,1\}^{k_3} \rightarrow \mathbb{Z}_p^*$, $H_2: \{0,1\}^{n+k_2+2k_3} \rightarrow \mathbb{Z}_p^*$, $H_3: \{0,1\}^{n+k_2+k_1+2k_3} \rightarrow \mathbb{Z}_p^*$, $H_4: \{0,1\}^{k_2} \rightarrow \{0,1\}^{n+k_1+k_2+k_3}$, where k_1, k_2 and k_3 denote the number of bits to represent elements of G_1, G_2 and identity respectively and n is the message bit length. PKG chooses random $s \in \mathbb{Z}_p^*$ as the master secret key and sets $P_{pub} = sP$. PKG publishes the system parameters as $\langle G_1, G_2, p, n, P, P_{pub}, e: G_1 \times G_1 \rightarrow G_2, g, H_1, H_2, H_3, H_4 \rangle$.

Let a function f be such that $f(ID) = 0$ if $ID = ID_{\emptyset}$ otherwise $f(ID) = 1$.

Extract Private Key: Given a user U with identity ID_u, the private key is computed by PKG as $D_u = (q_u + s)^{-1}P$, where $q_u = H_1(ID_u)$. For $ID_{\emptyset}$, we set $D_{\emptyset} = \mathcal{O}$.

IBGSC: The sender A for the receiver B

1. Chooses $r \in_R \mathbb{Z}_p^*$;
2. Computes
   i. $\alpha = g^r$
   ii. $r' = H_2(m, \alpha, ID_A, ID_B)$

iii. $X = r'T_B$ where $T_B = H_1(ID_B)P + P_{pub}$
iv. $h_3 = H_3(m, \alpha, X, ID_A, ID_B)$
v. $Z = (r + h_3)D_A$
vi. $y = m \parallel \alpha \parallel Z \parallel ID_A \oplus \{H_4(g^{r'})f(ID_B)\}$, and

3. Returns $\sigma = (y, X)$

UIBGSC: On receiving σ from A, the user B

1. Recovers $m \parallel \alpha \parallel Z \parallel ID_A = y$ if $X = \mathcal{O}$, otherwise
2. Computes $\omega = e(X, D_B)$ and recovers $m \parallel \alpha \parallel Z \parallel ID_A = y \oplus \{H_4(\omega)f(ID_B)\}$
3. If $Z = \mathcal{O}$, Computes $r' = H_2(m, \alpha, ID_A, ID_B)$ and accept the message iff $X = r'T_B$, otherwise
4. Computes $h_3 = H_3(m, \alpha, X, ID_A, ID_B)$ and accept the message iff $e\big(Z,\ H_1(ID_A)P + P_{pub}\big)g^{-h_3} = \alpha.$

Consistency:

$$\omega = e(X, D_B) = e(r'T_B, D_B) = e(r'(q_B + s)P, (q_B + s)^{-1}P) = e(P, P)^{r'} = g^{r'}$$

$$e\big(Z, H_1(ID_A)P + P_{pub}\big)g^{-h_3} = e\big((r + h_3)D_A, (q_A + s)P\big)g^{-h_3}$$

$$= e\big((r + h_3)(q_A + s)^{-1}P, (q_A + s)P\big)g^{-h_3} = e(P, P)^{(r+h_3)}g^{-h_3} = g^{r+h_3}g^{-h_3} = g^r = \alpha$$

Remarks:

1. When we only sign a message then specific receiver B does not exist therefore we use $ID_B = ID_\emptyset$ in IBGSC algorithm. Thus the function $f(ID_\emptyset)$ became 0 which helps to give us the signature $y = m \parallel \alpha \parallel Z \parallel ID_A$, also the component X of the output of IBGSC algorithm became $\mathcal{O}$. This will reduce the extra computation in UIBGSC.
2. When we only encrypt a message then specific sender A does not exist, therefore we use $ID_A = ID_\emptyset$ in IBGSC algorithm. Thus in the computation of Z we have $D_\emptyset = \mathcal{O}$ which will again reduce the extra computation in UIBGSC by checking $X = r'T_B$, which will also provide chosen ciphertext security while we only encrypt a message.
3. The form of ciphertext is (y, X) either we encrypt a message or signcrypt a message. This prevents an adversary to embed a encryption to valid signcryption or vice versa. Similarly an adversary cannot embed a signature of a message to valid signcryption or vice versa because when we only sign a message then $X = \mathcal{O}$ as well as the computations of r' and h_3 involve both sender's and receiver's identity.

Efficiency and Comparison:

The basic idea behind generalized signcryption is to reduce the implementation complexity using a single IBGSC scheme as an encryption scheme, a signature scheme and a signcryption scheme as per need. This renders some extra calculation while we use generalized signcryption for encryption and signature. However, the proposed IBGSC scheme significantly reduces the extra calculation in encryption and signature. Also, the proposed IBGSC scheme is as efficient as identity based signcryption scheme in [3] which is the most efficient identity based signcryption scheme till date. In the following table we compare the dominant operations required for IBGSC and other schemes.

Scheme	Sign/Encrypt			Decrypt/Verify		
	mul in G1	exps in G2	e cps	mul in G1	exps in G2	e cps
Barreto et al. [3]	2	1	0	0	1	2
Lal et al. [8]	5	0	1	1	0	4
Yu et al. [12]	3	1	1	0	2	4
Proposed IBGSC	2	2	0	1 or 0	1 or 0	2 or 1

Table 1

5. Certificateless Generalized Signcryption (CLGSC):

A certificateless generalized signcryption (CLGSC) consists of the following algorithms:

1. **Setup:** This algorithm takes input a security parameter k and outputs the system parameter **params** and a master secret key.
2. **Partial Private 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. **Set User Key:** Given input ID_U, partial private key D_U corresponding to ID_U, it outputs a public key PK_U of the identity ID_U and a secret value x_U, the secret key (SK_U) of the user is (x_U, D_U).
4. **CLGSC:** To send a message m form A to B, This algorithm takes input $(SK_A, m, ID_A, PK_A, ID_B, PK_B)$ and outputs $\sigma = CLGSC\ (SK_A, m, ID_A, PK_A, ID_B\ PK_B)$.
5. **UCLGSC:** This algorithm takes input $(\sigma, ID_B, S_B, PK_B, ID_A, PK_A,\ PK_A)$ and outputs m if σ is valid signcryption m form A to B of otherwise $\perp$.

There is no specific sender (receiver) when we only encrypt (only sign) a message m using CLGSC. We denote the absence of sender (or receiver) by $ID_\emptyset$. Thus to only sign or to only encrypt a message m, use $ID_B = ID_\emptyset$ or $ID_A = ID_\emptyset$ respectively.

Security model for CLGSC:

There are two different types of adversaries in certificateless cryptosystem. A Type-I adversary $\mathcal{A}_I$ which is not allowed access to the master key but $\mathcal{A}_I$ may request public keys and replace them with values of his choice. The Type-II adversary $\mathcal{A}_{II}$ is allowed access to the master key but cannot replace a public key.

Message Confidentiality:

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

GAME 3 (IND-CCA2):

Initialization: $\mathcal{C}$ runs the setup algorithm on input a security parameter k, and gives public parameters params to the adversary $\mathcal{A}$. $\mathcal{C}$ keeps the master key secret if $\mathcal{A}$ is Type-I adversary else it provides the master secret also to $\mathcal{A}$.

Find Stage: The adversary $\mathcal{A}$ asks the following queries adaptively.

- **Hash Queries:** $\mathcal{A}$ can request the hash values of any input and challenger responds with appropriate hash values.
- **Partial Private Key Extraction:** $\mathcal{A}$ submits an identity ID_U, and $\mathcal{C}$ computes the partial private key D_U and returns to $\mathcal{A}$. Note that an adversary $\mathcal{A} = \mathcal{A}_{II}$ does not need this oracle because it has the master secret key and can compute partial private key for any user.
- **Public Key Extraction:** $\mathcal{A}$ submits an identity ID_U for which he wants the public key, $\mathcal{C}$ computes the corresponding public key PK_U and sends it to $\mathcal{A}$.
- **Private Key Extraction:** $\mathcal{A}$ submits the identity ID_U, $\mathcal{C}$ computes the corresponding private key PK_U and sends it to $\mathcal{A}$. Note that if $\mathcal{A}$ is Type-I adversary then $\mathcal{A}$ is not allowed to extract the full private key of any identity for which corresponding public key has been replaced. Because in this case challenger is not able to provide the full private key of that user.
- **Public Key Replacement:** If $\mathcal{A}$ is Type-I adversary then $\mathcal{A}$ has access to this oracle. For any identity ID_U, $\mathcal{A}$ computes the new public key PK_U' by choosing a new secret value x_U' of his choice and replaces PK_U. Note that if $\mathcal{A}$ is Type-II adversary then $\mathcal{A}$ cannot replace public key of any user.
- **CLGSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B and a message m. Challenger $\mathcal{C}$ runs CLGSC with message m and identities ID_A and ID_B and returns the output σ to the adversary $\mathcal{A}$.
- **UCLGSC Queries:** $\mathcal{A}$ submits two identities ID_A, ID_B along with σ to the challenger $\mathcal{C}$. $\mathcal{C}$ runs the UCLGSC algorithm with input σ, ID_A and ID_B and returns the output of UCLGSC.

Note that it is possible that the public key PK_A (or PK_B) corresponding to ID_A (or ID_B) has been replaced earlier by $\mathcal{A}$ (if $\mathcal{A}$ is Type-I adversary) in CLGSC (or UCLGSC) queries. If so, $\mathcal{A}$ has to submit the corresponding secret value to $\mathcal{C}$ for the correctness of these oracles. Also we disallow queries to these oracle when $ID_A = ID_B$.

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 he wishes to be challenged. The adversary $\mathcal{A}$ must have made no private key extraction query (and partial private key extraction query if $\mathcal{A}$ is Type-I adversary) on ID_B^*, also $ID_B^* \neq ID_\emptyset$ for the confidentiality game. $\mathcal{C}$ picks randomly a bit $b \in \{0, 1\}$, runs the CLGSC algorithm with message m_b under ID_A^* and ID_B^* and returns the output σ^* to the adversary $\mathcal{A}$.

Guess stage: $\mathcal{A}$ asks queries adaptively again as in the find stage. It is not allowed to extract the private key (and partial private key if $\mathcal{A}$ is Type-I adversary) corresponding to ID_B^* and it is not allow to make an UCLGSC query on σ^* with sender ID_A^* and receiver ID_B^* unless the public key PK_A^* of the sender or that of the receiver PK_B^* has been replaced after the challenge if $\mathcal{A}$ is Type-I adversary.

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 3: A CLGSC scheme is said to IND-CCA2 secure if no polynomially bounded adversary $\mathcal{A}$ (Type-I or Type-II) has non-negligible advantage of winning the above game.

Signature unforgeability:

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

GAME 4 (EUF-CMA):

Initialization: Same as in GAME 3.

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, σ) that was not the obtained from CLGSC query during the game and for which private key (and partial private key if $\mathcal{A}$ is Type-I adversary) of ID_A was not exposed, also $ID_A \neq ID_\emptyset$ for signature unforgeability game. The adversary $\mathcal{A}$ wins the game if the result of $UCLGSC\ (\sigma, ID_B, S_B, PK_B, ID_A, PK_A)$ is not the $\perp$ symbol.

The adversary $\mathcal{A}$'s advantage is its probability of victory.

Definition 4: A CLGSC scheme is said to EUF-CMA secure if no polynomially bounded adversary $\mathcal{A}$ (Type-I or Type-II) has non-negligible advantage of winning the above game.

6. Review of Ji et al [7] Certificateless Generalized Signcryption:

Setup: given a security parameter 1^k, the PKG chooses two groups G_1 and G_2 of prime order p, two random generator P, Q of G_1 such that $P \neq Q$, and a bilinear map $e: G_1 \times G_1 \rightarrow G_2$. Compute $g = e(P, Q)$, define hash functions as $H_1: \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$, $H_2: G_2 \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_3: \{0,1\}^n \times G_2 \times \{0,1\}^* \times G_2 \times G_1 \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_4: \mathbb{Z}_p^* \times \{0,1\}^* \rightarrow \mathbb{Z}_p^*$, $H_5: G_2 \times G_2 \times G_2 \times \{0,1\}^* \rightarrow \{0,1\}^{k_1+k_2}$, where k_1, k_2 denotes the number of bits to represent G_1 and $\mathbb{Z}_p^*$ elements respectively. PKG chooses random $s \in \mathbb{Z}_p^*$ as the master secret key and set $P_{pub} = sP$. PKG publishes the system parameters as $\langle G_1, G_2, P, Q, P_{pub}, e: G_1 \times G_1 \rightarrow G_2, g, H_1, H_2, H_3, H_4, H_5 \rangle$.

Extract Partial Private Key: given ID_i, the partial private key of the user with identity ID_i is computed by PKG as $D_i = (q_i + s)^{-1}Q$, where $q_i = H_1(ID_i)$.

Set User Key: given D_i, the user with identity ID_i chooses random $x_i \in \mathbb{Z}_p^*$ and set his private key $SK_i = \langle x_i,\ D_i \rangle$ and public key $PK_i = \langle PK_{i1}, PK_{i2} \rangle = \langle g^{x_i},\ x_i T_i \rangle$, where $T_i = (q_i + s)P$.

CLGSC: This algorithm has three scenarios: signcryption, signature and encryption.

Signcryption: given message m, sender's identity A, receiver's identity B, A operates the following steps:

1. A chooses randomly $r, r' \in \mathbb{Z}_p^*$, computes $\alpha = g^r$;
2. Computes $h = H_2(\alpha, m, ID_A, ID_B)$ and $h_3 = H_3(m, \alpha, h, ID_A,\ PK_{A\,1},\ PK_{A\,2}, ID_B)$;
3. Computes $Z = \frac{r}{(x_A + h_3)} D_A$;
4. Computes $c = H_4(h,\ ID_A,\ ID_B) \oplus m \parallel \alpha$;
5. Computes $h_5 = H_5(g^{r'},\ (PK_{B\,1})^{r'},\ PK_{B\,1},\ ID_B)$;
6. Computes $d_1 = r'(q_B + s)P$ and $d_2 = h_5 \oplus h \parallel Z$;
7. Return ciphertext $\sigma = (c,\ d_1,\ d_2,\ ID_B)$.

Signature: given message m, sender's identity A, A operates the following steps:

1. A chooses randomly $r, r' \in \mathbb{Z}_p^*$, computes $\alpha = g^r$;
2. Computes $h = H_2(\alpha, m, ID_A, 0)$ and $h_3 = H_3(m, \alpha, h, ID_A,\ PK_{A\,1},\ PK_{A\,2}, 0)$;
3. Computes $Z = \frac{r}{(x_A + h_3)} D_A$;
4. Computes $c = m \parallel \alpha$;
5. Computes $h_5 = 0$;
6. Computes $d_1 = 0$ and $d_2 = h_5 \oplus h \parallel Z = h \parallel Z$;
7. Return ciphertext $\sigma = (c,\ d_1,\ d_2,\ 0)$.

Encryption: given message m, receiver's identity B, someone operates the following steps:

1. Chooses randomly $r, r' \in \mathbb{Z}_p^*$, computes $\alpha = g^r$;
2. Computes $h = H_2(\alpha, m, 0, ID_B)$ and $h_3 = H_3(m, \alpha, h, 0, 0, 0, ID_B)$;
3. Computes $c = H_4(h, 0,\ ID_B) \oplus m \parallel \alpha$;
4. Computes $h_5 = H_5(g^{r'},\ (PK_{B\,1})^{r'},\ PK_{B\,1},\ ID_B)$;
5. Computes $d_1 = r'(q_B + s)P$ and $d_2 = h_5 \oplus h \parallel 0$;
6. Return ciphertext $\sigma = (c,\ d_1,\ d_2,\ ID_B)$.

UCLGSC: given σ, a receiver's identity B, operates the following steps:

1. Computes $w' = e(d_1, D_B)$ and $(w')^{x_B}$ (if there is no receiver's identity, then $D_B = 0$, and $w' = 1$);
2. Sets $h_5' = H_5(w',\ (w')^{x_B},\ PK_{B\,1},\ ID_B)$; (if $D_B = 0$, then $h_5' = 0$);
3. Computes $h' \parallel Z' = d_2 \oplus h_5'$;
4. If $ID_B \neq 0$, computes $m' \parallel \alpha' = c \oplus H_4(h',\ ID_A,\ ID_B)$; (if $Z' = 0$, then $ID_A = 0$);
5. If $ID_B \neq 0$, computes $h_3 = H_3(m', \alpha', h', ID_A,\ PK_{A\,1},\ PK_{A\,2}, ID_B)$; (if $Z' = 0$, then $ID_A = 0$ and $PK_{A\,1} =\ PK_{A\,2} = 0$);
6. If $Z' \neq 0$, then B accepts m' if and only if $h' = H_2(\alpha', m', ID_A, ID_B)$ and $e(Z',\ PK_{A\,2} + h_3'(q_A + s)P) = \alpha'$ holds. Otherwise accept m' if and only if $h' = H_2(\alpha', m', 0, ID_B)$.

Attack on unforgeability of Ji et al [7] scheme by a Type-I adversary:

Now, we model the attack on unforgeability of Ji et al. scheme in signcryption mode by an insider Type-I adversary. Note that Type-I adversary $\mathcal{A}$ has the power to replace public keys of any user with his choice. To forge a signcrypted text, $\mathcal{A}$ does the following:

1. $\mathcal{A}$ replaces the public key $PK_A =< PK_{A\,1}, PK_{A\,2} > = < g^{x_A},\ x_A T_A >$ of A by $PK_A' =< PK'_{A\,1}, PK'_{A\,2} > = < g^{x_A'},\ x'_A T_A >$ by choosing x_A' randomly from $\mathbb{Z}_p^*$.
2. $\mathcal{A}$ submits a message m, sender's identity A, receiver's identity B to signcryption oracle. Note that $\mathcal{A}$ provides the secret value x_A' to the challenger $\mathcal{C}$ when public key of sender A is replaced.
3. $\mathcal{C}$ returns the ciphertext $\sigma = (c,\ d_1,\ d_2,\ ID_B)$
4. $\mathcal{A}$ extract Z and α from σ.

Now $\mathcal{A}$ can use $Z = \frac{r}{(x_A' + h_3)} D_A$ and $\alpha = g^r$ to signcrypt any message m' intended to any receiver B'. For this $\mathcal{A}$

1. Chooses randomly $r' \in \mathbb{Z}_p^*$.
2. Computes $h' = H_2(\alpha, m', ID_A, ID_{B'})$ and $h'_3 = H_3(m', \alpha, h', ID_A,\ PK'_{A\,1},\ PK'_{A\,2}, ID_{B'})$;
3. Computes $c' = H_4(h',\ ID_A, ID_{B'}) \oplus m' \parallel \alpha$;
4. Computes $h'_5 = H_5(g^{r'},\ (PK_{B'\,1})^{r'},\ PK_{B'\,1},\ ID_{B'})$;
5. Set $Z' = \left(\frac{x'_A + h_3}{x'_A + h'_3}\right) Z$;
6. Computes $d'_1 = r'(q_B + s)P$ and $d'_2 = h'_5 \oplus h' \parallel Z'$;
7. Return the ciphertext $\sigma' = (c',\ d'_1,\ d'_2,\ ID_{B'})$.

Now we show that σ' is valid forgery. For this B' does the following:

1. Computes $w = e(d'_1, D_{B'}) = e(r'(q_{B'} + s)P, (q_{B'} + s)^{-1}Q) = e(P,\ Q)^{r'} = g^{r'}$ and $(w)^{x_{B'}} = (g^{r'})^{x_{B'}} = (g^{x_{B'}})^{r'} = (PK_{B'\,1})^{r'}$;
2. Sets $h'_5 = H_5(w,\ (w)^{x_{B'}},\ PK_{B'\,1},\ ID_{B'})$;
3. Recover $h' \parallel Z' = d'_2 \oplus h'_5$;
4. Recover $m' \parallel \alpha = c' \oplus H_4(h',\ ID_A,\ ID_{B'})$;
5. Computes $h'_3 = H_3(m', \alpha, h', ID_A,\ PK_{A\,1},\ PK_{A\,2}, ID_{B'})$;
6. B' will accepts the message m' because $h' = H_2(\alpha, m', ID_A, ID_{B'})$ and $e(Z',\ PK_{A\,2} + h'_3(q_A + s)P) = \alpha$ holds.

Verification:

$$e(Z',\ PK_{A\,2} + h'_3(q_A + s)P) = e\left(\left(\frac{x'_A\ + h_3}{x'_A\ +\ h'_3}\right) Z, x'_A(q_A + s)P + h'_3(q_A + s)P\right)$$

$$= e\left(\left(\frac{x'_A\ + h_3}{x'_A\ +\ h'_3}\right)\frac{r}{x'_A\ + h_3}(q_A + s)^{-1}Q, (x'_A + h'_3)(q_A + s)P\right)$$

$$= e(P, Q)^r = g^r = \alpha.$$

Thus we have shown that a Type-I adversary can forge the signcryptext on any message for any receiver. The reason of such type of attack is that Ji et al. use the different randomness for encryption and signature. A similar type of attack can be modeled in the signature mode.

7. Proposed CLGSC Scheme:

In this section we will propose a simplified certificateless generalized signcryption scheme based on the certificateless encryption scheme proposed in [5].

Setup: Given a security parameter 1^k, the PKG chooses two groups G_1 and G_2 of prime order p, a random generator P of G_1, and a bilinear map $e: G_1 \times G_1 \rightarrow G_2$. Compute $g = e(P, P)$, define hash functions as $H_1: \{0, 1\}^{k_3} \rightarrow \mathbb{Z}_p^*$, $H_2: \{0,1\}^{n+k_2+2k_3} \rightarrow \mathbb{Z}_p^*$, $H_3: \{0,1\}^{n+k_2+3k_1+2k_3} \rightarrow \mathbb{Z}_p^*$, $H_4: \{0,1\}^{k_2+k_1} \rightarrow \{0,1\}^{n+k_1+k_2+k_3}$, where k_1, k_2 and k_3 denote the number of bits to represent elements of G_1, G_2 and identity respectively and n is the message bit length. PKG chooses random $s \in \mathbb{Z}_p^*$ as the master secret key and sets $P_{pub} = sP$. PKG publishes the system parameters as $\langle G_1, G_2, p, n, P, P_{pub}, e: G_1 \times G_1 \rightarrow G_2, g, H_1, H_2, H_3, H_4 \rangle$.

Let a function f be such that $f(ID) = 0$ if $ID = ID_{\emptyset}$ otherwise $f(ID) = 1$.

Extract Partial Private Key: Given a user U with identity ID_u the partial private key is computed by PKG as $D_u = (q_u + s)^{-1}P,$ where $q_u = H_1(ID_u)$. For $ID_\emptyset$, we set $D_\emptyset = \mathcal{O}$.

Set User Key: Given D_u, the user U chooses random $x_u \in \mathbb{Z}_p^*$ and set his private key $SK_u = \langle x_u,\ D_u \rangle$ and public key $PK_u = \mathrm{x_u T_u}$, where $T_u = (q_u + s)P$. For $ID_\emptyset$, we set $T_\emptyset = \mathcal{O}$ and $x_\emptyset = 0$, Thus $PK_\emptyset = \mathcal{O}$.

CLGSC: The sender A for the receiver B

1. Chooses $r \in_R \mathbb{Z}_p^*$
2. Computes
   i. $\alpha = g^r$
   ii. $r' = H_2(m, \alpha, ID_A, ID_B)$
   iii. $X = r'T_B$
   iv. $h_3 = H_3(m, \alpha, X, PK_A, PK_B, ID_A, ID_B)$
   v. $Z = \frac{r + r'}{x_A + h_3} D_A$
   vi. $y = m \parallel \alpha \parallel Z \parallel ID_A \oplus \left\{H_4\left(g^{r'} \parallel r'PK_B\right) f(ID_B)\right\}$, and
3. Returns $\sigma = (y, X)$

UCLGSC: On receiving σ from A, the user B

1. Recovers $m \parallel \alpha \parallel Z \parallel ID_A = y$ if $X = \mathcal{O}$, otherwise
2. Computes $\omega = e(X, D_B)$ and recovers $m \parallel \alpha \parallel Z \parallel ID_A = y \oplus \{H_4(\omega \parallel x_B X) f(ID_B)\}$
3. Computes $r' = H_2(m, \alpha, ID_A, ID_B)$
4. If $Z = \mathcal{O}$, accept the message iff $X = r'T_B$, otherwise
5. Computes $h_3 = H_3(m, \alpha, X, PK_A, PK_B, ID_A, ID_B)$ and accept the message iff $e(Z,\ PK_A + h_3 T_A) = \alpha g^{r'}$.

Consistency:

$$\omega = e(X, D_B) = e(r'T_B, D_B) = e(r'(q_B + s)P, (q_B + s)^{-1}P) = e(P, P)^{r'} = g^{r'}$$

$$x_B X = x_B r' T_B = r' PK_B$$

$$\begin{aligned} e(Z, PK_A + h_3 T_A) &= e\left(\frac{r \ + r'}{x_A + h_3} D_A, x_A T_A + h_3 T_A\right) \\ &= e\left(\frac{r \ + r'}{x_A + h_3} (q_A + s)^{-1}P, (x_A + h_3)(q_A + s)P\right) = e(P, P)^{r + r'} = g^r g^{r'} \\ &= \alpha g^{r'} \end{aligned}$$

Remarks:

1. When we only sign a message then specific receiver B does not exist therefore we use $ID_B = ID_\emptyset$ in CLGSC algorithm. Thus the function $f(ID_\emptyset)$ became 0 which helps to give us the signature $y = m \parallel \alpha \parallel Z \parallel ID_A$, also the component X of the output of CLGSC algorithm became $\mathcal{O}$. This will reduce the extra computation in UCLGSC.
2. When we only encrypt a message then specific sender A does not exist, therefore we use $ID_A = ID_\emptyset$ in CLGSC algorithm. Thus in the computation of Z we have $D_\emptyset = \ \mathcal{O}$ which will

again reduce the extra computation in UCLGSC by checking $X = r'T_B$, which will also provide chosen ciphertext security while we only encrypt a message.

3. The form of ciphertext is (y, X) either we encrypt a message or signcrypt a message. This prevents an adversary to embed a encryption to valid signcryption or vice versa. Similarly an adversary cannot embed a signature of a message to valid signcryption or vice versa because when we only sign a message then $X = \mathcal{O}$ as well as the computations of r' and h_3 involve both sender's and receiver's identity.
4. Also note that we use the same randomness for encryption and signature i.e. we use r' in the computation of Z, which avoids the unforgeability attack against proposed certificateless generalized signcryption, which we presented in section 6 on Ji et al. scheme.

8. Conclusion: In this paper we proposed two generalized signcryption scheme, first is identity based and second is certificateless. We also show that Ji et al. certificateless generalized signcryption scheme is not existentially unforgeable against insider Type-I adversary.

References:

1. S. S. Al-Riyami and K. G. Paterson: Certificateless public key cryptography. ASIACRYPT 2003, LNCS # 2894, pp. 452-473 Springer-Verlag, 2003.
2. M. Barbosa and P. Farshim: Certificateless signcryption. Proceedings of the 2008 ACM Symposium on Information, Computer and Communication Security, pp. 369-372, 2008.
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, Springler-Verlag, 2005.
4. D. Boneh and M. Franklin: Identity–based encryption scheme from Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 2001, 213-229.
5. Y. Chen and F. Zhang: A new certificateless public key encryption scheme. Wuhan University Journal of Natural Sciences, 13(6): 721-726, 2008.
6. Y. Han and X. Yang: ECGSC: Elliptic curve based generalized signcryption scheme. Cryptology ePrint Archive, Report 2006/126, 2006, http:/eprint.iacr.org/.
7. H. Ji, W. Han and L. Zhao: Certificateless generalized signcryption. Cryptology ePrint Archive, Report 2010/204, http://eprint.iacr.org/ 2010/204.pdf, 2010.
8. S. Lal and P. Kushwah: ID based generalized signcryption. Cryptology ePrint Archive, Report 2008/84, http://eprint.iacr.org/ 2008/84.pdf, 2008.
9. J. Malone-Lee: Identity-based signcryption, Cryptology ePrint Archive Report 2002/098.
10. A. Shamir: Identity-based cryptosystems and signature schemes. CRYPTO 84, LNCS # 196, pp 47-53 Springer-Verlag, 1984.
11. X. Wang, Y. Yang and Y. Han: Provable secure generalized signcryption. Cryptology ePrint Archive, Report 2007/173, 2007, http:/eprint.iacr.org/.
12. G. Yu, X. Ma, Y. Shen and W. Han: Provable secure identity based generalized signcryption scheme. Available at arXiv:1004.1304v1 [cs.CR], (to appear in Theoretical Computer Science), 2010.
13. 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.