Theoretical Computer Science 412 (2011) 6382–6389

Contents lists available at SciVerse ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

An efficient identity based generalized signcryption scheme

Prashant Kushwah[a,*], Sunder Lal[b]

[a] *Department of Mathematics and Statistics, Banasthali University, Rajasthan, India*

[b] *Department of Mathematics, Dr. B. R. A. (Agra) University, UP, India*

ARTICLE INFO

Article history:
Received 21 August 2010
Received in revised form 9 June 2011
Accepted 2 August 2011
Communicated by X. Deng

Keywords:
Signcryption
Generalized signcryption
Identity based cryptography
Provable security

ABSTRACT

Generalized signcryption is a new cryptographic primitive, which provides separate or joint encryption and signature as per need. It is more suitable for some storage constrained environments, e.g. smart card, WSN (Wireless Sensor Networks) etc. In this paper, we propose an efficient identity based generalized signcryption scheme. We also simplify the security notions for identity based generalized signcryption and prove the security of the proposed scheme under the new security model.

1. Introduction

The main advantages of public key cryptography are encryption and digital signatures, 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 [21] proposed a novel cryptographic primitive "Signcryption" which achieves both confidentiality and authenticity in a single logical step with the cost significantly lower than the "signature-then-encryption" approach. In 2002, Beak et al. [1] first formalized and defined security notions for signcryption, via semantic security against adaptive chosen ciphertext attack and existential unforgeability against adaptive chosen message attack. Many public key signcryption schemes have been proposed after [21]. Some of them are [2,12,13,22].

Identity based cryptography was first introduced by Shamir [18] in 1984. In the identity based cryptosystems, public keys 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). The first identity based signature scheme was given by Shamir [18] 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 [16] in 2002 and they also gave the security model for signcryption in identity based setting. Since then, many identity based signcryption schemes have been proposed in the literature [3,5,7,8,15]. Their main objective is to reduce the computational complexity and to design the more efficient identity based signcryption schemes.

Now consider the scenarios where sometimes we need confidentiality and authenticity separately and sometimes, we need both simultaneously. To achieve this, we can use three different schemes: an encryption scheme, a signature scheme and a signcryption scheme. However, in the low bandwidth environment e.g. smartcards and WSN (Wireless Sensor Networks), we cannot afford to use three different schemes to achieve confidentiality and authenticity separately or simultaneously. Han et al. [11] address the issue of implementation complexity of these cryptographic schemes and

[*] Corresponding author. Tel.: +91 9785039049.
E-mail addresses: pra.ibs@gmail.com (P. Kushwah), sunder_lal2@rediffmail.com (S. Lal).

0304-3975/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2011.08.009

proposed the concept of generalized signcryption, which can work as an encryption scheme or a signature scheme or a signcryption scheme as per need. Wang et al. [19] gave the security model for a generalized signcryption scheme and modified the scheme proposed in [11]. Han et al. proposed another generalized signcryption scheme based on bilinear pairing with the shortened ciphertext in [9] and a multi-recipient generalized signcryption scheme based on the gap Diffie–Hellman problem in [10]. The first identity based generalized signcryption along with a security model was proposed by Lal and Kushwah [14] in 2008. However, Yu et al. [20] showed that the security model for identity based generalized signcryption proposed in [14] is not complete. They modified the security model and proposed a concrete scheme which is secure in the modified model. In this work, we simplify the security model for identity based generalized signcryption and propose an efficient identity based generalized signcryption scheme. We also prove the security of the proposed scheme in the simplified model under the q-DHIP and q-BDHIP.

This paper is organized as follows. In Section 2, we define the identity based generalized signcryption scheme and propose a simplified security model for identity based generalized signcryption (IBGSC). Section 3 contains the preliminaries for the proposed scheme. In Section 4, we give the construction of the IBGSC scheme and in Section 5, we give the security results for our scheme in the new security model. In Section 6, we compare our scheme with the existing generalized signcryption schemes.

2. Identity based generalized signcryption (IBGSC)

An *identity based generalized signcryption (IBGSC) scheme* consists of the following 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. *IBGSC:* 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 $\sigma = IBGSC(D_A, m, ID_A, ID_B)$.
4. *IBGUSC:* This algorithm takes input $(\sigma, D_B, ID_B, ID_A)$ and outputs m and valid if σ is a valid generalized signcryption of m done by A for B, 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_φ. To only sign or encrypt a message m, use $ID_B = ID_\varphi$ or $ID_A = ID_\varphi$ respectively. Therefore, when $ID_B = ID_\varphi$, IBGSC becomes a signature scheme and output of the IBGSC algorithm is a signature of sender ID_A on the message m and when $ID_A = ID_\varphi$, IBGSC becomes an encryption scheme and output of the IBGSC algorithm is merely an encryption of message m for receiver ID_B. If $ID_A \neq ID_\varphi$, $ID_B \neq ID_\varphi$, then IBGSC works as the signcryption scheme and output of IBGSC is the signcryption of message m with the signature of sender ID_A to the receiver ID_B. Thus IBGSC works in three modes via signcryption mode, encryption-only mode and signature-only mode.

Security model for IBGSC

A security model for IBGSC was given in [14]. This model has recently been modified by Yu et al. [20]. In this section, we provide a new and simplified security model for IBGSC. The modified security notions for identity based generalized signcryption by Yu et al. [20] provide 7 oracles to the adversary namely Extract, Sign, Verify, Encrypt, Decrypt, GSC and GUSC. 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 the generalized signcryption algorithm. Similarly a single algorithm is used to decrypt and to verify a message. Therefore the oracles Encrypt, Decrypt, Sign and Verify seem redundant. In our simplified security model, we provide only two strong oracles namely IBGSC and IBGUSC to the adversary which she can query with specific inputs. The IBGSC oracle is so strong that it provides signcryption when $ID_A \neq ID_\varphi$ and $ID_B \neq ID_\varphi$, encryption when $ID_A = ID_\varphi$ and $ID_B \neq ID_\varphi$, signature when $ID_A \neq ID_\varphi$ and $ID_B = ID_\varphi$. Similarly, the IBGUSC oracle is so strong such that when $ID_A = ID_\varphi$ it only decrypts the message and when $ID_B = ID_\varphi$ it only verifies the signature. Otherwise it decrypts the message and verifies the signature.

2.1. 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.

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.
- *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 the IBGSC algorithm with message m and identities ID_A and ID_B and returns the output σ to the adversary $\mathcal{A}$. Note that if $\mathcal{A}$ sets $ID_A = ID_\varphi$, then $\mathcal{C}$ only encrypts the message m for ID_B and if $\mathcal{A}$ sets $ID_B = ID_\varphi$, then $\mathcal{C}$ only signs the message m under ID_A.
- *IBGUSC queries:* $\mathcal{A}$ submits two identities ID_A, ID_B along with σ to the challenger $\mathcal{C}$. $\mathcal{C}$ runs the IBGUSC algorithm with input σ, ID_A and ID_B and returns the output m and valid of IBGUSC. Note that if $\mathcal{A}$ sets $ID_A = ID_\varphi$, then σ is only the encryption for ID_B and if $\mathcal{A}$ sets $ID_B = ID_\varphi$, then σ is only the signature of ID_A on message m.

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 she wishes to be challenged. The adversary $\mathcal{A}$ must have made no private key extraction query on ID_B^*, also $ID_B^* \neq ID_\varphi$ for the confidentiality game. $\mathcal{C}$ picks randomly a bit $b \in \{0, 1\}$, runs the IBGSC algorithm with message m_b under ID_A^* and ID_B^* and returns the output σ^* 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 it is also not allowed to make an IBGUSC 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 $Adv_{\mathcal{A}}^{IND-CCA2} = 2\Pr[b = b'] - 1$.

Note:

1. Adversary $\mathcal{A}$ plays the above game with $ID_A^* = ID_\varphi$ for the confidentiality in the encryption only mode.
2. In the above game, adversary$\mathcal{A}$ cannot submit σ^* to the IBGUSC oracle strictly with sender ID_A^* and receiver ID_B^*. However, if σ^* is the signcrypted text, then $\mathcal{A}$ is allowed to transform the σ^* into a valid encrypted text and can query the IBGUSC oracle with sender ID_φ. Also, if σ^* is the encrypted text, then $\mathcal{A}$ is allowed to transform the σ^* into a valid signcrypted text and can query the IBGUSC oracle with sender $ID_A^* \neq ID_\varphi$.

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.

2.2. 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 the IBGSC query during the game and for which private key of ID_A^* was not exposed, also $ID_A^* \neq ID_\varphi$ for the signature unforgeability game. The forger wins if the output of $IBGUSC(\sigma, D_B^*, ID_B^*, ID_A^*)$ is not the $\perp$ symbol.
The adversary $\mathcal{A}$'s advantage is its probability of winning the above game.

Note:
1. Adversary $\mathcal{A}$ plays the above game with $ID_B^* = ID_\varphi$ for the unforgeability in the signature only mode.
2. In the above game σ is not a valid forgery if, it is the output of the IBGSC query strictly with identities ID_A^* and ID_B^*. But, it can be the transformation of valid signcrypted text obtained from the IBGSC query to the signature for the unforgeability in the signature only mode. Also it can be the transformation of valid signature obtained from the IBGSC query to the signcrypted text for some receiver ID_B^* for the unforgeability in the signcryption mode.

Definition 2. An IBGSC scheme is said to EUF-CMA secure, if no polynomially bounded adversary $\mathcal{A}$ has non-negligible advantage of winning the above game.

3. Preliminaries

Let $\mathbb{G}_1$ be an additive group and $\mathbb{G}_2$ be a multiplicative group both of the same prime order p. A function $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is called a *bilinear pairing* if it satisfies the following properties:

1. $\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}_p^*, e(aP, bQ) = e(P, Q)^{ab}$
2. For any $\mathcal{O} \neq P \in \mathbb{G}_1$, there is $Q \in \mathbb{G}_1$, such that $e(P, Q) \neq 1$
3. There exist an efficient algorithm to compute $e(P, Q) \forall P, Q \in \mathbb{G}_1$.

Given a $(q + 1)$ tuple $(P, aP, a^2P, \ldots, a^qP)$ to compute $\frac{1}{a}P$ is known as *q-Diffie–Hellman inversion problem (q-DHIP).*

Given a $(q + 1)$ tuple $(P, aP, a^2P, \ldots, a^qP)$ to compute $e(P, P)^{1/a} \in \mathbb{G}_2$ is known as *q-Bilinear Diffie–Hellman inversion problem (q-BDHIP).*

4. Proposed IBGSC scheme

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

Setup: Given a security parameter 1^k, the PKG chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order p, a random generator P of $\mathbb{G}_1$, and a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. PKG computes $g = e(P, P)$ and defines hash functions as $H_1 : \{0, 1\}^{k_3} \to \mathbb{Z}_p^*$, $H_2 : \{0, 1\}^{n+k_2+2k_3} \to \mathbb{Z}_p^*$, $H_3 : \{0, 1\}^{n+k_2+k_1+2k_3} \to \mathbb{Z}_p^*$, $H_4 : \{0, 1\}^{k_2} \to \{0, 1\}^{n+k_1+k_2+k_3}$, where k_1, k_2 and k_3 denote the number of bits to represent elements of $\mathbb{G}_1$, $\mathbb{G}_2$ 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 $\langle \mathbb{G}_1, \mathbb{G}_2, p, n, P, P_{pub}, e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2, g, H_1, H_2, H_3, H_4 \rangle$.

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

Key generation: 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_φ, we set $D_\varphi = \mathcal{O}$.

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. $X = r'f(ID_B)T_B$ where $T_B = H_1(ID_B)P + P_{pub}$, Note that $X = \mathcal{O}$ if $B = \varphi$
   iv. $h_3 = H_3(m, \alpha, X, ID_A, ID_B)$
   v. $Z = (r + h_3)D_A$
   vi. $y = m\|\alpha\|Z\|ID_A \oplus \{H_4(g^{r'})f(ID_B)\}$, and
3. Returns $\sigma = (y, X)$

IBGUSC: On receiving σ from A, the user B

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

Consistency:

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

$$\begin{aligned} e(Z, H_1(ID_A)P + P_{pub})g^{-h_3} &= e((r + h_3)D_A, (Q_A + s)P)g^{-h_3} \\ &= e((r + h_3)(Q_A + s)^{-1}P, (Q_A + s)P)g^{-h_3} = e(P, P)^{(r+h_3)}g^{-h_3} = g^{r+h_3}g^{-h_3} = g^r = \alpha. \end{aligned}$$

Remarks:

1. When we only sign a message, then specific receiver B does not exist therefore, we use $ID_B = ID_\varphi$ in the IBGSC algorithm. Thus the function $f(ID_\varphi)$ becomes 0 which helps to give us the component $X = \mathcal{O}$ and the signature $y = m\|\alpha\|Z\|ID_A$ of the output of the IBGSC algorithm. This reduces the extra computations in IBGUSC.
2. When we only encrypt a message, then specific sender A does not exist therefore, we use $ID_A = ID_\varphi$ in the IBGSC algorithm. Thus in the computation of Z, we use $D_\varphi = \mathcal{O}$ and obtain $Z = \mathcal{O}$. This reduces the extra computations in IBGUSC. By checking $X = r'f(ID_B)T_B$, we also get 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. The computations of r' and h_3 involve both sender's and receiver's identity. This prevents an adversary to embed an encryption to valid signcryption or vice versa. Similarly an adversary cannot embed a signature of a message to valid signcryption or vice versa.
4. An important feature of the proposed IBGSC scheme is that, there is no need to bind the information of sender and receiver to recognize that the ciphertext is the signcrypted text or the encrypted text or only the signature because the IBGUSC algorithm itself distinguish these modes.

5. Security results

Theorem 1 (*Message Confidentiality*). *Assume that an IND-CCA2 adversary $\mathcal{A}$ has an advantage ε against the proposed IBGSC scheme when running in time τ, asking q_{h_i} queries to the random oracles H_i $(i = 1, 2, 3, 4)$ and q_e, q_u IBGSC queries, IBGUSC queries respectively. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ with probability*

$$\varepsilon' > \frac{\varepsilon}{q_{h_1}(q_{h_4} + q_e)} \left(1 - \frac{q_u}{2^k}\right) \left(1 - \frac{q_e(q_e + q_{h_3})}{2^k}\right)$$

within a time $\tau' < \tau + O(q_e + q_u)\tau_p + O(q_{h_1}^2)\tau_{multi} + O(q_e)\tau_{\exp}$, where $\tau_{\exp}$, τ_{multi} and τ_p are the time for an exponentiation in $\mathbb{G}_2$, a multiplication in $\mathbb{G}_1$ and for a pairing computation.

Proof. Let $\mathcal{A}$ be an IND-CCA2 adversary against the proposed IBGSC scheme with advantage ε. We will show how adversary$\mathcal{A}$ is used to construct a simulator $\mathcal{B}$ that extract $e(P, P)^{1/a}$ on input $(P, aP, a^2P, \ldots, a^qP)$.

We will proceed similarly as in [3]. In the preparation phase, first $\mathcal{B}$ selects $\ell \in_R \{1, \ldots, q_{h_1}\}$, elements $\lambda_\ell \in_R \mathbb{Z}_p^*$, $\mu_1, \mu_2, \ldots, \mu_{\ell-1}, \mu_{\ell+1}, \ldots, \mu_q \in_R \mathbb{Z}_p^*$ and expands the polynomial $g(x) = \prod_{i=1, i\neq\ell}^{q} (x + \mu_i)$ to obtain the coefficients $c_1, c_2, \ldots, c_{q-1} \in_R \mathbb{Z}_p^*$ such that $g(x) = \sum_{i=0}^{q-1} c_i x^i$. $\mathcal{B}$ also computes $\lambda_i = \lambda_\ell - \mu_i \in \mathbb{Z}_p^*$ for $i = 1, \ldots, \ell - 1, \ell + 1, \ldots, q$.

Now $\mathcal{B}$ sets $G = \sum_{i=0}^{q-1} c_i(a^iP) = g(a)P$ as a public generator of $\mathbb{G}_1$ and computes another element $U \in \mathbb{G}_1$ as $U = \sum_{i=1}^{q} c_{i-1}(a^iP) = aG$. Note that $\mathcal{B}$ does not know a. Further $\mathcal{B}$ computes

$$g_i(x) = \frac{g(x)}{(x + \mu_i)} = \sum_{i=0}^{q-2} d_i x^i$$

for $i = 1, \ldots, \ell - 1, \ell + 1, \ldots, q$ such that

$$\frac{1}{(a + \mu_i)} G = \frac{g(a)}{(a + \mu_i)} = g_i(a)P = \sum_{i=0}^{q-2} d_i(a^iP).$$

Thus $\mathcal{B}$ can compute $q - 1 = q_{h_1} - 1$ pairs $\left(\mu_i, D_i = \frac{1}{a+\mu_i} G\right)$ by the last term of the above equation. The system wide public key P_{pub} is chosen as $P_{pub} = -U - \lambda_\ell G = (-a - \lambda_\ell)G$ with (unknown) private key $z = -a - \lambda_\ell \in \mathbb{Z}_p^*$. For all $i = 1, \ldots, \ell - 1, \ell + 1, \ldots, q$, $\mathcal{B}$ have $(\lambda_i, -D_i) = (\lambda_i, \frac{1}{\lambda_i + z} G)$.

Now simulator $\mathcal{B}$ starts the interaction with $\mathcal{A}$ on input (G, P_{pub}). $\mathcal{A}$ asks queries to $\mathcal{B}$ throughout the simulation. It is assumed that H_1 queries are distinct and any query involving the identity ID comes after an H_1 query on ID. The target identity ID_B^* is submitted to H_1 at some point of simulation. Also to maintain consistency in queries, $\mathcal{B}$ makes the lists L_i for the random oracles H_i for $i = 1, 2, 3, 4$. $\mathcal{B}$ initializes a counter η to 1 and starts answering $\mathcal{A}$'s queries as follows.

- *H_1 queries:* It takes input an identity ID. $\mathcal{B}$ answers λ_η to the ηth one such query and increment η. $\mathcal{B}$ sets the identity ID as ID_η.
- *H_2 queries:* It takes input $(m, \alpha, ID_\zeta, ID_\eta)$. $\mathcal{B}$ checks the list L_2, it returns a previous value if it exists. Otherwise it chooses a random $h_2 \in_R \mathbb{Z}_p^*$ and returns this value as the answer. It also stores this value in the L_2 list.
- *H_3 queries:* It takes input $(m, \alpha, X, ID_\zeta, ID_\eta)$. $\mathcal{B}$ checks the list L_3, it returns a previous value if it exists. Otherwise it chooses a random $h_3 \in_R \mathbb{Z}_p^*$ and returns this value as the answer. It also stores this value in the L_3 list.
- *H_4 queries:* It takes input $g^{r'}$. $\mathcal{B}$ checks the list L_4, it returns a previous value if it exists. Otherwise it chooses a random $h_4 \in_R \{0, 1\}^{n+k_1+k_2+k_3}$ and returns this value as the answer. It also stores this value in the L_4 list.
- *Keygen queries:* It takes input an identity ID_η. $\mathcal{B}$ fails if $\eta = \ell$ otherwise it knows that $H_1(ID_\eta) = \lambda_\eta$ and returns $-D_\eta = \frac{1}{\lambda_\eta + z} G$.
- *IBGSC queries:* It takes input a plaintext m and identities $(ID_A, ID_B) = (ID_\zeta, ID_\eta)$ where $\zeta, \eta \in \{1, \ldots, q_{h_i}\}$. If $\zeta \neq \ell$, $\mathcal{B}$ knows the sender's private key of ID_ζ is $-D_\zeta$ and can answer the query by following the specification of the IBGSC algorithm. So we assume that $\zeta = \ell$, then $\mathcal{B}$ does the following:
  i. Chooses $h_3 \in_R \mathbb{Z}_p^*$ and $Z \in_R \mathbb{G}_1$
  ii. Computes $e(Z, H_1(ID_\ell)G + P_{pub})e(G, G)^{-h_3} = \alpha$
  iii. Simulates H_2 as $H_2(m, \alpha, ID_\ell, ID_\eta) = r'$ and stores in the L_2 list.
  iv. Computes $X = r'T_\eta$ where $T_\eta = H_1(ID_\eta)G + P_{pub}$
  v. Sets $H_3(m, \alpha, X, ID_\ell, ID_\eta) = h_3$ and stores in L_3 list.
  vi. Simulates H_4 as $H_4(e(G, G)^{r'}) = h_4$ and stores in L_4 list.
  vii. Computes $y = m\|\alpha\|Z\|ID_\ell \oplus \{h_4 f(ID_\eta)\}$
  viii. Returns $\sigma = (y, X)$.

Note that if $ID_\eta = ID_\varphi$, $\mathcal{B}$ answers the IBGSC query in the same way using ID_φ in place of ID_η and returns the signature $(m\|\alpha\|Z\|ID_\ell, \mathcal{O})$. Also $\mathcal{B}$ fails if H_3 is already defined but this happens with a probability smaller than $(q_e + q_{h_3})/2^k$.

- *IBGUSC queries:* It takes input a ciphertext (y, X) and a receiver's identity ID_η. If $ID_\eta \neq ID_\ell$, then $\mathcal{B}$ knows receiver's private key of ID_η is $-D_\eta$. $\mathcal{B}$ runs the IBGUSC algorithm normally and returns the output to $\mathcal{A}$. Also if $ID_\eta = ID_\varphi$, then $\mathcal{B}$ is able to give an appropriate answer to $\mathcal{A}$. If $ID_\eta = ID_\ell$, then $\mathcal{B}$ rejects the ciphertext. Across the whole game an inappropriate rejection occurs with probability at most $q_u/2^k$.

At the end of challenge phase, $\mathcal{A}$ outputs two messages m_0, m_1 and identities ID_A^*, ID_B^* such that she has not made Keygen query on ID_B^*. Note that for the confidentiality in the encryption mode, adversary $\mathcal{A}$ will choose $ID_A^* = ID_\varphi$. If $ID_B^* \neq ID_\ell$, $\mathcal{B}$ aborts the simulation. Otherwise it picks $\xi \in_R \mathbb{Z}_p^*$, $y \in_R \{0, 1\}^{n+k_1+k_2+k_3}$ to return the challenge $\sigma^* = (y, X)$ where $X = -\xi G \in \mathbb{G}_1$. If we define $\delta = \xi/a$ and since $z = -a - \lambda_\ell$, we can check that

$$X = -\xi G = -a\delta G = (\lambda_\ell + z)\delta G = \delta\lambda_\ell G + \delta P_{pub}.$$

$\mathcal{A}$ cannot recognize that σ^* is not a valid ciphertext unless she queries H_2, H_3 or H_4 on $e(G, G)^\delta$. Also in the guess stage, her view is simulated as before and her eventual output is ignored. Standard arguments can show that a successful $\mathcal{A}$ is very likely to query H_2, H_3 or H_4 on the input $e(G, G)^\delta$ if the simulation is indistinguishable from a real attack environment.

To produce a result, $\mathcal{B}$ fetches a random record from the L_4 list. As L_4 contains no more than $(q_{h_4} + q_e)$ records by construction thus with probability $\frac{1}{(q_{h_4}+q_e)}$, $\mathcal{B}$ chooses the record which will contain the right element $e(G, G)^\delta = e(P, P)^{g(a)^2\xi/a}$ where $G = g(a)P$.

The q-BDHIP solution can be extracted as follows. If $\omega^* = e(P, P)^{1/a}$, then

$$e(G, G)^{1/a} = (\omega^*)^{c_0^2} e\left(\sum_{i=0}^{q-2} c_{i+1}(a^i P), c_0 P\right) e\left(G, \sum_{j=0}^{q-2} c_{j+1}(a^j P)\right).$$

In an analysis of $\mathcal{B}$'s advantage, following events will cause $\mathcal{B}$ to abort the simulation:

E_1: $\mathcal{A}$ does not choose to be challenge on ID_ℓ
E_2: a Keygen query is made on ID_ℓ
E_3: $\mathcal{B}$ aborts in the IBGSC query because of a collision on H_3
E_4: $\mathcal{B}$ rejects a valid ciphertext at some point of the game.

We clearly have probability $\Pr[\neg E_1] = 1/q_{h_1}$ and we know that $\neg E_1$ implies $\neg E_2$. Also $\Pr[E_3] \le q_e(q_e + q_{h_3})/2^k$ and $\Pr[E_4] \le q_u/2^k$. Thus we find that

$$\Pr[\neg E_1 \wedge \neg E_3 \wedge \neg E_4] \ge \frac{1}{q_{h_1}}\left(1 - \frac{q_u}{2^k}\right)\left(1 - \frac{q_e(q_e + q_{h_3})}{2^k}\right).$$

Also the probability that $\mathcal{B}$ selects the correct record from the L_4 list is $\frac{1}{(q_{h_4}+q_e)}$. Therefore the advantage of $\mathcal{B}$ is

$$\varepsilon' > \frac{\varepsilon}{q_{h_1}(q_{h_4} + q_e)}\left(1 - \frac{q_u}{2^k}\right)\left(1 - \frac{q_e(q_e + q_{h_3})}{2^k}\right).$$

The time bound is obtained as there are $O(q_{h_1}^2)$ multiplications in the preparation phase, $O(q_e + q_u)$ pairing computations and $O(q_e)$ exponentiations in $\mathbb{G}_2$. □

Theorem 2 (*Signature Unforgeability*). *Assume that there is an EUF-CMA adversary $\mathcal{A}$ against the proposed IBGSC scheme. Also assume that $\mathcal{A}$ produces a forgery with probability $\varepsilon \ge 10(q_e + 1)(q_e + q_{h_3})/2^k$ when asking q_{h_i} queries to the random oracles H_i $(i = 1, 2, 3, 4)$ and q_e, q_u IBGSC queries, IBGUSC queries respectively, within the time τ. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ in the expected time $\tau' \le 120686 q_{h_1} q_{h_3}(\tau + O(q_e + q_u)\tau_p + O(q_u q_{h_3})\tau_{\exp})/\varepsilon(1 - 1/2^k) + O(q_{h_1}^2)\tau_{multi}$ where $\tau_{\exp}$, τ_{multi} and τ_p are the same as in Theorem 1.*

Proof. Proof is the combination of the following two lemmas.

Lemma 1. *Assume that there is a forger $\mathcal{A}$ for an adaptively chosen message and identity attack having advantage ε against our scheme when asking q_{h_i} queries to the random oracles H_i $(i = 1, 2, 3, 4)$ and q_e, q_u IBGSC queries, IBGUSC queries respectively. Then there exists an algorithm $\mathcal{A}'$ for adaptively chosen message and given identity attack, asking same number of queries as $\mathcal{A}$ and has the advantage $\varepsilon' > \frac{\varepsilon}{q_{h_1}}\left(1 - \frac{q_u}{2^k}\right)$.*

Proof. The proof of Lemma 1 is similar to the proof of lemma 1 in [6]. □

Lemma 2. *Assume that there is chosen message and given identity attacker $\mathcal{A}$ against the proposed IBGSC scheme. Let $\mathcal{A}$ produces a forgery with probability $\varepsilon \ge 10(q_e + 1)(q_e + q_{h_3})/2^k$ when asking q_{h_i} queries to the random oracles H_i $(i = 1, 2, 3, 4)$ and q_e, q_u IBGSC queries, IBGUSC queries respectively, within the time τ. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ in the expected time $\tau' \le 120686 q_{h_3}(\tau + O(q_e + q_u)\tau_p + O(q_e)\tau_{\exp})/\varepsilon + O(q_{h_1}^2)\tau_{multi}$ where $\tau_{\exp}$, τ_{multi} and τ_p are the same as in Theorem 1.*

Proof. We are going to use "forking lemma" technique of Pointcheval and Stern [17] to prove our result.

We will in fact reduce the q-DHIP in bilinear group $\mathbb{G}_1$ to the problem of forging. Since a black box for the q-DHIP is sufficient to solve the q-BDHIP the result will follow. We will now show how an EUF-CMA adversary $\mathcal{A}$ of IBGSC may be used to construct a simulator $\mathcal{B}$ that solves the q-DHIP. Let $(P, aP, a^2P, \ldots, a^qP)$ be the instant of the q-DHIP that we wish to solve.

In the preparation phase, $\mathcal{B}$ setup similarly as in Theorem 1. Then simulator $\mathcal{B}$ starts answering $\mathcal{A}$'s queries throughout the simulation. Also $\mathcal{B}$ makes the lists L_i for the random oracles H_i $(i = 1, 2, 3, 4)$ to maintain consistency. $\mathcal{B}$ initializes a counter η to run $\mathcal{A}$ on input (G, P_{pub}, ID_ℓ) for a random chosen challenge identity $ID_\ell \in \{0, 1\}^*$.

Also to simulate $\mathcal{A}$'s environment in a chosen message and given identity attack, $\mathcal{B}$ answers $\mathcal{A}$'s queries to the random oracles H_1, H_2, H_3, H_4, IBGSC and IBGUSC as in the proof of Theorem 1. Let us assume that $\mathcal{A}$ forges a ciphertext (y, X) for a recipient's identity ID_B (or a signature $(m\|\alpha\|Z\|ID_\ell, \mathcal{O})$ with recipient's identity ID_φ) in time τ with probability

Table 1

Scheme	Sign/Encrypt			Decrypt/Verify		
	mul in $\mathbb{G}_1$	exps in $\mathbb{G}_2$	e cps	mul in $\mathbb{G}_1$	exps in $\mathbb{G}_2$	e cps
Barreto et al. [3]	2	1	0	0	1	2
Lal et al. [14]	5	0	1	1	0	4
Yu et al. [20]	3	1	1	0	2	4
Proposed IBGSC	2	2	0	1 or 0	1 or 0	2 or 1

$\varepsilon \geq 10(q_e + 1)(q_e + q_{h_3})/2^k$ when making q_e IBGSC queries and q_{h_3} random oracle queries on H_3. Also ID_B cannot be ID_ℓ because of the irreflexivity assumption, so $\mathcal{B}$ can extract clean message signature pair from ciphertext. Therefore in both the cases when $ID_B = ID_\varphi$ or $ID_B \neq ID_\varphi$, $\mathcal{B}$ has a message signature pair $(m, \alpha, h_3, Z, ID_\ell)$. Note that $\mathcal{A}$ does not know the private key corresponding to ID_ℓ. Then by forking lemma there exists a turning machine $\mathcal{A}'$ that runs $\mathcal{A}$ sufficient number of times on input (G, P_{pub}, ID_ℓ) to obtain two suitable related forgeries which gives $(m, \alpha, h_3, Z, ID_\ell)$ and $(m, \alpha, h_3', Z', ID_\ell)$ with $h_3 \neq h_3'$, in the expected time $\tau' \leq 120686 q_{h_3}\tau/\varepsilon$. To solve the q-DHIP simulator $\mathcal{B}$ runs $\mathcal{A}'$ to obtain two forgeries $(m^*, \alpha, h_3, Z, ID_\ell)$ and $(m^*, \alpha, h_3', Z', ID_\ell)$ with $h_3 \neq h_3'$ for the same message m^* and commitment α. Since both forgeries satisfy the verification equation, we have

$$e(Z, T_{ID_\ell})e(G, G)^{-h_3} = e(Z', T_{ID_\ell})e(G, G)^{-h_3'}$$

where $T_{ID_\ell} = (\lambda_\ell + z)G = -aG$. Then it gives

$$e(Z - Z', T_{ID_\ell}) = e(G, G)^{h_3 - h_3'}$$
$$e((h_3 - h_3')(Z - Z'), T_{ID_\ell}) = e(G, G)$$

and hence $V^* = (h_3 - h_3')(Z - Z') = \frac{1}{a}G$. From V^*, $\mathcal{B}$ can extract $\delta^* = \frac{1}{a}P$; as it knows

$$g(x)/x = (c_0/x) + \sum_{i=0}^{q-2} c_i x^i$$

and eventually computes $\delta^* = \frac{1}{c_0}\left[V^* - \sum_{i=0}^{q-2} c_i(a^i P)\right] = \frac{1}{a}P$ which is return as a result.

Thus if $\mathcal{A}$ makes a forgery in time τ with probability $\varepsilon \geq 10(q_e + 1)(q_e + q_{h_3})/2^k$, then $\mathcal{B}$ solves the q-DHIP in expected time $\tau' \leq 120686 q_{h_3}(\tau + O(q_e + q_u)\tau_p + O(q_e)\tau_{\exp})/\varepsilon + O(q_{h_1}^2)\tau_{multi}$. □

6. 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 calculations while we use generalized signcryption for encryption and signature. However, the proposed IBGSC scheme significantly decreases the extra calculation in encryption and signature. Also, the proposed IBGSC scheme is as efficient as the identity based signcryption scheme in [3] which is the most efficient identity based signcryption scheme till date. In Table 1, we compare the dominant operations required for IBGSC and other schemes.

7. Conclusion

In this paper, we proposed an efficient identity based generalized signcryption scheme. We compare our scheme with the identity based generalized signcryption scheme proposed earlier and showed that our scheme is the most efficient among the available identity based generalized signcryption schemes. We also gave the proofs of security based on q-DHIP and q-BDHIP in the random oracle model.

Acknowledgement

The authors would like to thank the anonymous referees for their helpful comments.

References

[1] J. Baek, R. Steinfeld, Y. Zheng, Formal proofs of security of signcryption, in: PKC'02, in: LNCS, vol. 2274, 2002, pp. 81–98.

[2] F. Bao, R.H. Deng, A signcryption scheme with signature directly verifiable by public key, in: Proceeding of PKC'98, in: LNCS, vol. 1431, Springer-Verlag, 1998, pp. 55–59.

[3] P.S.L.M. Barreto, B. Libert, N. McCullagh, J.J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, in: Asicrypto'05, in: LNCS, vol. 3788, Springer-Verlag, 2005, pp. 515–532.

[4] D. Boneh, M. Franklin, Identity-based encryption scheme from Weil pairing, in: CRYPTO 2001, in: LNCS, vol. 2139, Springer-Verlag, 2001, pp. 213–229.

[5] X. Boyen, Multipurpose Identity based signcryption: A Swiss army knife for identity based cryptography, in: CRYPTO 2003, in: LNCS, vol. 2729, Springer-Verlag, 2003, pp. 389–399.

[6] J.C. Cha, J.H. Cheon, An identity-based signature from Gap Diffie–Hellman groups, in: PKC-2003, in: LNCS, vol. 2567, Springer-Verlag, 2003, pp. 18–30.

[7] L. Chen, J. Malone-Lee, Improved identity-based signcryption, in: PKC 2005, in: LNCS, vol. 3386, Springer-Verlag, 2005, pp. 362–379.

[8] S.S.M. Chow, S.M. Yiu, L.C.K. Hui, K.P. Chow, Efficient forward and provably secure ID based signcryption scheme with public verifiability and public cipher text authenticity, in: ICISC'2003, in: LNCS, vol. 2971, Springer-Verlag, 2003, pp. 352–369.

[9] Y. Han, X. Gui, BPGSC, Bilinear pairing based generalized signcryption scheme. GCC, in: Eighth International Conference on Grid and Cooperative Computing, 2009, pp. 76–82.

[10] Y. Han, X. Gui, Adaptive secure multicast in wireless networks, International Journal of Communication System 22 (9) (2009) 1213–1239.

[11] Y. Han, X. Yang, P. Wei, Y. Wang, Y. Hu, ECGSC: Elliptic Curve Based Generalized Signcryption. UIC 2006, in: LNCS, vol. 4159, 2006, pp. 956–965.

[12] R. Hwang, C. Lai, F. Su, An efficient signcryption scheme with forward secrecy based on elliptic curve, Applied Mathematics and Comutation 165 (2005) 870–881.

[13] H.Y. Jung, K.S. Chang, D.H. Lee, J.I. Lim, Signcryption schemes with forward secrecy, in: Proceeding of WISA 2 2001, pp. 403–233.

[14] S. Lal, P. Kushwah, ID based generalized signcryption, Cryptology ePrint Archive, Report 2008/84, http://eprint.iacr.org/2008/84.pdf, 2008.

[15] B. Libert, J.J. Quisquater, New identity based signcryption schemes from pairings, IEEE Information Theory Workshop, Paris, France, http://eprint.iacr.org/2003/023, 2003.

[16] J. Malone-Lee, Identity-based signcryption, Cryptology ePrint Archive Report 2002/098.

[17] D. Pointcheval, J. Stein, Security arguments for digital signatures and blind signatures, Journal of Cryptology 13 (3) (2000) 361–396. Springer-Verlag, Berlin.

[18] A. Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO'84, in: LNCS, vol. 196, Springer-Verlag, 1984, pp. 47–53.

[19] X. Wang, Y. Yang, Y. Han, Provable secure generalized signcryption. Cryptology ePrint Archive, Report 2007/173, 2007, http://eprint.iacr.org/.

[20] G. Yu, X. Ma, Y. Shen, W. Han, Provable secure identity based generalized signcryption scheme, Theoretical Computer Science 411 (40–42) (2010) 3614–3624.

[21] Y. Zheng, Digital signcryption or how to achieve cost (Signature & Encryption) Cost (Signature) + Cost (Encryption), in: CRYPTO'97, in: LNCS, vol. 1294, Springer-Verlag, 1997, pp. 165–179.

[22] Y. Zheng, H. Imai, How to construct efficient signcryption schemes on elliptic curves, Information Proceeding Letters 68 (5) (1998) 227–233.