Generalization of Barreto et al ID based Signcryption Scheme

Sunder Lal and Prashant Kushwah
Department of Mathematics
Dr B. R. A. (Agra) University
Agra- 282002 (UP) - INDIA
E-mail: sunder_lal2@rediffmail.com, pra.ibs@gmail.com

Abstract: This paper presents an efficient and provable secure identity based generalized signcryption scheme based on [1] which can work as signcryption scheme, encryption scheme and signature scheme as per need. Its security is proved under the difficulty of q-BDHIP. A generalized signcryption scheme in multiple PKGs environment is also proposed.

Keywords: ID based signcryption, generalized signcryption, and multiple PKGs environment.

1. Introduction:

Signcryption is a cryptographic primitive due to Zheng [13] in 1997 which achieves both confidentiality and authenticity in a single logical step. Signcryption is to reduce the computation cost and communication overhead in comparison of sign-then-encrypt approach. An identity based signcryption was given by Malone Lee [9] in 2002 based on bilinear pairing. Several identity based signcryption schemes have been proposed since then. However, the construction of Barreto et al [1] on asymmetric bilinear pairing is considered as most efficient one till the date.

In 2006, Han and Yang [4] generalized the concept of signcryption. The idea of this new primitive is to reduce the implementation complexity and not the computation cost or communication overhead. In most communication scenarios, the users need both confidentiality and authentication. However, in some cases they just need confidentiality, and sometimes they just need authentication. In this scenario, according to Zheng, signcryption may be replaced with signature/encryption algorithm. Thus to resolve problem, Zheng's solution requires the use of three cryptographic algorithms signcryption, encryption and signature as per need. This however is problematic. Generalized signcryption is an attempt to solve this problem. Generalized signcryption is a new primitive which can work as an encryption scheme, a signature scheme, and a signcryption scheme as per need. In [4] Han and Yang gave the generalized signcryption scheme based on elliptic curve. Wang et al [12] improved upon the scheme [4] and provided security notions of generalized signcryption. In [12] Wang et al made some modifications in the scheme [4]. First they removed the additional property from the hash functions that is $\mathrm{H}(0) \to 0, \mathrm{K}(0) \to 0, \mathrm{LH}(0) \to 0, \quad \mathrm{MAC}(0) \to 0$ because if there exists non-change point in hash function this would bring bad effects to hash function. Secondly they removed if-else clause from the scheme.

An identity based generalized signcryption (IDGSC) scheme is given by Lal and Kushwah in [7]. They also consider the security notion of generalized signcryption in identity based setting. The scheme in [7] reduces to basic scheme of Boneh-Franklin ID based encryption which is only chosen plaintext secure.

In this paper we present an efficient and secure identity based generalized signcryption based on Barreto et al signcryption scheme [1].

2. IDGSC and its Security notions:

An IDGSC scheme consists of the following algorithm

Set Up: On input of a security parameter 1^k the private key generator (PKG) uses this algorithm to produce a pair (**param**, s), where params are global public parameters for the system and s is the master secrete key. The public parameters include P_{pub}, the public key of PKG, a description of finite message space $\mathcal{M}$, a description of a finite signature space $\mathcal{S}$ and a description of a finite ciphertext space $\mathcal{C}$.. Further, there is no need for publicly known **param** to be explicitly provided as input to any other algorithm.

Extract: On input of an identity ID_U and the master key s, PKG uses this algorithm to compute secrete key d_{ID_U} corresponding to ID_U.

GSC: Suppose Alice (ID_A) wants to send a message m to Bob (ID_B). On input (d_{ID_A} , $ID_{B,}$ m), Alice uses this algorithm to produce cipher text c.

UGSC: On receiving c, Bob uses this algorithm with input ($ID_{A,} S_B$, c) and obtains m if c is valid ciphertext, and the symbol $\perp$ if c is invalid ciphertext.

The two algorithms GSC and UGSC are such that c =(S_A , $ID_{B,}$ m) iff m= UGSC ($ID_{A,} S_B$, c).

Signature-Only mode: If Alice wants only to sign a message m, then the specific receiver Bob does not exist. In this case $ID_B = ID_\phi$, GSC (S_A , ID_ϕ, m) = Sign (S_A , m), and UGSC ($ID_{A,}$ S_ϕ, c) = Verify (ID_A, m).

Encryption-Only mode: If a message is encrypted for Bob, then the specific sender Alice does not exist. In this case GSC (S_ϕ, $ID_{B,}$ m) = Enc ($ID_{B,}$ m), and UGSC (ID_ϕ , S_B , c) = Dec (S_B , c).

Security notions for IDGSC:

We now discuss the security model for proposed identity based generalized signcryption scheme.

2.1 Message Confidentiality (signcryption-mode)

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting **params** to the adversary. It keeps s secrete.

Probing:

Phase1: The adversary makes the following queries to probes the challenger.

- **Sign:** The adversary submits a signer identity and a message to the challenger. The challenger responds with the signature of the signer on the message.
- **Signcrypt:** The adversary submits identities of a sender and a receiver and a message to the challenger. The challenger responds with the signature of the sender on the message, encrypted under the public key of the receiver.
- **Decrypt:** The adversary submits a ciphertext and a receiver's identity to the challenger. The challenger decrypts the ciphertext under the secrete key of receiver and returns the message.
- **Unsigncrypt:** The adversary submits a ciphertext and identities of a sender and a receiver to the challenger. The challenger decrypts the ciphertext under the secrete key of receiver. It then verifies that the resulting decryption is a valid message/signature pair under the public key of the sender. If so the challenger returns the message, its signature and the identity of the signer, otherwise it returns $\perp$.
- **Extract:** The adversary submits an identity to the challenger. The challenger responds with the secrete key of that identity.

At the end of phase1 the adversary outputs two identities $\{ ID_A, ID_B \}$ and two messages $\{ m_0, m_1 \}$. The adversary must not have made extraction query on ID_B and $ID_B \neq ID_\phi$.

Challenge: The challenger chooses a bit b uniformly at random. It signs m_b under secrete key corresponding to ID_A and encrypts the result under the public key of ID_B to produce c. The challenger returns c to the adversary.

Phase2: The adversary continues to probe the challenger with the same type of queries that it made in the phase1. It is not allowed to extract the private key corresponding to ID_B and it is not allowed to make a decrypt and unsigncrypt query for c under ID_B .

Response: The adversary returns a bit b'. The adversary wins if $b' = b$.

Let $\mathcal{A}$ denote an adversary that plays the game above. The scheme is said to be *semantically secure against adaptive chosen ciphertext attack*, or IND-IDGSC-CCA2 secure in signcryption mode if the quantity $\mathbf{Adv}[\mathcal{A}]= 2\Pr[b' = b] - 1$ is negligible.

Note that above definition deals with insider security since the adversary is assumed to have access to the private key of the sender of a signcrypted message. This means that confidentiality is preserved even if a sender's key is compromised.

2.2 Message Confidentiality (encryption-only mode)

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting **params** to the adversary. It keeps s secrete.

Probing: The challenger is probed by the adversary who makes queries as in the phase1 of the game in section 2.1.

At the end of phase1 the adversary outputs receiver's identity ID_B and two messages $\{m_0, m_1\}$.

The adversary must not have made extraction query on ID_B and $ID_B \neq ID_\phi$.

Challenge: The challenger chooses a bit b uniformly at random. It signs m_b under secrete key corresponding to ID_ϕ and encrypts the result under the public key of ID_B to produce c. The challenger returns c to the adversary.

Phase2: The adversary continues to probe the challenger with the same type of queries that it made in the phase1. It is not allowed to extract the private key corresponding to ID_B and it is not allowed to make a decrypt and unsigncrypt query for c under ID_B.

Response: The adversary returns a bit b'. The adversary wins if $b' = b$.

Let $\mathcal{A}$ denote an adversary that plays the game above. The scheme is said to be *semantically secure against adaptive chosen ciphertext attack*, or IND-IDGSC-CCA2 secure in encryption-only mode if the quantity $\mathbf{Adv}[\mathcal{A}]= 2\Pr[b' = b] - 1$ is negligible.

2.3 Signature Non-repudiation (signcryption mode)

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting **params** to the adversary. It keeps s secrete.

Probing: The challenger is probed by the adversary who makes queries as in the phase1 of the game in section 2.1.

Forge: The adversary returns a recipient identity ID_B and a ciphertext c. Let (m, ID_A, σ) be the result of decrypting c under the secrete key corresponding to ID_B. The adversary wins if $ID_A \neq ID_B$; $ID_A \neq ID_\phi$; **Verify** $(m, ID_A, \sigma) = \top$; no extraction query was made on ID_A; no sign query was responded with (m, ID_A, σ) and no signcrypt query $(m, ID_A, ID_{B'})$ was responded to with a ciphertext whose decryption under the private key of $ID_{B'}$ is (m, ID_A, σ).

Let $\mathcal{A}$ denote an adversary that plays the game above. The scheme is said to be *existentially unforgeable against adaptive chosen message and ciphertext attack*, or EUF-IDGSC-CMA secure in signcryption mode if the quantity $\mathbf{Adv}[\mathcal{A}] = \Pr[\mathcal{A} \text{ wins}]$ is negligible.

The above definition allows the adversary access to the secret key of the recipient of the forgery. It thus gives us insider security.

2.4 Signature Non-repudiation (signature-only mode)

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting **params** to the adversary. It keeps s secrete.

Probing: The challenger is probed by the adversary who makes queries as in the phase1 of the game in section 2.1.

Forge: The adversary returns a triplet (m, ID_A, σ). The adversary wins if $ID_A \neq ID_\phi$; **Verify** $(m, ID_A, \sigma) = \top$; no extraction query was made on ID_A; no sign query was responded with (m, ID_A, σ) and no signcrypt query (m, ID_A, ID_B) was responded to with a ciphertext whose decryption under the private key of ID_B is (m, ID_A, σ).

Let $\mathcal{A}$ denote an adversary that plays the game above. The scheme is said to be *existentially unforgeable against chosen message and identity attack*, or EUF-IDGSC-CMA secure in signature-only mode if the quantity **Adv**[$\mathcal{A}$]=Pr[$\mathcal{A}$ wins] is negligible.

3. IDGSC scheme [7]:

Setup: Establishes parameters G_1, G_2, q, $e: G_1 \times G_1 \to G_2$, $H_0: \{0,1\}^{k_1} \to G_1$, $H_1: \{0,1\}^{k_0+n} \to \mathbb{Z}_q^*$, $H_2: G_2 \to \{0,1\}^{k_0+k_1+n}$, where k_0 is the number of bits required to represent an element of G_1, k_1 is the number of bits required to represent an identity of a user and n is a number of bits of a message unit. Let P be the generator of cyclic group G_1. PKG chooses a random $s \in_R \mathbb{Z}_q^*$ and computes his public key P_{Pub} = sP. The system parameter **params** are $\langle G_1, G_2, q, e, P, P_{pub}, n, H_0, H_1, H_2 \rangle$. Further the output of $H_2(1)$ is $(k_0 + k_1 + n)$ bit zero string.

Extract: Extracts private key of the user U with $ID_U \in \{0,1\}^{k_1}$

Computes the public key $Q_U = H_0(ID_U)$ and the private key $S_U = sQ_U$.

For signature-only mode (encryption-only mode) where receiver (sender) does not exist, we use the key pair $(\mathcal{O}, \mathcal{O}) \leftarrow (Q_U, S_U)$ when U= $ID_U = ID_\phi$ where ID_ϕ is a k_1 bits zero string.

Signcryption mode:

$\mathbf{GSC(S_A, ID_B, m):}$ To send a message $m \in \{0,1\}^n$ to Bob (ID_B) in a secure and authenticated way, Alice (ID_A) does the following:

1. Chooses $r \in_R \mathbb{Z}_q^*$
2. Computes
   (i) $X = rP + rQ_A$, where $Q_A = H_0(ID_A)$
   (ii) $Z = rP_{Pub} + (r + h_1)S_A$, where $h_1 = H_1(X \| m)$
   (iii) $\omega = e(rP_{Pub} + rS_A, Q_B)$, where $Q_B = H_0(ID_B)$
   (iv) $y = (Z \| ID_A \| m) \oplus H_2(\omega)$
3. Returns $c = (X, y)$.
   Here c is the signcryptext of message m.

$\mathbf{UGSC(ID_A, S_B, c):}$ On receiving the signcrypt-text $c = (X, y)$, Bob

1. Computes
   (i) $Q_A = H_0(ID_A)$
   (ii) $\omega = e(X, S_B)$
   (iii) $y \oplus H_2(\omega) = Z \| ID_A \| m$
   (iv) $h_1 = H_1(X \| m)$
   (v) $e(Z, P)$
   (vi) $e(P_{pub}, X + h_1 Q_A)$
2. Returns valid iff
   $e(Z, P) = e(P_{pub}, X + h_1 Q_A)$

Signature-only mode:

GSC (S_A, ID_ϕ, m) = Sign (S_A, m)

If Alice only wants to sign $m \in \{0,1\}^n$, then she

1. Chooses $r \in_R \mathbb{Z}_q^*$
2. Computes
   (i) $X = rP + rQ_A$, where $Q_A = H_0(ID_A)$
   (ii) $Z = rP_{Pub} + (r + h_1)S_A$, where $h_1 = H_1(X \| m)$
   (iii) $1 = e(P_{Pub} + S_A, \mathcal{O})^r$
   (iv) $Z \| ID_A \| m = (Z \| ID_A \| m) \oplus H_2(1)$, and
3. Returns $\sigma = (Z \| ID_A \| m, X)$.

Here σ is the signature on message m.

UGSC (ID_A, ID_ϕ, σ) = Verify (ID_A, σ)

Any one can verify the signature on m by computing

(i) $Q_A = H_0(ID_A)$
(ii) $1 = e(X, \mathcal{O})$
(iii) $Z \| ID_A \| m \oplus H_2(1) = Z \| ID_A \| m$
(iv) $h_1 = H_1(X \| m)$
(v) $e(Z, P)$
(vi) $e(P_{pub}, X + h_1 Q_A)$

and concluding that σ is valid iff

$$e(Z, P) = e(P_{pub}, X + h_1 Q_A).$$

Encryption-only mode:

GSC (ID_ϕ, ID_B, m) = Enc (ID_B, m)

If user wants to send a message $m \in \{0,1\}^n$ in a secure manner to Bob then he/she

1. Chooses $r \in_R \mathbb{Z}_q^*$
2. Computes
   (i) $X = rP = rP + \mathcal{O}$
   (ii) $h_1 = H_1(X \| m)$
   (iii) $Z = rP_{Pub} = rP_{Pub} + (r+h_1)\mathcal{O}$
   (iv) $\omega = e(rP_{Pub}, Q_B) = e(rP_{Pub} + \mathcal{O}, Q_B)$
   (v) $y = (Z \| ID_\phi \| m) \oplus H_2(\omega)$
3. Returns $c = (X, y)$ as the ciphertext of the message m.

UGSC (ID_ϕ, d_{ID_B}, c) = Dec (S_B, c)

On receiving ciphertext $c = (X, y)$, Bob

1. Computes
   (i) $\omega = e(X, S_B)$
   (ii) $Z \| ID_\phi \| m = y \oplus H_2(\omega)$
   (iii) $h_1 = H_1(X \| m)$
   (iv) $e(Z, P)$
   (v) $e(P_{pub}, X + h_1\mathcal{O})$
2. Accepts m as plaintext iff

$$e(Z, P) = e(P_{pub}, X + h_1\mathcal{O}).$$

4. Preliminaries:

Asymmetric Bilinear Pairing [1]: Let k be a security parameter and q be a k-bit prime number. Let us consider groups $(\mathbb{G}_1, +)$, $(\mathbb{G}_2, +)$ and $(\mathbb{G}_T, .)$ of the same prime order q. Let $\mathbb{G}_1 = \langle P \rangle$ and $\mathbb{G}_2 = \langle Q \rangle$. There exists an asymmetric bilinear pairing $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ satisfying the following properties

1. **Bilinearty:** $\forall (S, T) \in \mathbb{G}_1 \times \mathbb{G}_2, \forall a, b \in \mathbb{Z}$, $e(aS, bT) = e(S, T)^{ab}$
2. **Non-degeneracy:** $\forall S \in \mathbb{G}_1$, $e(S, T) = 1$ for all $T \in \mathbb{G}_2$ iff $S = \mathcal{O}$
3. **Computability:** $\forall (S, T) \in \mathbb{G}_1 \times \mathbb{G}_2$, e(S, T) is efficiently computable
4. There exists an efficient, publicly computable (but not necessarily invertible) isomorphism $\psi: \mathbb{G}_2 \to \mathbb{G}_1$ such that $\psi(Q) = P$

Here we can use elliptic curve groups presented in [2], which allow both an efficient pairing and an efficient computable isomorphism.

As in [1], security of our scheme depend on the q-BDHIP assumption [1] defined below:

Let us consider bilinear map group $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ and generator P and Q of group $\mathbb{G}_1$ and $\mathbb{G}_2$.

The **q-Diffie-Hellman inversion problem** (q-DHIP) in $(\mathbb{G}_1, \mathbb{G}_2)$ consists in, given a (q+2)-tuple $(P, Q, \alpha Q, \alpha^2 Q, ..., \alpha^q Q)$, finding $\frac{1}{\alpha} P$.

The **q-Bilinear Diffie-Hellman inversion problem** (q-BDHIP) in $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ consists in, given a (q+2)-tuple $(P, Q, \alpha Q, \alpha^2 Q, ..., \alpha^q Q)$, computing $e(P, Q)^{1/\alpha} \in \mathbb{G}_T$.

Barreto et al signcryption scheme [1]:

Setup: given k, the PKG chooses bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ of prime order $p > 2^k$ and generator $Q \in \mathbb{G}_2$, $P = \psi(Q) \in \mathbb{G}_1$, $g = e(P, Q) \in \mathbb{G}_T$. It then chooses a master key $s \in_R \mathbb{Z}_p^*$, a system wide public key $Q_{pub} = sQ \in G_2$ and hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_p^*$, $H_2 : \{0,1\}^* \times G_T \to \mathbb{Z}_p^*$ and $H_3 : G_T \to \{0,1\}^n$. The public parameters are

$$\text{params} = \left\langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, Q_{pub}, e, \psi, H_1, H_2, H_3 \right\rangle$$

Extract: for an identity ID, the private key is $d_{ID} = \frac{1}{H_1(ID) + s} Q \in \mathbb{G}_2$

Sign/Encrypt: given a message $m \in \{0,1\}^*$, a receiver's identity ID_B and a sender's private key d_{ID_A}

1. Pick $x \in_R \mathbb{Z}_p^*$
2. Compute
   (i) $r = g^x$
   (ii) $c = m \oplus H_3(r)$
   (iii) $S = (x + h)\psi(d_{ID_A})$ where $h = H_2(m, r)$
   (iv) $T = x(H_1(ID_B)P + \psi(Q_{pub}))$

The ciphertext is $\sigma = (c, S, T)$

Decrypt/Verify: given $\sigma = (c, S, T)$ and some sender's identity ID_A

1. Compute
   (i) $r = e(T, d_{ID_B})$
   (ii) $m = c \oplus H_3(r)$
   (iii) $h = H_2(m, r)$
   (iv) $e(S, H_1(ID_A)Q + Q_{pub})g^{-h}$

Accept the message iff

$$r = e(S, H_1(ID_A)Q + Q_{pub})g^{-h}$$

5. Generalization of Barreto et al scheme:

Setup/Extract: Same as Barreto et al scheme [1] except some consideration

(i) Consider 0P= $\mathcal{O}_{\mathbb{G}_1}$ (additive identity of $\mathbb{G}_1$) and 0Q=$\mathcal{O}_{\mathbb{G}_2}$ (additive identity of $\mathbb{G}_2$)

(ii) For signature only mode (encryption only mode), receiver (sender) does not exist we use ID_ϕ as the identifier for the absence of the user.

(iii) Define a function such that

$$f(ID_U) = \begin{cases} 0, \text{ if } ID_U = ID_\phi \\ 1, \text{ if } ID_U \neq ID_\phi \end{cases}$$

(iv) Set $d_{ID_\phi} = \frac{1}{s} Q$

Now public parameters are params = $\left\langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, Q_{pub}, d_{ID_\phi}, e, \psi, H_1, H_2, H_3, f(ID_U) \right\rangle$

Signcryption mode:

Signcrypt: given a message $m \in \{0,1\}^*$, a receiver's identity ID_B and a sender's private key d_{ID_A}

1. Pick $x \in_R \mathbb{Z}_p^*$
2. Compute
   (i) $r = g^x$
   (ii) $c = m \oplus \{H_3(r)f(ID_B)\}$
   (iii) $S = (x+h)\psi(d_{ID_A})$ where $h = H_2(m,r)$
   (iv) $T = x(\{H_1(ID_B)f(ID_B)\}P + \psi(Q_{pub}))$

The ciphertext is $\sigma = (c, S, T, f(ID_A), f(ID_B))$

Unsigncrypt: given $\sigma = (c, S, T, f(ID_A), f(ID_B))$ and some sender's identity ID_A

1. Compute
   (i) $r = e(T, d_{ID_B})$
   (ii) $m = c \oplus \{H_3(r)f(ID_B)\}$
   (iii) $h = H_2(m,r)$
   (iv) $e(S, \{H_1(ID_A)f(ID_A)\}Q + Q_{pub})g^{-h}$

Accept σ iff

$$r = e(S, \{H_1(ID_A)f(ID_A)\}Q + Q_{pub})g^{-h}$$

Signature-only mode:

Sign: given a message $m \in \{0,1\}^*$, a sender's private key d_{ID_A}

1. Pick $x \in_R \mathbb{Z}_p^*$
2. Compute
   (i) $r = g^x$
   (ii) $c = m \oplus \{H_3(r)f(ID_\phi)\}$
   (iii) $S = (x+h)\psi(d_{ID_A})$ where $h = H_2(m,r)$
   (iv) $T = x(\{H_1(ID_\phi)f(ID_\phi)\}P + \psi(Q_{pub}))$

The signature is $\sigma = (m, S, T, f(ID_A), f(ID_\phi))$

Verify: given $\sigma = (c, S, T, f(ID_A), f(ID_\phi))$ and some sender's identity ID_A and d_{ID_ϕ}

1. Compute
   (i) $r = e(T, d_{ID_\phi})$
   (ii) $m = m \oplus \{H_3(r)f(ID_\phi)\}$
   (iii) $h = H_2(m,r)$
   (iv) $e(S, \{H_1(ID_A)f(ID_A)\}Q + Q_{pub})g^{-h}$

Accept σ iff

$$r = e(S, \{H_1(ID_A)f(ID_A)\}Q + Q_{pub})g^{-h}$$

Encryption-only mode:

Encrypt: given a message $m \in \{0,1\}^*$, a receiver's identity ID_B and d_{ID_ϕ}

1. Pick $x \in_R \mathbb{Z}_p^*$
2. Compute
   (i) $r = g^x$
   (ii) $c = m \oplus \{H_3(r)f(ID_B)\}$
   (iii) $S = (x+h)\psi(d_{ID_\phi})$ where $h = H_2(m,r)$
   (iv) $T = x(\{H_1(ID_B)f(ID_B)\}P + \psi(Q_{pub}))$

The ciphertext is $\sigma = (c, S, T, f(ID_\phi), f(ID_B))$

Decrypt: given $\sigma = (c, S, T, f(ID_\phi), f(ID_B))$ and some sender's identity ID_A

1. Computes
   (i) $r = e(T, d_{ID_B})$
   (ii) $m = c \oplus \{H_3(r)f(ID_B)\}$
   (iii) $h = H_2(m,r)$
   (iv) $e(S, \{H_1(ID_\phi)f(ID_\phi)\}Q + Q_{pub})g^{-h}$

Accept σ iff

$$r = e(S, \{H_1(ID_\phi)f(ID_\phi)\}Q + Q_{pub})g^{-h}$$

Remarks: Note that the proposed scheme is Barreto et al [1] signcryption scheme in signcryption mode. In the encryption-only mode where signer does not exist, the proposed scheme gives the ciphertext as the signcrypted text with sender ID_ϕ. The verification process of signature of ID_ϕ gives the CCA security in the encryption-only mode. In the signature-only mode where receiver does not exist, the proposed scheme gives signature on message m as the signcrypted text with receiver ID_ϕ.

Security Results:

We prove the security of proposed IDGSC scheme in signcryption mode. Since the definitions of ***IND-IDGSC-CCA2*** and ***EUF-IDGSC-CMA*** in signcryption mode consider the insider security, this makes the analysis of message confidentiality and signature non-repudiation in encryption-only mode and signature-only mode similar to signcryption mode. Thus we give the proof of these notions in signcryption mode. The proofs of the theorems are adapted from [1].

Theorem 1: Assume that an IND-IDGSC-CCA2 adversary $\mathcal{A}$ has an advantage ε against signcryption mode (encryption-only mode) of proposed scheme when running in time τ, asking q_{h_i}, queries to random oracle H_i (i = 1, 2, 3) and q_{se}, q_s, q_{dv}, q_d signcrypt, sign, unsigncrypt, decrypt queries respectively. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ with probability

$$\varepsilon' > \frac{\varepsilon}{(q_{h_1}-1)(2q_{h_2}+q_{h_3})}\left(1-(q_{se}+q_s)\frac{(q_{se}+q_s+q_{h_2})}{2^k}\right)\left(1-\frac{q_{dv}+q_d}{2^k}\right)$$

within a time $\tau' < \tau + O(q_{se}+q_s+q_{dv}+q_d)\tau_p + O(q_{h_1}^2)\tau_{multi} + O((q_{dv}+q_d)q_{h_2})\tau_{exp}$ where τ_{exp} is time complexity of exponentiation in $\mathbb{G}_T$, and τ_{multi} is the time complexity of multiplication in $\mathbb{G}_2$ and τ_p is the time complexity of a pairing computation.

Proof: See appendix.

Before giving the theorem for signature non-repudiation we give the two lemmas. The proof of lemma 1 is similar to the proof of lemma 1 [3].

Lemma 1: If there is a forger $\mathcal{F}_o$ for an adaptively chosen ciphertext (chosen message) and identity attack having advantage ε_0 against the proposed scheme in signcryption mode (signature-only mode) when running in time τ_0 and making q_1 queries to random oracle H_1, then there exists an algorithm $\mathcal{F}_1$ for an adaptively chosen ciphertext and given identity attack which has advantage $\varepsilon_1 \le \varepsilon_0(1-\frac{1}{2^k})\big/(q_{h_1}-1)$ with in a running time $\tau_1 \le \tau_0$. Moreover $\mathcal{F}_1$ asks the same number of key extraction, signcrypt, sign, unsigncrypt, decrypt, H_2 and H_3 queries as $\mathcal{F}_o$ does.

Lemma 2: Assume that there is an adaptively chosen ciphertext (chosen message) and given identity attacker $\mathcal{F}$ against signcryption mode (signature-only mode) of proposed scheme. When running in time τ, asking q_{h_i}, queries to random oracle H_i (i = 1, 2, 3) and q_{se}, q_s, q_{dv}, q_d signcrypt, sign, unsigncrypt, decrypt queries respectively, $\mathcal{F}$ produces a forgery with probability $\varepsilon \ge 10(q_{se}+q_s)(q_{se}+q_s+q_{h_2})\big/2^k$. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ in an expected time

$$\tau' \le 120686 q_{h_2}(\tau + O(q_{se}+q_s+q_{dv}+q_d)\tau_p + O((q_{dv}+q_d)q_{h_2})\tau_{exp})\big/\varepsilon(1-q/2^k) + O(q_{h_1}^2)\tau_{multi}$$

where τ_{multi}, τ_{exp} and τ_p are the same quantity as in theorem 1.

Proof: See appendix.

The combination of these two lemmas yields the following theorem.

Theorem 2: Assume that there exists an ESUF-IDGSC-CMA attacker $\mathcal{F}$ against signcryption mode (signature-only mode) of proposed scheme. When running in time τ, asking q_{h_i}, queries to random oracle H_i (i = 1, 2, 3) and q_{se}, q_s, q_{dv}, q_d signcrypt, sign, unsigncrypt, decrypt queries respectively, $\mathcal{F}$ produces a forgery with probability $\varepsilon \ge 10(q_{se}+q_s)(q_{se}+q_s+q_{h_2})/2^k$. Then there is an algorithm $\mathcal{B}$ to solve the q-BDHIP for $q = q_{h_1}$ in an expected time

$$\tau' \le 120686(q_{h_1}-1)q_{h_2}\frac{(\tau + O(q_{se}+q_s+q_{dv}+q_d)\tau_p + O((q_{dv}+q_d)q_{h_2})\tau_{exp})}{\varepsilon(1-1/2^k)(1-q/2^k)} + O(q_{h_1}^2)\tau_{multi}$$

where τ_{multi}, τ_{exp} and τ_p are the same quantity as in theorem 1.

6. Efficiency discussion: The proposed scheme in the signcryption mode is the scheme [1], which is most efficient signcryption scheme till the date. Hence our scheme is as efficient as [1] in the signcryption mode. Encryption-only mode and signature-only mode have an extra pairing calculation than encryption and signature. Now in table 1, we compare our scheme with the generalized signcryption scheme proposed in [7].

IDGSC	Signcrypt			Unsigncrypt		
	G_1 mls	G_2 exp	e cps	G_1 mls	G_2 exp	e cps
[7]	3	---	1	1	---	3
proposed scheme	2	1	---	---	1	2

Table 1

7. IDGSC in multiple PKGs environment (IDGSCMP):

The multiple PKGs environment is presented by Wang [11], where he gave an ID based encryption scheme which is more practical in multiple PKGs environment. Some ID based signcryption schemes in multiple PKGs environment have been proposed in literature [5, 6, 8]. In this section we propose identity based generalized signcryption scheme in multiple PKGs environment based on [5].

Global-Setup: given k, the globally trusted third party chooses bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ of prime order $p > 2^k$ generator $Q \in \mathbb{G}_2$, $P = \psi(Q) \in \mathbb{G}_1$, $g = e(P,Q) \in \mathbb{G}_T$ and hash functions $H_1 : \{0,1\}^* \to \mathbb{Z}_p^*$, $H_2 : \{0,1\}^* \times G_T \to \mathbb{Z}_p^*$ and $H_3 : G_T \to \{0,1\}^n$. Similar to the scheme proposed in section 5, Consider 0P= $\mathcal{O}_{\mathbb{G}_1}$ and 0Q=$\mathcal{O}_{\mathbb{G}_2}$. For signature only mode (encryption only mode), receiver (sender) does not exist we use ID_ϕ as the identifier for the absence of the user. It also sets the function

$$f(ID_U) = \begin{cases} 0, \text{ if } ID_U = ID_\phi \\ 1, \text{ if } ID_U \ne ID_\phi \end{cases}$$

The public parameters are

$$\text{params} = \langle \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, P, Q, g, e, \psi, H_1, H_2, H_3, f(ID_U) \rangle$$

Domain Setup: Using global public parameters, each domain PKG_i chooses $s_i \in_R \mathbb{Z}_p^*$ as the domain master private key and keeps it's secrete. It calculates $Q_{pub,i} = s_i Q$ and $d_{ID_{\phi,i}} = \frac{1}{s_i} Q$ as domain master public key and secrete value corresponding to ID_ϕ, it makes both public.

Extract: for an identity ID_U, the domain PKG_{i_U} computes the private key as

$$d_{ID_U} = \frac{1}{H_1(ID, Q_{pub,i_U}) + s_{i_U}} Q \in \mathbb{G}_2$$

Generalized Signcryption for multiple PKGs:

Signcrypt: given a message $m \in \{0,1\}^*$, a receiver's identity ID_B and a sender's private key d_{ID_A}

1. Pick $x \in_R \mathbb{Z}_p^*$
2. Compute

(i) $r = g^x$

(ii) $c = m \oplus \{H_3(r) f(ID_B)\}$

(iii) $S = (x + h)\psi(d_{ID_A})$ where $h = H_2(m, r)$

(iv) $T = x(\{H_1(ID_B, Q_{pub,i_B}) f(ID_B)\}P + \psi(Q_{pub,i_B}))$

The ciphertext is $\sigma = (c, S, T, f(ID_A), f(ID_B))$

Unsigncrypt: given $\sigma = (c, S, T, f(ID_A), f(ID_B))$ and some sender's identity ID_A

1. Computes

(i) $r = e(T, d_{ID_B})$

(ii) $m = c \oplus \{H_3(r) f(ID_B)\}$

(iii) $h = H_2(m, r)$

(iv) $e(S, \{H_1(ID_A, Q_{pub,i_A}) f(ID_A)\}Q + Q_{pub,i_A}) g^{-h}$

Accept σ iff

$r = e(S, \{H_1(ID_A, Q_{pub,i_A}) f(ID_A)\}Q + Q_{pub,i_A}) g^{-h}$

Conclusion: In this paper we proposed an efficient and provable secure ID based generalized signcryption scheme based on [1]. The proposed scheme has many advantages over the scheme given in [7]. It has CCA security in encryption-only mode. We extend the security notions of generalized signcryption as we consider separate definition for message confidentiality and signature unforgeability in encryption-only mode and signature-only mode. The security of our scheme rely on q-BDHIP. Further we proposed an ID based generalized signcryption scheme for multiple PKGs environment.

Reference:

1. P. S. L. M. Barreto, B. Libert, N. McCullagh and J. Quisquater, "Efficient and Provably-Secure Identity Based Signatures and Signcryption from Bilinear Maps", Advances in Cryptology Proceedings of ACRYPT'05, Vol. 3788 of LNCS, Springer-Verlag Berlin, pages 515–532, 2005.
2. P. S. L. M. Barreto and M. Naehrig, "Pairing friendly elliptic curves of prime order", Cryptology ePrint Archive, Report 2005/133, http:/eprint.iacr.org/, 2005
3. J.C. Cha and J.H. Cheon: An identity-based signature from Gap Diffie-Hellman groups. PKC-2003, LNCS # 2567, Springer-Verlag, 2003, 18-30.
4. Y. Han and X. Yang, "ECGSC: Elliptic curve based generalized signcryption scheme", Cryptology ePrint Archive, Report 2006/126, http:/eprint.iacr.org/, 2006.
5. Z. Jin, H. Zuo, H. Du and Q. Wen, An efficient and provably secure identity based signcryption scheme for multiple PKGs. Cryptology ePrint Archive, Report 2008/195, http://eprint.iacr.org/ 2008/195.pdf, 2008.
6. S. Lal and P. Kushwah, "Multi-PKG ID Based Signcryption", Cryptology ePrint Archive, Report 2008/050, http://eprint.iacr.org/2008/050, 2008.
7. S. Lal and P. Kushwah, "ID based generalized signcryption", Cryptology ePrint Archive, Report 2008/84, http://eprint.iacr.org/ 2008/84.pdf, 2008.
8. F. Li, Y. Hu and C. Zhang, "An Identity-based Signcryption Scheme for Multi-domain Ad Hoc Networks", Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS 2007), Vol. 4521 of LNCS, Springer-Verlag, Berlin, pages 373–384, 2007.
9. J. Malone-Lee, "Identity based signcryption", Cryptology ePrint Archive, Report 2002/098, http:/eprint.iacr.org/, 2002.
10. D. Pointcheval and J. Stein, "Security arguments for digital signatures and blind signatures", Journal of Cryptology, Vol. 13, No. 3, Springer-Verlag, Berlin, pages 361–396, 2000.
11. S. Wang and Z. Cao: Practical identity-based encryption (IBE) in multiple PKG environment and its applications, http://eprint.iacr.org/2007/100.pdf, 2007.
12. X. Wang, Y. Yang and Y. Han "Provable secure generalized signcryption", Cryptology ePrint Archive, Report 2007/173, http:/eprint.iacr.org/, 2007.
13. Y. Zheng, "Digital signcryption or How to Achieve cost (Signature & Encryption) << cost (Signature) + cost (Encryption)", CRYPTO'97, LNCS # 1294, Springer-Verlag, 165-179, 1997.

Appendix:

Proof of Theorem 1: We will show how an IND-IDGSC-CCA2 adversary $\mathcal{A}$ of IDGSC may be used to constructs a simulator $\mathcal{B}$ that extract $e(P,Q)^{1/\alpha}$ on input $(P,Q,\alpha Q,\alpha^2 Q,...,\alpha^q Q)$.

We proceed similarly as in [1]. In the preparation phase $\mathcal{B}$ builds generator $G_2 \in \mathbb{G}_2$, $G_1 = \psi(G_2) \in \mathbb{G}_1$, a domain wide public key $Q_{pub} = xG_2 \in \mathbb{G}_2$ and a domain wide private key ID_ϕ i.e. $d_{ID_\phi} = \frac{1}{x}G_2 \in \mathbb{G}_2$ (for some unknown element $x \in \mathbb{Z}_p^*$) such that it knows q-1 pairs $\left(I_i, \frac{1}{I_i+x}G_2\right)$ for $I_1, I_2, ..., I_{\ell-1}, I_{\ell+1}, ..., I_{q-1} \in_R \mathbb{Z}_p^*$ (including $\frac{1}{x}G_2$). To do so,

1. $\mathcal{B}$ selects $\ell \in_R \{1,...,q_{h_1}\}$, elements $I_\ell \in_R \mathbb{Z}_p^*$, $\omega_2, ..., \omega_{\ell-1}, \omega_{\ell+1}, ..., \omega_q \in_R \mathbb{Z}_p^*$ and sets $\omega_1 = I_\ell$. Expands the polynomial $f(z) = \prod_{i=1, i\neq\ell}^{q}(z+\omega_i)$ to obtained the coefficients $c_0, ..., c_{q-1} \in \mathbb{Z}_p^*$ such that $f(z) = \sum_{i=0}^{q-1} c_i z^i$. For $i = 1, ..., \ell-1, \ell+1, ..., q$ it also compute $I_i = I_\ell - \omega_i \in \mathbb{Z}_p^*$ (observe that $I_1 = 0$).

2. It sets $G_2 = \sum_{i=0}^{q-1} c_i(\alpha^i Q) = f(\alpha)Q$ as public generator of $\mathbb{G}_2$ and $G_1 = \psi(G_2) = f(\alpha)P$ as a generator of $\mathbb{G}_1$. Another group element $U \in \mathbb{G}_2$ is then set to $U = \sum_{i=1}^{q} c_{i-1}(\alpha^i Q)$. We note that $U = \alpha G_2$ although $\mathcal{B}$ does not know α.

3. For $i = 1, ..., \ell-1, \ell+1, ..., q$, $\mathcal{B}$ expands $f_i(z) = f(z)/(z+\omega_i) = \sum_{i=0}^{q-2} d_i z^i$ that satisfy

$$\frac{1}{\alpha+\omega_i}G_2 = \frac{f(\alpha)}{\alpha+\omega_i}Q = f_i(\alpha)Q = \sum_{i=0}^{q-2} d_i(\alpha^i Q)$$

Thus $\mathcal{B}$ can compute q-1 = $q_{h_1} - 1$ pairs $\left(\omega_i, S_i = \frac{1}{\alpha+\omega_i}G_2\right)$ by the last term of above equation.

The system wide public key Q_{pub} is chosen as $Q_{pub} = -U - I_\ell G_2 = (-\alpha - I_\ell)G_2$ so that its (unknown) private key is $x = -\alpha - I_\ell \in \mathbb{Z}_p^*$. For all $i = 1, ..., \ell-1, \ell+1, ..., q$, we have $(I_i, -S_i) = (I_i, (1/(I_i + x))G_2)$. Observe that private key (d_{ID_ϕ}) for ID_ϕ corresponds to I_1.

Now simulator $\mathcal{B}$ then runs the algorithm $\mathcal{A}$ with input $(G_1, G_2, Q_{pub}, d_{ID_\phi})$. $\mathcal{A}$ probes the simulator $\mathcal{B}$ throughout the simulation and it is assumed that H_1 queries are distinct, the target identity ID_R^* is submitted to H_1 at some point and any query involving the identity ID comes after a H_1 query on ID. To maintain consistency in queries $\mathcal{B}$ makes the lists L_i for random oracle H_i for i = 1, 2, 3. $\mathcal{B}$ initialize a counter ν to 2 and starts answering $\mathcal{A}$'s queries.

- Simulator $H_1(ID_\nu)$: $\mathcal{B}$ answer I_ν and increment ν.

- Simulator $H_2(m,r)$: If $((m,r),h_2) \in L_2$ for some h_2, $\mathcal{B}$ returns h_2. Otherwise a random $h_2 \in_R \mathbb{Z}_p^*$ is returns. $\mathcal{B}$ additionally simulates random oracle H_3 on its own to obtain $H_3(r) \in \{0,1\}^n$ and stores the information $(m, r, h_2, c = m \oplus h_3, \gamma = r(G_1, G_2)^{h_2})$ in L_2 list. We will see how $\mathcal{B}$ use this information to answer unsigncrypt and decrypt oracles.

- Simulator $H_3(r)$: If $(r, h_3) \in L_3$ for some h_3, $\mathcal{B}$ returns h_3. Otherwise $\mathcal{B}$ chooses a h_3 uniformly at random form $\{0,1\}^n$ and stores (r, h_3) in the L_3 list.

- **Simulator Extract ($\mathbf{ID_\nu}$):** If $\nu = \ell$ then $\mathcal{B}$ fails. Otherwise, it knows that $H_1(ID_\nu) = I_\nu$ and returns $-S_\nu = (1/(I_\nu + x))G_2 \in \mathbb{G}_2$.

- **Simulator Signcrypt $(\mathbf{m, ID_S, ID_R})$:** Let $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ for $\mu, \nu \in \{2, ..., q_{h_1}\}$. If $ID_\mu \neq ID_\ell$, then $\mathcal{B}$ knows the sender's private key $d_{ID_\mu} = -S_\mu$ and can answer the query according to the specification of Signcrypt of signcryption mode. We thus assume $ID_\mu = ID_\ell$ and hence $ID_\nu \neq ID_\ell$ by the irreflexivity assumption. Also $ID_\mu \neq ID_\phi \neq ID_\nu$ (by the definition of signcryption mode). In this case $\mathcal{B}$ knows the receiver's private key $d_{ID_\nu} = -S_\nu$ by construction. To find a triple (S, T, h)$\in \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{Z}_p^*$ for which

$$e(T, d_{ID_\nu}) = e(S, Q_{ID_\ell})e(G_1, G_2)^{-h} \tag{1}$$

where $Q_{ID_\ell} = I_\ell G_2 + Q_{pub}$ holds, $\mathcal{B}$ randomly chooses $t, h \in_R \mathbb{Z}_p^*$ and computes $S = t\psi(d_{ID_\nu}) = -t\psi(S_\nu)$, $T = t\psi(Q_{ID_\ell}) - h\psi(Q_{ID_\nu})$ where $Q_{ID_\nu} = I_\nu G_2 + Q_{pub}$ such that $r = e(T, d_{ID_\nu}) = e(S, Q_{ID_\ell})e(G_1, G_2)^{-h} = e(\psi(d_{ID_\nu}), Q_{ID_\ell})^t e(G_1, G_2)^{-h}$. $\mathcal{B}$ stores the value of $H_2(m, r)$ to h in L_2 list ($\mathcal{B}$ fails if H_2 is already defined but this only happens with probability $((q_{se} + q_s + q_{h_2})/2^k)$. The ciphertext $\sigma = \langle m \oplus H_3(r), S, T \rangle$ is returned.

- **Simulator Sign $(\mathbf{m, ID_S})$:** Analysis of sign simulator is similar to signcrypt simulator with replacing ID_ν by ID_ϕ.

- **Simulator Unsigncrypt $(\boldsymbol{\sigma} = \mathbf{(c, S, T), ID_R, ID_S})$:** Let $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ for $\mu, \nu \in \{2, ..., q_{h_1}\}$. If $ID_\nu \neq ID_\ell$, then $\mathcal{B}$ knows the receiver's private key $d_{ID_\nu} = -S_\nu$ and can answer the query according to the specification of unsigncrypt of signcryption mode. We thus assume $ID_\nu = ID_\ell$ and hence $ID_\mu \neq ID_\ell$ by the irreflexivity assumption. Also $ID_\mu \neq ID_\phi \neq ID_\nu$ (by the definition of signcryption mode). In this case $\mathcal{B}$ knows the receiver's private key $d_{ID_\mu} = -S_\mu$ and also knows that, for all valid cipher texts, $\log_{d_{ID_\mu}}(\psi^{-1}(S) - hd_{ID_\mu}) = \log_{\psi(Q_{ID_\nu})}(T)$, where $h = H_2(m, r)$ is the hash value obtained in the L_2 list and $Q_{ID_\nu} = I_\nu G_2 + Q_{pub}$. Hence we have the relation

$$e(T, d_{ID_\mu}) = e(\psi(Q_{ID_\nu}), \psi^{-1}(S) - hd_{ID_\mu}) \tag{2}$$

or
$$e(T, d_{ID_\mu}) = e(\psi(Q_{ID_\nu}), \psi^{-1}(S))e(\psi(Q_{ID_\nu}), d_{ID_\mu})^{-h}$$

observe that the latter equality can be tested without inverting ψ as $e(\psi(Q_{ID_\nu}), \psi^{-1}(S)) = e(S, Q_{ID_\nu})$. Thus the query is handled by computing $\gamma = e(S, Q_{ID_\mu})$, where $Q_{ID_\mu} = I_\mu G_2 + Q_{pub}$ and searching through the list L_2 for entries of the form $(m_i, r_i, h_{2,i}, c, \gamma)$ indexed by $i \in \{1, ..., q_{h_2}\}$. If none is found, σ is rejected. Otherwise each one of them is further examined; for the corresponding indexes, $\mathcal{B}$ checks if

$$e(T, d_{ID_\mu})/e(S, Q_{ID_\nu}) = e(\psi(Q_{ID_\nu}), d_{ID_\mu})^{-h_{2,i}} \tag{3}$$

(the pairings are computed only once and at most q_{h_2} exponentiations are needed), meaning that (2) is satisfied. If the unique $i \in \{1, ..., q_{h_2}\}$ satisfying (3) is detected, the matching pair $(m_i, < h_{2,i}, S >)$ is returned. Otherwise σ is rejected. Overall an inappropriate rejection occurs with probability smaller than $q_{dv}/2^k$ across the whole game.

- Simulator decrypt ($\sigma = (c,S,T), ID_R$): Analysis of decrypt simulator is similar to unsigncrypt simulator with replacing ID_μ by ID_ϕ. Here an appropriate rejection occurs with probability smaller than $q_d/2^k$ across the whole game.

At the challenge phase, $\mathcal{A}$ outputs messages (m_0, m_1) and identities (ID_S, ID_R) for which she never obtained ID_R's private key. If $ID_R \neq ID_\ell$, $\mathcal{B}$ aborts. Otherwise it picks $\xi \in_R \mathbb{Z}_p^*, c \in_R \{0,1\}^n$ and $S \in_R \mathbb{G}_1$ to return the challenge $\sigma^* =< c, S, T >$ where $T = -\xi G_1 \in \mathbb{G}_1$. If we define $\rho = \xi/\alpha$ and since $x = -\alpha - I_\ell$, we can check that

$$T = -\xi G_1 = -\alpha\rho G_1 = (I_\ell + x)\rho G_1 = \rho I_\ell G_1 + \rho\psi(Q_{pub})$$

$\mathcal{A}$ cannot recognize that σ^* is not a proper ciphertext unless she queries H_2 or H_3 on $e(G_1, G_2)^\rho$. Along the guess stage, her view is simulated as before and her eventual output is ignored. A successful $\mathcal{A}$ is very likely to query H_2 or H_3 on the input $e(G_1, G_2)^\rho$ if the simulator is indistinguishable from real attack environment.

To produce a result $\mathcal{B}$ fetches a random entry (m, r, h_2, c, γ) or $\langle \gamma, \cdot \rangle$ from the list of L_2 or L_3 with probability $1/(2q_{h_2} + q_{h_3})$ (as L_3 contains more than $q_{h_2} + q_{h_3}$ records by construction), the chosen entry contains the right element $\gamma = e(G_1, G_2)^\rho = e(P, Q)^{f(\alpha)^2 \xi/\alpha}$, where $f(z) = \sum_{i=0}^{q-1} c_i z^i$ is the polynomial for which $G_2 = f(\alpha)Q$. The q-BDHIP solution can be extracted by noting that, if $\gamma^* = e(P, Q)^{1/\alpha}$, then

$$e(G_1, G_2)^{1/\alpha} = \gamma^{*(c_0^2)} e\left(\sum_{i=0}^{q-2} c_{i+1}(\alpha^i P), c_0 Q\right) e\left(G_1, \sum_{j=0}^{q-2} c_{j+1}(\alpha^j Q)\right)$$

In an analysis of $\mathcal{B}$'s advantage, we note that it only fails in providing a consistent simulation because one of the following independent events:

E_1: $\mathcal{A}$ does not choose to be challenged on ID_ℓ

E_2: a key extraction query is made on ID_ℓ

E_3: $\mathcal{B}$ aborts in a signcrypt or sign query because of collision on H_2

E_4: $\mathcal{B}$ rejects valid ciphertext in unsigncrypt or decrypt query at some point of the game.

We clearly have $\Pr[\neg E_1] = 1/(q_{h_1} - 1)$ and we know that $\neg E_1$ implies $\neg E_2$. We already observe that $\Pr[E_3] \leq (q_{se} + q_s)(q_{se} + q_s + q_{h_2})/2^k$ and $\Pr[E_4] \leq (q_{dv} + q_d)/2^k$. We thus find

$$\Pr[\neg E_1 \wedge \neg E_3 \wedge \neg E_4] \geq \frac{1}{q_{h_1} - 1}\left(1 - (q_{se} + q_s)\frac{(q_{se} + q_s + q_{h_2})}{2^k}\right)\left(1 - \frac{q_{dv} + q_d}{2^k}\right)$$

We obtained the announced bound by noting that $\mathcal{B}$ selects the correct element from L_2 or L_3 with probability $1/(2q_{h_2} + q_{h_3})$. Its workload is dominated by $O(q_{h_1}^2)$ multiplication in the preparation phase, $O(q_{se} + q_s + q_{dv} + q_d)$ pairing evaluation and $O((q_{dv} + q_d)q_{h_2})$ exponentiation in $\mathbb{G}_T$ in its simulation of the signcrypt, sign, unsigncrypt, decrypt oracles.

Proof of Lemma 2: we are going to use the "forking lemma" technique of Pointcheval and Stern [10] to prove our result. We will infect reduce the q-DHIP in bilinear groups $(\mathbb{G}_1, \mathbb{G}_2)$ 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-IDGSC-CMA adversary $\mathcal{A}$ of IDGSC may be used to construct a simulator $\mathcal{B}$ that solves q-DHIP. Let $(P, Q, \alpha Q, \alpha^2 Q, ..., \alpha^q Q)$ be the instant of the q-DHIP that we wish to solve.

In the preparation phase, $\mathcal{B}$ set up similarly as in theorem 1. The simulator $\mathcal{B}$ is then ready answer $\mathcal{A}$'s queries throughout the simulation. To maintain consistency in queries $\mathcal{B}$ makes the lists L_i for random oracle H_i for i = 1, 2, 3. It first initializes a counter ν to and runs $\mathcal{A}$ on input $(G_1, G_2, Q_{pub}, d_{ID_\phi}, ID_\ell)$ for a randomly chosen challenge identity $ID_\ell \in_R \{0,1\}^*$. Also queries to the H_1, H_2, H_3, signcrypt, sign, unsigncrypt and decrypt oracles are answered as in the proof of theorem 1.

This explain how $\mathcal{B}$ simulate $\mathcal{A}$'s environment in a chosen message and given identity attack. Let us assume that the attacker $\mathcal{A}$ forges a ciphertext $< c, S, T >$ for a recipient's identity ID_R in a time τ with probability $\varepsilon \geq 10(q_{se} + q_s)(q_{se} + q_s + q_{h_2})/2^k$ when making q_{se} signcrypt query, q_s sign queries, q_{h_2} random oracle queries on H_2. By the irreflexivity assumption, $ID_R \neq ID_\ell$, it makes possible to extract clear message signature pairs from ciphertext produce by the forger. Let the output of unsigncryption of $< c, S, T >$ is $< m, r, h_1, S_1 >$. Note that $\mathcal{A}$ does not know the private key corresponding to ID_ℓ. Then by forking lemma there exist a turning machine $\mathcal{A}'$ that runs $\mathcal{A}$ sufficient number of times on the input $(G_1, G_2, Q_{pub}, d_{ID_\phi}, ID_\ell)$ to obtain two suitable related forgeries which give $< m, r, h_1, S_1 >$, $< m, r, h_2, S_2 >$ with $h_1 \neq h_2$, in the expected time $\tau' \leq 120686 q_{h_2} \tau/\varepsilon$.

The reduction then works as follows. The simulator $\mathcal{B}$ runs $\mathcal{A}'$ to obtain two forgeries $< m^*, r, h_1, S_1 >$ and $< m^*, r, h_2, S_2 >$ for the same message m^* and commitment r with $h_1 \neq h_2$. Both forgeries satisfy the verification equation, this gives

$$e(G_1, G_2)^{-h_1} = e(S_2, Q_{ID_\ell}) e(G_1, G_2)^{-h_2}$$

with $Q_{ID_\ell} = (I_\ell + x)G_2 = -\alpha G_2$. Then its gives $e((h_1 - h_2)^{-1}(S_1 - S_2), Q_{ID_\ell}) = e(G_1, G_2)$ and hence

$$T^* = (h_1 - h_2)^{-1}(S_1 - S_2) = \frac{1}{\alpha} G_1$$

From T^*, $\mathcal{B}$ can extract $\sigma^* = \frac{1}{\alpha} P$; it knows that $f(z)/z = c_0/z + \sum_{i=0}^{q-2} c_i z^i$ and eventually computes

$$\sigma^* = \frac{1}{c_0}\left[T^* - \sum_{i=0}^{q-2} c_i \psi(\alpha^i Q)\right] = \frac{1}{\alpha} P$$

which is returned as a result.

It finally comes that, if $\mathcal{A}$ makes a forgery in time τ with probability $\varepsilon \geq 10(q_{se} + q_s)(q_{se} + q_s + q_{h_2})/2^k$ then $\mathcal{B}$ solves the q-DHIP in expected time

$$\tau' \leq 120686 q_{h_2} (\tau + O(q_{se} + q_s + q_{dv} + q_d)\tau_p + O((q_{dv} + q_d) q_{h_2})\tau_{exp}) / \varepsilon(1 - q/2^k) + O(q_{h_1}^2)\tau_{multi}.$$