An Identity based Multi-receiver Generalized Signcryption Scheme

Tej Singh[1,*], Rashid Ali[2]

[1] Department of Mathematics, IMS Engineering College,
Ghaziabad, Uttar Pradesh 201009, India

[2] Department of Mathematics, Krishna Engineering College
Ghaziabad, Uttar Pradesh 201001, India

[*]*Corresponding author's email: tejsingh2009 [AT] gmail.com*

ABSTRACT— Generalized signcryption can adaptively work as a signcryption scheme, a signature scheme or an encryption scheme jointly with only one algorithm. It is very suitable for the storage constrained environments, like smart card, the embedded system and wireless sensor networks. In this paper, we proposed an identity based multi –receiver generalized signcryption. We also prove the security of the proposed scheme in the simplified modal under the q-DHIP and q-BDHIP.

Keywords— Multi- receiver generalized signcryption, generalized signcryption, identity based cryptography, provable security.

1. INTRODUCTION

Zheng [1] introduced the concept of signcryption in 1997. Signcryption can realize signature and encryption simultaneously with lower computational costs and communication overheads than the traditional sign-then-encrypt approach. Since then, many public key signcryption schemes have been proposed [2-4].

Identity based cryptography first introduced, in 1984 by Shamir [5]. In this system, public keys of user's can be calculated from their identities information such as name, email addresses, or IP addresses. Private keys of users generated by a trusted third party, called a private key generator (PKG). The first identity based signature scheme was introduced by Shamir [5] in 1984. Bonech and Franklin [6] first introduce identity based encryption scheme in 2001. In 2002 Malone Lee [7] proposed the first identity-based signcryption scheme and they also gave the security model. Many identity based signcryption schemes have been proposed after [7]. Some of them are [8-16].

The concept of generalized signcryption scheme proposed by Han et al. [17]; which can work as an encryption scheme or a signature scheme or a signcryption scheme as per need. Wang et al. [18] gave the first security model and revised Han et al. [17]; scheme. In 2008, Lal et al. [18] proposed the first identity based generalized signcryption scheme along with security model. In 2010,Yu et al. [19] pointed out Lal et al. [18] security model is not complete, then they modified the security model. Later, Kushwah et al. [20] simplified Yu et al. [19] security model and gave another efficient identity based generalized signcryption scheme. Since then many identity based generalized signcryption scheme have been proposed [21, 22, 23, 24].

All of the schemes [17-24] are suitable for one receiver scenario. Han [25] first proposed multi-receiver GSC scheme, but this scheme is a trivial n-receiver scheme that runs generalized signcryption repeatedly n times. Han [26] proposed a multi- receiver generalized signcryption scheme in 2009. In 2012, Zhou [27] proposed Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme. In 2014, Zhou [28] proposed identity based multi-receiver GSC scheme. In 2015, Cai-Xue Zhou [29] proposed an improved multi-receiver generalized signcryption scheme based on CDH problem. In 2015, Mishra [30] pointed out that Han et al.'s [26] multi-receiver GSC scheme is not IND-CCA2 secure in the pure encryption mode and hybrid encryption mode and proposed a study on improvement of multi-receiver generalized signcryption scheme.

In this paper, we proposed an identity based multi-receiver generalized signcryption scheme. Using the Kushwah et al. [26] scheme we also prove the security of the scheme in the simplified model under the hardness of q-DHIP and q-BDHIP. The Rest of the paper is organized as follows. In section 2, we define some preliminaries related to this paper. Section 3 presents formal model of identity based multi-receiver generalized signcryption schemes and security model. In

section 4, we give the proposed IBMGSC scheme. Section 5 analyzes the security of proposed scheme. Finally, conclusions are present in section 6.

2. PRELIMINARIES

Definition 1. (Bilinear Pairing). Let G_1 and G_2 be two multiplicative cyclic groups of prime order q. A bilinear map $e: G_1 \times G_1 \to G_2$ satisfies the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1,\ a, b \in Z_q$.
2. Non-degeneracy: There exists $P, Q \in G_1$, such that $e(P, Q) \neq 1$.
3. Computability: There exits an efficient algorithm to compute $e(P, Q)$, for all $P, Q \in G_1$.

Definition2. q-Diffie –Hellman inversion problem. Given $(q+1)$ tuple $(P, aP, a^2P, \ldots\ldots\ldots, a^qP)$ to compute $\frac{1}{a}P$ is known as q-DHIP.

Definition3. q-Bilinear Diffie –Hellman inversion problem. Given $(q+1)$ tuple $(P, aP, a^2P, \ldots\ldots, a^qP)$ to compute $\frac{1}{a}P$ is known as q-DHIP.

3. FORMAL MODEL OF IDENTITY BASED MULTI-RECEIVER GENERALIZED SIGNCRYPTION (IBMGSC) SCHEMES

3.1. Generic Scheme

An identity based multi- receiver generalized signcryption scheme consists of the following four algorithms:

- Setup: Given a security parameter k, the private key generator (PKG) generates system parameters *params* and a master key *s*. *params* is made public while s is kept secret.
- Key generation: Given input *params*, master secret key and a user's identity $P, Q \in G_1$, it outputs a partial private key D_U corresponding to ID_U.
- IBMGSC: To send a message $m_i\ (i = 1, \ldots n)$ from a sender S to receivers $R_i\ (i = 1, \ldots n)$, this algorithm takes input $(D_S, m_i, ID_S, ID_{R_i})$ and out puts ciphertext $\sigma = IBMGSC(D_S, m_i, ID_S, ID_{R_i})$.
- IBMGUSC: This algorithm takes the input $(\sigma, D_{R_i}, ID_S, ID_{R_i})$ and outputs m_i and valid if σ is a valid multi-receiver generalized signcryption of m_i done by sender S to receivers $R_i\ (i = 1, \ldots n)$, otherwise $\perp$ if σ is not valid.

There is no specific sender (or receivers) when we only encrypt (or sign) a message using IBMGSC. We denote the absence of sender (or receivers') by ID_φ.To only sign or encrypt a message m_i, use $ID_{R_i} = ID_\varphi$ or $ID_S = ID_\varphi$ respectively. Therefore, when $ID_{R_i} = ID_\varphi$, IBMGSC becomes a signature scheme and output of IBMGSC algorithm is a signature of sender ID_S on the message m_i and when $ID_S = ID_\varphi$, IBMGSC becomes an encryption scheme and output of the IBMGSC algorithm is merely an encryption of message m_i for receiver ID_{R_i}. If $ID_{R_i} \neq ID_\varphi$ or $ID_S \neq ID_\varphi$, then IBGSC works as the signcryption scheme. Thus IBMGSC works in three modes via signcryption mode, encryption-only mode and signature-only mode.

3.2. Security Model

The security notions for signcryption scheme are indistinguishability against adaptive chosen ciphertext attack (IND-SC-CCA2) and existential unforgeability against adaptive chosen message attack (EUF-SC-CMA). WE modify these definitions to adapt for the multi-recevier GSC scheme. Namely, a multi-recevier GSC scheme should satisfy confidentiality (IND-MGSC-CCA2) and unforgeability (EUF-MGSC-CMA).

Definition 4. A multi-receiver GSC scheme is said to be IND-MGSC-CCA2 secure if no probabilistic polynomial time adversary has a non-negligible advantage in following game.

The challenger C runs Setup algorithm to generate the system public parameters and to generate multiple key pairs $(D^*_{U_i}, ID^*_{U_i})$ where $(i = 1,...n)$. $D^*_{U_i}$ is kept secret while $ID^*_{U_i}$ is given to adversary A. These key pairs are the challenge key pairs.

a. **Phase 1:** A makes polynomially bounded number of queries to the following oracles.

- **MGSC Oracle:** A produces message $M = \{m_i, i = 1,...n\}$ and n arbitrary public keys $ID^*_{U_i}$ and requires the result of the operation $\sigma = MGSC(D^*_{S_J}, M, ID_{R_i})$ for an attacked user's private key $D^*_{S_J}, (j = 1,...n)$. Challenger C runs MGSC algorithm and returns the output σ to A.
- **MGUSC Oracle:** A produces a ciphertext σ, an arbitrary public key ID_S of the sender and requires the result of MGUSC $(\sigma, D^*_{U_i}, ID_S)$ for the attacked user's private key $D^*_{U_J}, (j = 1,...n)$. C runs MGUSC algorithm and returns the output of MGUSC to A.

b. **Challenge:** A produces two message vectors $M^*_0 = \{m^*_{0i}, i = 1,...n\}$ and $M^*_1 = \{m^*_{1i}, i = 1,...n\}$, an arbitrary private key D^*_S, B flips a coin $b \in \{0, 1\}$ to compute a ciphertext $\sigma^* = MGSC(M^*_b, ID^*_{U_i}, D^*_S)$ under the attacked user's public keys $ID^*_{U_J}, (j = 1,...n)$. B return σ^* to a as a challenge.

c. **Phase 2**: A is allowed to make polynomially bounded number of new queries as in phase 1 with the restriction that A should not query the MGUSC $(\sigma^*, D^*_{U_i}, ID^*_S)$.

d. **Guess**: At the end of this game, A outputs a bit b'. A wins the game if $b = b'$ .A's advantage is defined as follows: $Adv_A^{IND-MGSC-CCA2} = 2\Pr[b = b'] - 1$.

Definition 5. A multi-receiver GSC scheme is said to be EUF-MGSC-CMA secure if no probabilistic polynomial time adversary has a non-negligible advantage in following game.

The challenger C runs Setup algorithm to generate the system public parameters and to generate multiple key pairs $(D^*_{U_i}, ID^*_{U_i})$, $(i = 1,...n)$. $D^*_{U_i}$ is kept secret while $ID^*_{U_i}$ is given to adversary A. The key pair cannot be null and is considered as the challenge key pair.

a. **Attack:** A can adaptively perform queries to the oracles as those defined in Definition 4.

b. **Forgery:** At the end of the game, A produces a ciphertext σ^* and n arbitrary receiver's key pairs $(D^*_{R_i}, ID^*_{R_i}), (i = 1,...n)$. A wins the game if the result of MGUSC $(\sigma^*, D^*_{R_i}, ID^*_S)$ is a valid message m^*_i under the attacked users public key ID^*_S and the i-th receivers secret key $D^*_{R_i}$ and σ^* is not the output of $MGSC(D^*_{S_J}, M^*, ID_{R_i}), M^* = \{m^*_1, m^*_2, ...m^*_n\}$. A's advantage is its probability of victory.

4. PROPOSED IBMGSC SCHEME

In this section based on Kushwah et al. [26] scheme, we will propose an identity based multi-receiver generalized signcryption scheme.

Set up: Let k be a secure parameter, q be a k bit prime, the PKG chooses two solve G_1 and G_2 of same prime order q, a bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ and P is a generator of G_1.PKG computes $g = e(P, P)$ and defines $H_1 : \{0,1\}^{k_3} \to Z^*_q, H_2 : \{0,1\}^{n+k_2+2k_3} \to Z^*_q, H_3 : \{0,1\}^{n+k_2+k_1+2k_3} \to Z^*_q$ $H_4 : \{0,1\}^{k_2} \to \{0,1\}^{n+k_1+k_2+k_3}$,

where k_1, k_2 and k_3 denote the number of bits to represent elements of G_1, G_2 and identity respectively and n is the message bit length. Now PKG chooses $s \in_R Z_q^*$ as the master key and set $P_{Pub} = sP$ .Publishes the system parameters $\{G_1, G_2, q, n, P, P_{Pub}, \hat{e}, g, H_1, H_2, H_3, H_4\}$.In order to get adaptive outputs we define a function f such that $f(ID) = 0$ if $ID = ID_\phi$ else $f(ID) = 1$.

Keygen: For given ID, PKG computes user U private key $D_U = (Q_U + s)^{-1} P$, where $Q_U = H_1(ID_U)$ .For ID_ϕ, we set $D_\phi = o \in G$ is the zero element.

IBMGSC: To signcrypt message vector $M = \{m_i / m_i \in \{0,1\}^n, i = 1,2,...I\}$ to the intended receiver procedure.

1. Picks randomly $r \in_R Z_q^*$ and computes $b = g^r$
2. For i = 1,2.....l

a. Computes $r_i' = H_2(m_i, b, ID_s, ID_{R_i})$

b. $X_i = r_i' f(ID_{R_i}) T_{R_i}$

Where $T_{R_i} = H_1(ID_{R_i})P + P_{Pub}$, Note that $X_i = 0 \; if \;\; R_i = \phi$

c. $V_i = H_3(m_i, b, X_i, ID_S, ID_{R_i})$

d. $z_i = (r + V_i) D_S$

e. $y_i = m_i \parallel b \parallel z_i \parallel ID_S \oplus \{H_4(g^{r_i'}) f(ID_{R_i})\}$

3. Return $\sigma = (y_i, X_i)$

IBMGUSS: When receiving σ, the receiver R_i, gets his signcryption $\sigma_i = (y_i, X_i)$ and performs the following steps:

a. Recovers $m_i \parallel b \parallel z_i \parallel ID_S = y_i$ if $X_i = 0$ otherwise

b. Computes $w_i = e(X_i, D_{R_i})$ and recovers $m_i \parallel b \parallel z_i \parallel ID_S = y_i \oplus (H_4(w_i) f(ID_{R_i})$

c. If $z_i = 0$ computes $r_i' = H_2(m_i, b, ID_S, ID_{R_i})$ and accepts the message iff $X_i = r_i' f(ID_{R_i}) T_{R_i}$

Otherwise compute $V_i = H_3(m_i, b, X_i, ID_S, ID_{R_i})$ and accepts the message iff

$e(z_i, H_1(ID_S)P + P_{Pub}) g^{-v_i} = b$.

Consistency:

$$\begin{aligned} w_i &= e(X_i, D_{R_i}) = e(r_i' T_{R_i}, D_{S_i}) \\ &= e(r_i'(Q_{R_i} + s)P,\ (Q_{R_i} + s)^{-1} P) \\ &= e(P, P)^{r_i'} \\ &= g^{r_i'} \end{aligned}$$

$$\begin{aligned} & e(z_i, H_1(ID_S)P + P_{Pub}) g^{-v_i} \\ &= e((r + v_i) D_S,\ (Q_S + s)P)\, g^{-v_i} \\ &= e((r + v_i)\ (Q_s + s)^{-1} P,\ (Q_s + s)P)\, g^{-v_i} \end{aligned}$$

$$= e((P,\ P)^{(r+v_i)}\ g^{-v_i}$$
$$= g^{(r+v_i)}\ g^{-v_i}$$
$$= g^{r}$$
$$= b$$

5. SECURITY ANALYSIS

Theorem 1 (Message Confidentiality). In the random oracle model with secure parameter k, if an adversary A has non-negligible advantage ε against the IND-MGSC-CCA2 security of the multi-receiver GSC scheme running in time t and performs q_e, q_u IBMGSC queries, IBMGUSC queries respectively to oracles $H_i\ (i=1,2,3,4)$, then there exists an algorithm B that solve the q-BDHIP problem for $q = q_{h_1}$, with probability

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

With a time $t' < t + O(q_e+q_u)t_p + O(q_{h_1}^2)t_{multi} + O(q_e)t_{\exp}$

Where $t_{\exp}$, t_{multi} and t_p are the time for an exponentiation in G_2, a multiplication in G_1 and for a pairing computation.

Proof. We show how adversary A used to build a simulator B that attempts to extract $e(P,P)^{\frac{1}{\alpha}}$ on input $(P,\alpha P,\alpha^2 P,...\alpha^q P)$.

Preparation phase: First B selects $l \in \{1,.....,q_{h_1}\}$, elements $\lambda_l \in_R Z_q^*$,

$\chi_1,\chi_2,.....\chi_{l-1},\chi_{l+1},....,\chi_q \in_R Z_q^*$ and generate the polynomial $p(x)=\prod_{i=1,i\neq l}^{q}(x+\chi_i)$ to find the coefficient $\beta_1,\beta_2,.....,\beta_{q-1} \in_R Z_q^*$ such tha $p(x)=\sum_{i-0}^{q-1}\beta_i x^i$. B also computes $\lambda_i = \lambda_l - \chi_i \in Z_q^*$ for $i=1,.....l-1,l+1,...,q$. Now B sets $G=\sum_{i-0}^{q-1}\beta_i(\alpha_i P)=p(\alpha)P$ as a public generator of G_1 and computes random element $U \in G_1$ as $U=\sum_{i-0}^{q-1}\beta_{i-1}(\alpha^i P)=\alpha G$. Here we know that B have no information about a. After that B computes $p_i(x)=\frac{p(x)}{(x+\chi_i)}=\sum_{i=0}^{q-2}d_i x^i$ and for $i=1,.....l-1,l+1,...,q$

$$\frac{1}{(\alpha+\chi_i)}G=\frac{p(\alpha)}{(\alpha+\chi_i)}=p_i(\alpha)P=\sum_{i=0}^{q-2}d_i(\alpha^i P).$$

Thus B can compute $q-1=q_{h_1}-1$ pairs $(\chi_i, D_i=\frac{1}{\alpha+\chi_i}G)$ by the last term of the above equation. The system wide public key P_{pub} is chosen as $P_{pub}=-U-\lambda_l G=(-\alpha-\lambda_l)G$ with private key which is unknown $z=-\alpha-\lambda_l \in Z_q^*$. For all $i=1,.....l-1,l+1,...,q$, B have $(\lambda_i,-D_i)=(\lambda_i,\frac{1}{\lambda_i+z}G)$.

Now using input (G,P_{pub}), B starts the interaction with A. Here A asks the queries to B throughout the simulation.

Simulator: (H_1,H_2,H_3,H_4)

B maintains lists L_1,L_2,L_3,L_4 for the random oracles H_1,H_2,H_3,H_4. B initializes η $to1$ and starts answering A's queries as follows.

- H_1 Queries: It takes input ID. B answers λ_η to the η^{th} one such query and increment η. B sets the identity ID as ID_η.

- H_2 Queries: It takes input $(m_i, b, ID_\xi, ID_{\eta_i})$. B checks the list L_2 ,it returns a previous value if it exists. Otherwise it chooses a random $h_2 \in Z_q^*$ and returns this value as the answer. It also store this value in the list L_2 .
- H_3 Queries: It takes input $(m_i, b, X_i, ID_\xi, ID_{\eta_i})$. B checks the list L_3, it returns a previous value if it exists. Otherwise it chooses a random $h_3 \in Z_q^*$ and returns this value as the answer. It also stores this value in the list L_3 .
- H_4 Queries: It takes input $g^{r'}$. B checks the list L_4 , it returns a previous value if it exists. Otherwise it chooses a random $h_4 \in \{0,1\}^{n+k_1+k_2+k_3+k_4}$ and returns this value as the answer. It also stores this value in the list L_4 .

Keygen queries: It takes input an identity ID_{η_i} . B fails if $\eta_i = l$ otherwise it knows that $H_1(ID_{\eta_i}) = \lambda_{\eta_i}$ and returns $-D_{\eta_i} = \frac{1}{\lambda_{\eta_i} + z} G$.

IBMGSC queries: It takes input a plain text m_i and $(ID_s, ID_{R_i}) = (ID_\xi, ID_{\eta_i})$ where $\xi, \eta_i \in \{1,....,q_{h_i}\}$. If $\xi \neq l$, B knows the sender's private key of ID_ξ is $-D_\xi$ and can answer the query by following the specification of the IBMGSC algorithm. So we assume that $\xi = l$, then B does the following:

a. $V_i \in_R Z_q^*$ and $z_i \in_R G_1$

b. Compute $e(z_i, H_1(ID_l)G + P_{pub})e(G,G)^{-V_i} = b$

c. Simulates H_2 as $H_2(m_i, b, ID_l, ID_{\eta_i}) = r_i^{'}$ and store in the list L_2 .

d. Computes $X_i = r_i^{'} T_{\eta_i}$ where $T_{\eta_i} = H_1(ID_{\eta_i})G + P_{pub}$

e. Set $H_3(m_i, b, X_i, ID_l, ID_{\eta_i}) = V_i$ and store in L_3 list.

f. Simulate H_4 as $H_4(e(G,G)^{r_i^{'}}) = h_4$ and store in L_4 list.

g. Computes $y_i = m_i \| b \| z_i \| ID_l \oplus \{h_4 f(ID_{\eta_i})\}$

h. Returns $\sigma = (y_i, X_i)$

Note that if $ID_{\eta_i} = ID_\varphi$, B answer the IBMGSC query in same way using ID_φ in place of ID_{η_i} and return the signature $(m_i \| b \| z_i \| ID_l, o)$. Also B fails if H_3 is already defined but this happens with a probability smaller than $(q_e + q_{h_3}) / 2^k$.

IBMGUSC queries: It takes input a ciphertext (y_i, X_i) and a receivers identity ID_{η_i} . If $ID_{\eta_i} \neq ID_l$. Then B knows receivers private key of ID_{η_i} is $-D_{\eta_i}$, B runs the algorithm normally and returns the output to A. Also if $ID_{\eta_i} = ID_\varphi$ then B is able to given an appropriate answer to A. If $ID_{\eta_i} = ID_l$ then 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, A produce two message vectors $M_0 = \{m_{0i}, i = 1,.....,n\}$, $M_1 = \{m_{1i}, i = 1,.....,n\}$ and identity $(ID_S^*, ID_{R_i}^*)$ such that she has not made key gen queries on $ID_{R_i}^*$. Then Adversary A will choose $ID_S^* = ID_\varphi$. If $ID_{R_i}^* \neq ID_l$, B aborts the simulation. Otherwise it picks $\xi_i \in_R Z_q^*$, $y_i \in_R \{0,1\}^{n+k_1+k_2+k_3}$ to return the challenge $\sigma = (y_i, X_i)$ where $X_i = -\xi_i G \in G_1$ .If we define $\delta = \xi_i / \alpha$ and since $z = -\alpha - \lambda_l$, we can check that

$X_i = -\xi_i G = -\alpha \delta G = (\lambda_l + z)\delta G = \delta \lambda_l G + \delta P_{pub}$.

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.

To produce a result, 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 $\frac{1}{(q_{h_4}+q_e)}$, B chooses the record which will contain the right element $e(G,G)^{\delta}=e(P,P)^{p(\alpha)\xi_i/\alpha}$ where $G=p(\alpha)P$. The q-BDHIP solution can be extracted as follows. If

$$e(G,G)^{1/\alpha}=(\omega^*)^{\beta_0^2}\, e\left(\sum_{i=0}^{q-2}\beta_{i+1}(\alpha^i P),\beta_0 P\right).e\left(G,\sum_{j=0}^{q-2}\beta_{j+1}(\alpha^i P)\right)$$

In an analysis of B's advantage, following events will cause B to abort the simulation:

E_1 : A does not choose to be challenge on ID_l

E_2 : a keygen query is made on ID_l

E_3 : B aborts in the IBMGSC query because of a collision on H_3.

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

Also the probability that selects the correct record from the L_4 is $\frac{1}{(q_{h_4}+q_{h_3})}$. Therefore the advantage of B is

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

The time bound is obtained as there are $o(q_{h_1}^2)$ multiplication in the preparation phase, $o(q_e+q_u)$ pairing computations and $o(q_e)$ exponentiations in G_2.

Theorem 2 (Signature Unforgeability). Assume that there is an EUF-CMA adversary A against the proposed IBMGSC scheme. Also assume that A produce 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 IBMGUSC queries respectively, within the time t. Then there is an algorithm B to solve the q-BDHIP for $q=q_{h_1}$ in the expected time

$$t'\le 12068\, q_{h_1}\, q_{h_3}\,(t+o(q_e+q_u)t_p+o(q_u\, q_{h_3})t_{\exp})/\varepsilon(1-1/2^k)+o(q_{h_1}^2)t_{multi}$$

Where $t_{\exp}$, t_{multi} and t_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 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 IBMGSC queries, IDBMGUSC queries respectively. Then there exists an algorithm A' for adaptively chosen message and given identity attack, asking same number of queries as A and has the advantage $\varepsilon'>\frac{\varepsilon}{q_{h_1}}(1-\frac{q_u}{2^k})$.

Proof. The proof of Lemma 1 is similar to the proof of Lemma 1 in [31].

Lemma 2. Assume that there is chosen message and given identity attacker A against the proposed IBMGSC scheme. Let 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 IBMGSC queries, IDBMGUSC queries respectively within the time t. Then there is an algorithm B to solve q-BDHIP for $q = q_{h_1}$ in the expected time

$t' \le 12068\, q_{h_3}\,(t + o(q_e + q_u)t_p + o(q_e)t_{\exp})/\varepsilon + o(q_{h_1}^2)t_{multi}$

Where $t_{\exp}$, t_{multi} and t_p are the same as in Theorem 1.

Proof. We are going to use "forking lemma" technique of Pointcheval and Stern [32] to prove our result. In the preparation phase, B setup similarly as in Theorem 1. Then simulator B starts answering A's queries throughout the simulation. Also B makes the lists L_i for the random oracles H_i $(i=1,2,3,4)$ to maintain consistency. B initializes a counter η to run A on input (G, P_{pub}, ID_l) for a random chosen challenge identity $ID_l \in \{o,1\}^*$.

Also to simulate A's environment in a chosen message and given identity attack, B answers A's queries to the random oracles H_i $(i=1,2,3,4)$, IBMGSC and IBMGUSC in the proof of Theorem 1. Let us assume A forges a ciphertext (y_i, X_i) for a recipients identity ID_{R_i} (or a signature $(m_i \| b \| z_i \| ID_l, o)$ with recipient's identity ID_φ) in time t with probability $\varepsilon \ge 10(q_e+1)(q_e+q_{h_3})/2^k$ when making q_e IBMGSC queries and q_{h_3} random oracle queries on H_3. Also ID_{R_i} cannot be ID_l because of the irreflexivity assumption, so B an extract clean message signature pair from ciphertext. Therefore in both the case when $ID_{R_i} = ID_\varphi$ or $ID_{R_i} \ne ID_\varphi$, B has a message signature pair (m_i, b, V_i, Z_i, ID_l). Note that A does not know the private key corresponding to ID_l. Then by forking lemma there exists a turning machine A' that runs A sufficient number of times on input (G, P_{pub}, ID_l) to obtain two suitable related forgeries which gives (m_i, b, V_i, Z_i, ID_l) and $(m_i, b, V_i', Z_i', ID_l)$ with $V_i = V_i'$, in the expected time $t' \le 12068\, q_{h_3}\frac{t}{\varepsilon}$. To solve the q-DHIP simulator B runs A' to obtain two forgeries $(m_i^*, b, V_i, Z_i, ID_l)$ and $(m_i^*, b, V_i', Z_i', ID_l)$ with $V_i = V_i'$ for the same message m_i^* and commitment b .Since both forgeries satisfy the verification equation, we have $e(Z_i, T_{ID_l})\, e(G,G)^{-V_i} = e(Z_i', T_{ID_l})\, e(G,G)^{V_i'}$ Where $T_{ID_l} = (\lambda_l + z)G = -\alpha G$. Then it gives $e(Z_i - Z_i', T_{ID_l}) = e(G,G)^{V_i' - V_i'}$

$e((V_i - V_i')(Z_i - Z_i'), T_{ID_l}) = e(G,G)$ and hence $V_i^* = (V_i - V_i')(Z_i - Z_i') = \frac{1}{\alpha}G$.

From V_i^*, B can extract $\delta^* = \frac{1}{\alpha}P$ as it knows $p(x)/x = (\beta_0/x) + \sum_{i=0}^{q-2}\beta_i x^i$ and eventually computes $\delta^* = \frac{1}{\beta_0}\left[V_i^* - \sum_{i-0}^{q-2}\beta_i(\alpha^i P)\right] = \frac{1}{\alpha}P$ which is return as a result.

Thus if A makes a forgery in time t with probability $\varepsilon \ge 10(q_e+1)(q_e+q_{h_3})/2^k$, then B solve the q-DHIP in expected time $t' \le 12068\, q_{h_3}\,(t + o(q_e+q_u)t_p + o(q_e)t_{\exp})/\varepsilon + o(q_{h_1}^2)t_{multi}$.

6. CONCLUSION

In this paper, we proposed an identity based multi receiver generalized signcryption scheme. We also prove the security of the proposed scheme under the new security model based on q-DHIP and q-BDHIP. Also, proposed scheme is as efficient as the identity based generalized signcryption scheme by Kushwah et al. [26].

7. ACKNOWLEDGEMENT

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

8. REFERENCES

[1] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption). CRYPTO'97, LNCS #1924, Springer-Verlag, pp. 165-179, (1997).

[2] Y.Zheng; H.Imai, How to construct efficient signcryption schemes on elliptic curves. Inf. Process. Lett. 1998, 68, 227–233.

[3] F. Bao and R.H. Deng, A signcryption scheme with signature directly verifiable by public key. In Proceedings of the Public Key Cryptography-PKC'98, LNCS 1431, Yokohama, Japan, 5–6 February1998; pp. 55–59.

[4] J.Malone-Lee and W.Mao, Two birds one stone: Signcryption using RSA. In Proceedings of the Topics in Cryptology-CT-RSA'03, LNCS 2612, San Francisco, CA, USA, 13–17 April 2003; pp. 210–224.

[5] A. Shamir, Identity-based cryptosystems and signature schemes. In Proceedings of the Advances in Cryptology-CRYPTO'84, LNCS 196, Santa Barbara, CA, USA, 19–22 August 1984; pp. 47–53.

[6] D. Boneh and M. Franklin, Identity-based encryption from the weil pairing. In Proceedings of the Advances in Cryptology-CRYPTO'01, LNCS 2139, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.

[7] J. Malone-Lee, Identity Based Signcryption. Cryptology ePrint Archive,Report 2002/098, 2002. Available online: http://eprint.iacr.org/2002/098.

[8] B. Libert and J.J. Quisquator, A new identity based signcryption scheme from pairings. In Proceedings of the IEEE Information Theory Workshop-ITW'03, Paris, France, 31 March–4 April 2003; pp. 155–158.

[9] S.S.M. Chow, S.M. Yiu, L.C.K. Hui and K.P. Chow, Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In Proceedings of the Information Security and Cryptology-ICISC'03, LNCS 2971, Seoul, Korea, 27–28 November 2004; pp. 352–369.

[10] X. Boyen, Multipurpose identity based signcryption: A Swiss army knife for identity based cryptography. In Proceedings of the Advance in Cryptology-CRYPTO'03, LNCS 2729, Santa Barbara, CA, USA, 17–21 August 2003; pp. 383–399.

[11] L. Chen and J. Malone-Lee, Improved identity-based signcryption. In Proceedings of the Public Key Cryptography-PKC'05, LNCS 3386, Les Diablerets, Switzerland, 23–26 January 2005; pp. 362–379.

[12] 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. In Proceedings of the Advance in Cryptology-ASIACRYPT'05, LNCS 3788, Chennai, India, 4–8 December 2005; pp. 515–532.

[13] S.S.D. Selvi, S.S. Vivek, and C.P. Rangan, Identity based public verifiable signcryption scheme. In Proceedings of the ProvSec'10, LNCS 6402, Malacca, Malaysia, 13–15 October 2010; pp. 244–260. 15. Yu, Y.; Yang, B.; Sun, Y.; Zhu, S. Identity based signcryption scheme without random oracles. Comput. Stand. Interfaces 2009, 31, 56–62.

[14] Y. Yu, B. Yang, Y. Sun and S. Zhu, Identity based signcryption scheme without random oracles. Comput. Stand. Interfaces 2009, 31, 56–62.

[15] Z. Jin, Q. Wen and H. Du, An improved semantically-secure identity-based signcryption scheme in the standard model. Comput. Electr. Eng. 2010, 36, 545–552.

[16] F. Li, F. Muhaya, M. Zhang and T. Takagi, Efficient identity-based signcryption in the standard model. In Proceedings of the ProvSec'11, LNCS 6980, Xi'an, China, 16–18 October 2011; pp. 120–137.

[17] Y. Han, X. Yang, ECGSC: Elliptic Curve Based Generalized Signcryption Scheme. Cryptology ePrint Archive, Report 2006/126, 2006. Available online: http://eprint.iacr.org/2006/126.

[18] S. Lal and P. Kushwah, ID Based Generalized Signcryption. Cryptology ePrint Archive, Report 2008/084, 2008. Available online: http://eprint.iacr.org/2008/084.

[19] G. Yu, X. Ma, Y. Shen, and W. Han. Provable secure identity based genrealized signcryption schem. Theor. Comput. Sci. 2010, 411, 3614–3624.

[20] P. Kushwah, S. Lal, An efficient identity based generalized signcryption scheme. Theor. Comput. Sci. 2011, 412, 6382–6389.

[21] H. F. Ji, W. B. Han and L. D. Liu, Identity based generalized signcryption scheme for multiple pkgs in standard model. Journal of Electronics and Information Technology (in Chinese), vol. 33, no. 5, pp. 1204–1210, 2011.

[22] H. F. Ji, W. B. Han, and L. Zhao, Certificateless generalized signcryption. In Cryptology ePrint Archive, 2010. (http://eprint.iacr.org/2010/204)

[23] P. Kushwah and S. Lal, Provable secure certificateless generalized signcryption scheme. In International Journal of Computer Technology and Applications, vol. 3, no. 3, pp. 925–939, 2012.

[24] X. Shen, Y. Ming and J. Feng, Identity based generalized signcryption scheme in the standard model. In entropy 2017, 19,121; doi:10.3390/e19030121.

[25] Y.L. Han, Generalization of signcryption for resources-constrained environments. In wireless communication and mobile computing, vol 8, no. 7, pp. 919-931, 2009.

[26] Y. L. Han and X. L. Gui, Adaptive secure multicast in wireless network. In International Journal of Communication Systems, vol. 22, no. 9, pp. 1213– 1239, 2009.

[27] C. X. Zhou, Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme. Cryptology ePrint Archive, 2012 (eprint.iacr.org/2012/638.pdf)

[28] C. X. Zhou, Provably secure and efficient multi-receiver identity-based generalized signcryption scheme, in 2014 Ninth Asia Joint Conference on Information Security, pp. 82–89, 2014.

[29] C. X. Zhou, An improved multi-receiver generalized signcryption scheme. In International Journal of Network Security, pp. 340–350, May 2015.

[30] D.Mishra and S.Singh, A Study on Improvement of Multi-receiver Generalized Signcryption Scheme. In International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-11, November 2015.

[31] 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.

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