Improved Cryptanalysis of Provable Certificateless Generalized Signcryp- tion

Abdul Waheed1
School of Electrical and Computer Engineering
Seoul National University Korea Republic of
Department of Information Technology
Hazara University Mansehra, KP

Nizamud Din3
Department of Computer Science
University of Chitrak, KP

Arif Iqbal Umar5
Department of Information Technology
Hazara University Mansehra, KP

Jawaid Iqbal2
Department of Information Technology
Hazara University Mansehra, KP

Shahab Ul Islam4
Department of Computer Science
IQRRA National University

Noor Ul Amin6
Department of Telecommunication
Hazara University Mansehra, KP

Abstract—Certificateless generalized signcryption adaptively work as certificateless signcryption, signature or encryption scheme having single algorithm for suitable storage-constrained environments. Recently, Zhou et al. proposed a novel Certificates generalized scheme, and proved its ciphertext indistinguishability under adaptive chosen ciphertext attacks (IND-CCA2) using Gap Bi-linear Diffie-Hellman and Computational Diffie-Hellman assumption as well as proved existential unforgeability against chosen message attacks (EUF-CMA) using the Gap Bi-linear Diffie-Hellman and Computational Diffie-Hellman assumption in random oracle model. In this paper, we analyzed Zhou et al. scheme and unfortunately proved IND-CCA2 insecure in encryption and signcryption modes in defined security model. We also present a practical and improved scheme, provable secure in random oracle model.

Keywords—Digital signature; certificateless encryption; certificateless generalized signcryption; malicious-but-passive KGC; random oracle model

I. INTRODUCTION

Diffie-Hellman [2] introduced the concept of trapdoor one way function, while the concept of encryption and digital signature using public key approach were realized by Rivest, Shamir and Adleman [3], within Public Key Infrastructure (PKI). PKI has centralized and hierarchical infrastructure, consists of trusted third party provides solution for proving public keys authenticity. It most commonly use in scalable communication environment, but having limitations such as high cost, storage cost, difficult to verify, revoke of certificates and its distribution. To make certificate management more simple for public key in PKI Shamir [4] introduced notion of Identity Based Encryption (IBE), later on Boneh Franklin [5] realized in 2001 using Weil pairing. IBE has limitations having lacking of scalability and compromising Private Key Generator (PKG), which lead to compromise whole system and over authority of PKG. Riyan and Paterson [6] first time gave Certificateless Public Key Cryptography (CLPKC) concept, a more flexible infrastructure in-between PKI and IBE. The role of PKG split between user and Key Generation Center (KGC). User identity and associated public key used for composition of key pair. It does not require pricey infrastructure like PKI and cope the limitations of IBE. An alternative to sign-then-encrypt approach, Zheng [7] first proposed a novel and efficient crypto primitive named signcryption in PKI, while Barbosa and Farshim [8] first coined the concept of certificateless signcryption.

Signcryption is efficient when combined authenticity and confidentiality are required. However, in scenario where one or both of authenticity and confidentiality is required separately or simultaneously a signature or encryption or signcryption will be used, which is optimal in memory constrained environments like smart card, sensor networks, etc. This problem was addressed by Han [9] and proposed generalized signcryption (GSC) adaptively works as a signature (if authentication mandatory), encryption scheme (if confidentiality mandatory), or signcryption (if authentication+confidentiality mandatory) scheme within one algorithm. Kushwah and Lal [10] proposed ID Based generalized signcryption (GSC) scheme within a security model for the first time. Huifang et al. [11] first proposed certificateless generalized signcryption (CLGSC) scheme, and introduced CLGSC formal definition and security model. But Kushwah and Lal [12] proved scheme [11] Type I insecurity and introduced new efficient and secure CLGSC scheme. Ji et al. [13] introduced new CLGSC scheme based on [8], and later on [14] proved scheme [8] insecure against IND − CCA2 and EUF − CMA, and thus scheme [13] insecurity also proved indirectly. Au et al. [15] introduced Type − II adversary a novel approach known as “Malicious-but-Passive Key Generation Center” (MP − KGC). Hwang et al. [16] proposed certificateless scheme only for encryption purpose but Xiong et al. [17] proposed certificateless scheme for the purpose of only signature and Weng et al. [18] proposed certificateless signcryption scheme secured against MP − KGC. Zhou et al. [1] introduced a formal security model for new CLGSC (N − CLGSC) scheme and claimed its security against MP-KGC attacks.

In 2013 [19] the concept of heterogeneous signcryption firstly adopted which provided inter-operable environment for communications between sender and receiver and thus in 2016[20] Li et al. introduced heterogeneous signcryption two way communication for PKI and Identity Based Cryptography (IBC) environment but faced heavy cost in the form of pairing. After that IBC to Certificateless (CLC)
scheme also presented in 2017[21] and that same year Wang et al.[22] introduced ID based to PKI in standard model scheme. These above few heterogeneous schemes found in literature but the generalized form still missing.

We analyzed Zhou et al. [1] CLGSC scheme and unfortunately proved IND – CCA – II insecure in encryption and signcryption modes in their defined security model. We provided a fix to Zhou et al. N – CLGSC and proposed an improved N – CLGSC(IN – CLGLSC) scheme. The improved scheme is efficient and secure compare with Zhou et al. N – CLGSC and few others found in literature.

Remaining sections of this paper is organizes as: Section 2 gives preliminaries overview and security model. Section 3 present of Zhou et al. scheme review. Section 4 presents attacks on stated scheme. Section 5 presents attacks over improved scheme. Security and cost analysis are presented in Section 6 and at the end Section 7 conclude paper.

II. PRELIMINARIES

Definitions evoke in following are used in proposed scheme [1].

Let \((G_1,+)(G_2,+)\) be two additive cyclic group having \(P_1\) and \(P_2\) elliptic curve points generator defined over finite field of order \(n\). Let \(G_T(G_1,+)\) be a multiplicative cyclic subgroup of finite field.

A bilinear group description \(\Gamma(G_1,G_2,\hat{e},G_T)\) where \(\hat{e} : G_1 \times G_2 \rightarrow G_T\) is able to compute efficient group laws and non degeneracy of bilinear mapping.

Let a bilinear group plan \(\Gamma\), such that \(\mathcal{BDH}\) assumption is hold if advantages of probabilistic polynomial time(PPT) intruder defined is considered negligible as below.

\[
\text{Adv}_{\Gamma}^{\mathcal{BDH}}(A,q_{\mathcal{BDH}}) = \Pr \left[ T := \hat{e}(P,P)^{xy} \mid x,y,\xi \leftarrow Z_p; T \leftarrow A^{O_T}(\xi P,\xi P,\xi P) \right] \tag{1}
\]

By \(O_T\) point to the Decisional Bilinear Diffie Hellman oracle is used for tuple \((\xi P,\xi P,\xi P,T)\). The result is 1, if the statement \(T := \hat{e}(P,P)^{xy}\) hold else 0 otherwise, and \(q_{\mathcal{BDH}}\) represents number of queries in eq.(1).

Let a bilinear group plan \(\Gamma\) such that in presence of Decisional Bilinear Diffie Hellman oracle assumption if the advantage of PPT attacker defined under below probability is consider negligible.

\[
\text{Adv}_{\Gamma}^{\mathcal{CDH}}(A,q_{\mathcal{BDH}}) = \Pr \left[ Q = \xi y P \mid x,y \leftarrow Z_p; Q \leftarrow A^{O_T}(\xi P,\xi y P) \right] \tag{2}
\]

\(O_T\) and \(q_{\mathcal{BDH}}\) define as above.

A. Framework of N-CLGSC

The N – CLGSC defined using five Probabilistic Polynomial Time (PPT) and one Deterministic Polynomial Time (DPT) algorithms.

1) Setup (\(I^K\)): Its is a PPT algorithm executed by \(KGC\), which takes security parameter \((I^k)\) security parameter key and public key pair \((m_{pk},m_{sk})\), with global parameters params.

2) Extract-partial-private-key (ID, \(m_{sk}\), params): This PPT algorithm executed by \(KGC\), which takes user identity \(ID_i \in \{0,1\}^\ast\), params \((m_{sk},\text{params})\) as input, and returns partial-private-key \(D_i\).  

3) Generates user keys (ID, params): This PPT algorithm executed by user, which takes \((ID_i,\text{params})\) as input and returns secret key and public key pairs \((x_i, P_i)\).

4) Set-private-key (D, x, params): This PPT algorithm executed by the user and run in three modes: signature, encryption and signcryption.

- Signature only mode: If sender sign message \(m \in M\) with definite receiver, it takes inputs \((S_A, m, ID_o)\), with null receiver identity \(ID_o\) and returns \(\sigma = \text{GSC}(m,S_A,ID_o) = \text{sign}(m,S_A)\).

- Encryption only mode: If Alice confidentially sends message \(m\) to receiver Bob, it takes inputs \((m,S_B,ID_B)\), with null sender identity \(S_B\), and returns \(\sigma = \text{GSC}(S_B,m,ID_B) = \text{encrypt}(m,D_B,ID_B)\).

- Signcryption only mode: If Alice transmits a message \(m\) in an authenticated and confidential way to receiver, it takes inputs \((m,S_B,ID_B)\), and returns \(\sigma = \text{GSC}(S_B,m,ID_A,ID_B) = \text{signcrypt}(m,S_A,ID_A,D_B,ID_B)\).

5) GSC(m,S_A, ID_A, D_B, ID_B): This PPT algorithm executed by the user and run in three modes: signature, encryption and signcryption.

B. Security Analysis

Confidentiality

The N – CLGSC notion is captured here to represent two games between challenger (C) and adversary (A). First for adversary-I (A-I) and second for adversary-II (A-II).

1) GAME 01: (IND – CLGSC – CCA2 – I):

- Initialization: Challenger C start this algorithm and take security parameters \(k\) as input and returns params as output to adversary A-I.

- Final stage: At this level adversary A-I makes few oracles adaptively.

- Challenge: A-I selects \(m_0\) and \(m_1\) equal length two distinct messages, \(ID_A^0\) is sender’s ID and \(ID_A^1\)
receiver’s ID using which he/she makes challenges. Adversary A-I must have no private key for extraction query on $ID^*_B$, and also $ID^*_B \neq ID_A$ for confidentiality game. Challenger C selects a bit $\lambda \in \{0, 1\}$ randomly, and runs GSC algorithm with message $m_\lambda$ using $ID^*_A$ and $ID^*_B$ and returns output $(\sigma^*)$ as a ciphertext to A-I.

**Guess stage:** Just like find stage A-I makes few queries adaptively. For private key extraction corresponding to replace with public keys ($PK^*_A, PK^*_B$) after a challenge. Eventually, A-I wins the game after output a bit $\hat{\lambda}$ and if $\lambda := \hat{\lambda}$.

Advantage of adversary A-I define as;

$$Adv^{IND-CLGSC-CCA2-I}_{A-I} := 2Pr[\lambda := \hat{\lambda}] - 1$$

**Note:** In above game, we consider only encryption mode of CLGSC where sender private key $ID^*_A$ is equal to zero therefore in challenge phase algorithm runs in only encryption mode. For encryption and signcryption only modes use same confidentiality game.

A New – CLGSC scheme is secure against IND – CLGSC – CCA2 – I in encryption only mode or signcryption only mode if it is secure for all Probabilistic Polynomial Time $PPT$ adversary A-I and game winning consider negligible.

2) **GAME 02 (IND – CLGSC – CCA2 – II):** Here in this game $k$ represents security parameters and $\mathcal{C}$ represents simulator.

Simulator $\mathcal{C}$ executes A-II using input $1^k$ and master key gen. A master key pair $(M_{SK}, M_{PK})$ set params generated by adversary A-II provides $M_{SK}$ and set params to $\mathcal{C}$ without making query to any oracle.

$\mathcal{C}$ executes A-II on $1^k$ again with different tag makes above query adaptively and A-II select two equal length messages $(m_0, m_1)$ and $ID^*_A, ID^*_B$ on which makes challenges. For the purpose of extraction query on $ID^*_B$ A-II must has no choice to make private key.

$\mathcal{C}$ selects a bit $\lambda \in \{0, 1\}$ randomly, and also runs A-II using challenged ciphertext $\sigma^*$ with guess.where;

$$\sigma^* \leftarrow GSC(m_\lambda, ID^*_A, ID^*_B)$$

Like step 2 A-II makes queries again adaptively. Extraction and GSC query on ciphertext $\sigma^*$ not allowed. Eventually, A-II wins the game after output a bit $\hat{\lambda}$ and if $\lambda := \hat{\lambda}$. Advantages of A-II’s is define as;

$$Adv^{IND-CLGSC-CCA2-II}_{A-II} := 2Pr[\lambda := \hat{\lambda}] - 1$$

**Note:** At step second in above algorithm, if sender $ID^*_A$ vacant, it will be run in encryption only mode else it will be run in signcryption only mode, for both modes share similar confidentiality game.

**CLGSC scheme:** is to be secured against IND – CLGSC – CCA2 – II in encryption only mode or signcryption only mode if it is secure for all Probabilistic Polynomial Time $PPT$ adversary A-II, and consider it negligible to win game.

3) **Unforgeability:** For EUF – CMA the CLGSC security notion is captured here using following two games between challenger (C) and adversary (A).

4) **GAME 03 (EUF – CLGSC – CMA – I):**

- **Initialization:** This phase is similar to game 01.
- **Queries:** Adversary A-I makes polynomial time above phases oracles adaptively.
- **Forgery:** A-I produces $(ID_A, ID_B, \sigma)$ without exposed private key $ID_A$ where $ID_A = ID_\phi$ for unforgeability game. If final results of UGSC $(\sigma, ID_B, S_B, PK_B, ID_A, PK_A)$ is not $\perp$ A-I succeed to win the game. The advantage of A-I defines from the probability of their wining.

**Note:** In above game, we consider CLGSC signature only mode and signcryption only mode. If in forgery phase the sender $ID^*_B$ vacant then algorithm runs in signature only mode else runs in signcryption only mode and that is why we consider similar game for both modes.

A CLGSC scheme $EUF – CLGSC – CMA – I$ is to be declared secure in signature only mode or in signcryption only mode if it secure against all types of $PPT$ adversary A-I and consider negligible to win the game.

5) **GAME 04 (EUF – CLGSC – CMA – II):**

1) This phase is similar to game 02.
2) Challenger C again invokes A-II on $1^k$ with tag forge. A-II makes above oracles polynomial time adaptively.
3) At final stage A-II produces output $(ID_A, ID_B, \sigma)$ without exposed private key $ID_A$ where $ID_A = ID_\phi$ for unforgeability game.
4) If result of UGSC $(\sigma, ID_B, S_B, PK_B, ID_A, PK_A)$ is not $\perp$ then A-II succeed to win the game. A-II advantage defines from the probability of victory.

**Note:** At step 2 of above algorithm, if sender $ID^*_B$ vacant then it will be run in signature only mode else it runs in signcryption only mode and we consider same game for both type modes.

The scheme $N – CLGSC$ will be $EUF – CLGSC – CMA – II$ secured in signature only mode or in signcryption only mode if it is secure for all type of $PPT$ adversary A-II and consider it negligible to win this game.

III. REVIEW OF ZHOU ET AL. N-CLGSC

In this section of paper, we review Zhou et al. scheme, which has the following algorithms:

- **Setup** ($1^k$)- Given ($1^k$), the Key Generation Center chooses two groups $(G_1, +)$ and $(G_2, *)$ having generator $P$ of prime order $n$, using a bilinear map such that $e : G_1 \times G_1 \rightarrow G_2$, 4 hash functions as $H_1 : \{0, 1\}^* \rightarrow G_1, H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^k, H_3 : \{0, 1\}^* \rightarrow G_1, H_4 : \{0, 1\}^* \rightarrow G_1$, $KGC$ selects random integer $s \in Z_n$.
and computes $P_{pub} = sP$ and then defines function $f(ID_i)$, if $ID_i \in \varphi$, $f(ID_i) = 0$ else $f(ID_i) = \{G_3, G_2, e, q, f(\cdot), P, P_{pub}, H_1, H_2, H_3, H_4\}$ as system parameters.

Note: At initial stage it is also possible that KGC be malicious.

- **Extract partial private key:** For the given $i$th user identity $ID_i$, KGC computes partial private key as $D_i = sQ_i = sH_1(ID_i)$.

- **Generate user keys:** The $i$th user chooses random integer $x_i \in z_q^+$ and computes public key as $PK_i = x_iP$.

- **Set private key:** The $i$th user sets $SK_i = \langle x_i, D_i \rangle$ as a private key.

- **N–CLGSC** $(m, D_A, ID_A, ID_B, PK_B, PK_A)$:
  1) Computes $f(ID_A), f(ID_B)$
  2) Chooses random number $r \in z_q^+$ and then computes $U = rP$
  3) Computes $w := \hat{\epsilon}(P_{pub}, QB)^{f(ID_B)}$
  4) Computes $h = f(ID_B)H_2(w, U, r, PK_B, PK_B, ID_A, PK_A, PK_B)$
  5) Computes $H := H_3(U, V, ID_A, ID_B, PK_B)$
  6) Computes $\hat{H} = H_4(U, V, ID_A, PK_A, ID_B, PK_B)$
  7) Computes $W = f(ID_A)D_A + rH + f(ID_A)x_A$
  8) At the end returns $c$ as ciphertext $= (U, V, W)$

- **UGSC** $(U, V, W, ID_A, ID_B, PK_B, PK_A, x_B)$:
  1) Computes $H = f(ID_B)$
  2) Computes $H_3(U, V, ID_A, PK_A, ID_B, PK_B)$
  3) Computes $\hat{H} = H_4(U, V, ID_A, ID_B, PK_A, PK_B)$
  4) If $\hat{\epsilon}(P_{pub}, Q_A)^{f(ID_A)}\hat{\epsilon}(H, U)\hat{\epsilon}(PK_A)$, $\hat{H} \hat{\epsilon}(ID_A)$ else return $\perp$.
  5) Computes $w := \hat{\epsilon}(U, V, D_B)^{f(ID_B)}$
  6) Computes $h = f(ID_B)H_2(w, x_B, U, ID_A, PK_A, ID_B, PK_B)$
  7) Computes $m = V \oplus h$
  8) Returns $m$

A. Adaptation

$N–CLGSC$ work adaptively and impeccably switches on user inputs to three different modes according to the applications need without any other additional operation.

- **Signature only mode:** When $ID_A \neq \varphi$, and $f(ID_A) = 1$ as well as $f(ID_B) = 0$, $W = m \oplus h = m, c = (U, m, W)$.

- **Encryption only mode:** When $ID_A = \varphi$, and $ID_B \neq \varphi$ then $f(ID_A) = 1$ as well as $f(ID_B) = 0, W = rH$, and $c = (U, V, W)$.

- **Signcryption only mode:** When $ID_A \neq \varphi$, and $ID_B \neq \varphi$ then $f(ID_A) = 1$ as well as $f(ID_B) = 1, W = D_A + rH + x_A$

IV. CRYPTOANALYSIS OF N-CLGSC

In this section of the paper, we presented attack and proved Zhou et al. scheme ($N–CLGSC$) insecure against IND–CCA2 under encryption and signcryption only modes and working securely in signature only mode.

- **Encryption only Mode**

Setup:- Let $k$ represent security parameter and $C$ represents a simulator and executes $A$-II using $1^k$ and a master-key-generator. $A$-II generates a master key pair $(M_{SK}, M_{PK})$ and params and atedthcalA–IIHandM_{SK} to $C$ without making any query to oracle.

Phase 1: Not to ask any queries.

Phase 2: $A$-II selects $(m_0$ and $m_1$) two equal length messages and $ID_A^*$ and $ID_B^*$ to make challenges. For the purpose of extraction query on $ID_B^* := ID_A^*$ $A$-II must has no choice to make private key. $C$ randomly chooses a bit $\lambda \in \{0, 1\}$ and $A$-II runs a challenge where ciphertext $\sigma^*$ and a tag guess where:

$$\sigma^* \leftarrow GLSC(m, ID_A^*, ID_B^*)$$

1) Computes $U^* = r^*P$

2) Computes $w^* = \hat{\epsilon}(P_{pub}, QB)^{f(ID_B)}$

3) Computes $h^* = f(ID_B, H_2, U^*, w^*, r^*, PK_A, PK_B)$

4) Computes $V^* = m_{k^*}^l$ + $h^*$

5) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$

6) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$

7) Computes $W^* = 0.1D_A + r^*H^*$

8) Returns ciphertext $c^* = (U^*, V^*, W^*)$

Send $c^* = (U^*, V^*, W^*)$ to $A$.

Upon receipt of the challenge ciphertext $c^* = (U^*, V^*, W^*)$, $A$ computes

1) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$

2) Computes $r^* = \frac{-W^*}{m_{k^*}}$

3) Chooses another equal length message $m^+$ as that of $m_{k^*}^l$

4) Computes $V^* = V^* \oplus m^+$

5) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$

6) Computes $W^* = r^*H^*$

$A$ can legally queries $c^* = (U^*, V^*, W^*)$ to $C$, as $c^* = c^+$. $C$ will certainly return $m_3^+ \oplus m^+ \to A$ and $A$ can compute $m_{k^*}^l = m_{k^*}^l \oplus m^+ \oplus m^+$, guess the $\beta$ and wins the game. Hence it is proved that $N–CLGSC$ insecure against IND–CCA2 in encryption only mode.

- **Signcryption only Mode**

In this section of the paper, we presented an attack and proved that Zhou et al. provable certificateless generalized...
signcryption scheme \((N - \text{CLGSC})\) is not \(IND - CCA2\) secure in signcryption mode also.

Setup: Same as in encryption mode.

Phase 01: Same as in encryption mode.

Phase 02: \(A\)-II provides \((m_0, m_1)\) two equal length messages and sender’s identity \(ID_A\) and receiver’s identity \(ID_B\) use for challenge. \(A\)-II not to be allowed for private key extraction query on \(ID_B^*\), as \(ID_B^* = ID\) using for confidentiality game. The challenger \(C\) picks a bit \(\beta \in \{0, 1\}\) randomly and runs \(A\)-II takes a challenged ciphertext \(\sigma\) as input a challenged ciphertext \(\sigma \leftarrow \text{SCG}(m_0, ID_A^*, ID_B^*)\).

1. Computes \(U^* = r^*P\)
2. Computes \(w^* = \hat{e}(P_{pub}, QB)^{r^*f(ID_B)}\)
3. Computes \(h^* = f(ID_B, H_2)(U^*, w^*, r^*, PK_A, PK_B, ID_B)\)
4. Computes \(V^* = m_0^* \oplus h^*\)
5. Computes \(H^* = H_3(U^*, V^*, PK_A, ID, PK_B)\)
6. Computes \(H^* = H_4(U^*, V^*, PK_A, ID_B, PK_B)\)
7. Computes \(W^* = f(ID_A)D_A + r^*H^* + f(ID_A)x_A H^*\)
8. At the end send ciphertext \(c^* = (V^*, U^*, W^*)\)

A. Variation

\(IN - \text{CLGSC}\) works adaptively and impeccably switches on inputs of users, to three different modes according to the applications need without any other additional operation.

1. \(KGC\) publishes following system parameters as \(G_1, G_2, q, f(). P_{pub}, P, e, H_1, H_2, H_3, H_4\).

Note: At the initial stage it is also possible that \(KGC\) be malicious.

Extract partial private key: Given the \(ith\) user identity \(ID_i\), \(KGC\) computes partial private key as \(D_i = sQ_i = sH_1(ID_i)\).

Generate user keys: Given \(ith\) user partial private key \(D_i\) and identity \(ID_i\) chooses random integer \(x_1 \in z_q^*\) and thus computes public key \(PK_i = x_1P\).

Set private key: The \(ith\) user sets \(SK_i = (x_i, D_i)\) as a private key.

\(IN - \text{CLGSC}(m, D_A, ID_A, ID_B, PK_B, PK_A)\):

1. Computes \(f(ID_A), f(ID_B)\)
2. select a random integer value \(r \in z_q^*\)
3. Computes \(U := rP, \)
4. Computes \(w := \hat{e}(P_{pub}, QB)^{f(ID_B)}\),
5. Computes \(h := f(ID_B)H_2(U, w, r, PK_B, ID_A, PK_A, ID_B, PK_B)\)
6. Computes \(V := m \oplus (ID_A||ID_B) \oplus h\)
7. Computes \(H := H_3(U, V, w, PK_A, ID_A, PK_B)\),
8. Computes \(H := H_4(U, V, ID_A, ID_B, PK_A, PK_B)\),
9. Computes \(W := f(ID_A)D_A + r.H + f(ID_A)x_A H\)
10. At the end returns ciphertext \(c = (U, V, W)\) forward to receiver.

\(U - IN - CLGSC(U, V, W, ID_A, ID_B, PK_B, PK_A, x_B)\)

1. Computes \(f(ID_A), f(ID_B)\),
2. Computes \(w := \hat{e}(U, D_B)\),
3. Computes \(H := H_3(U, V, W, ID_A, ID_B, PK_A, PK_B)\)
4. Computes \(H := H_4(U, V, ID_A, ID_B, PK_A, PK_B)\)
5. If \(\hat{e}(P, W) := \hat{e}(P_{pub}, QA)^{f(ID_A)\hat{e}(U, H)\hat{e}(PK_A, H)}\), \(f(ID_A)\) else returns \(\bot\).
6. Computes \(h := f(ID_B)H_2(U, w, x_B U, ID_A, PK_A, ID_B, PK_B)\)
7. Computes \(m := V \oplus (ID_A||ID_B) \oplus h\)
8. Returns \(m\).

V. IMPROVED N-CLGSC

This section represents improved scheme, we proposed an Improved scheme \((IN - \text{CLGSC})\) scheme, comprises on the following algorithms:

1. \(KGC\) publishes following system parameters as \(G_1, G_2, q, f(). P_{pub}, P, e, H_1, H_2, H_3, H_4\).

A. Variation

\(IN - \text{CLGSC}\) works adaptively and impeccably switches on inputs of users, to three different modes according to the applications need without any other additional operation.
A. Correctness

The correctness proofs of Zhou et al. \( N - CLGSC \) and \( IN - CLGSC \) are same. As the proofs had not discussed in the existing scheme but here we demonstrate correctness proofs also as:

- **Signcryption only mode**
  
  If \( ID, f(ID_A) = 1 \) then
  
  \[
  \hat{e}(P, W) = \hat{e}(P, D_A + r.H + x'_A H) \\
  = \hat{e}(P, D_A)\hat{e}(P, r.H)\hat{e}(P, x'_A H) \\
  = \hat{e}(P, s.Q_A)\hat{e}(r.P, H)\hat{e}(x_A P, \hat{H}) \\
  = \hat{e}(sP, Q_A)\hat{e}(U, H)\hat{e}(PK_A, \hat{H}) \\
  = \hat{e}(P_{pub}, Q_A)\hat{e}(U, H)\hat{e}(PK_A, \hat{H}) \\
  = \hat{e}(P_{pub}, Q_A, f(ID_A))\hat{e}(U, H)\hat{e}(PK_A, \hat{H}), f(ID_A)
  \]

- **Encryption only mode**
  
  If \( ID_A = \varnothing, f(ID_A, h) = 0 \) then
  
  \[
  \hat{e}(P, W) = \hat{e}(P, r.H) \\
  = \hat{e}(r.P, H) = \hat{e}(U, H) = 1.\hat{e}(U, H).1 \\
  = \hat{e}(P_{pub}, Q_A, f(ID_A))\hat{e}(U, H)\hat{e}(PK_A, \hat{H}), f(ID_A)
  \]

- **Signature only mode**
  
  If \( ID_A \neq \varnothing, f(ID_A) = 1 \) then
  
  \[
  (P, W) = \hat{e}(P, D_A + r.H + x'_A H) \\
  = \hat{e}(P, D_A)\hat{e}(P, r.H)\hat{e}(P, x'_A H) \\
  = \hat{e}(P, sQ_A)\hat{e}(r.P, H)\hat{e}(x_A P, \hat{H}) \\
  = \hat{e}(sP, Q_A)\hat{e}(U, H)\hat{e}(PK_A, \hat{H}) \\
  = \hat{e}(P_{pub}, Q_A)\hat{e}(U, H)\hat{e}(PK_A, \hat{H}) \\
  = \hat{e}(P_{pub}, Q_A, f(ID_A))\hat{e}(U, H)\hat{e}(PK_A, \hat{H}), f(ID_A)
  \]

B. Security Analysis

Confidentiality proof of \( IN - CLGSC \)

**Theorem 01**: Against above proposed (signcryption or encryption only mode) scheme if PPT adversary A-I has non negligible advantage to win game \( IND - CLGSC - CCA2 - I \) in random oracle model then A-I must be used algorithm B to solve a hard GBDH problem as:

\[
Adv^{IND-CCA2-I}_{CLGSC}(A - I) \leq q_T Adv^{CDH}_{I}(B, q_D^2 + 2q_{DQ} + q_2) + q_{SC}(q_{SC} + q_D + q_3 + 1)/2^k
\]

Where \( q_T = q_1 + q_x + q_{SK} + 2q_D + 2q_{SC} + 2 \). Here \( q_{PK} \) represents maximum queries which an adversary could place to \( H_1, H_2, H_3 \), for full and partial private keys extraction as well as for GSC and UGSC oracles.

**Theorem 02**: Against above proposed (encryption or signcryption only mode) scheme if PPT adversary A-II has non negligible advantage to win game \( IND - CLGSC - CCA2 - II \) in random oracle model then A-II must be used algorithm B to solve a hard CDH problem as:

\[
Adv^{IND-CCA2-II}_{CLGSC}(A - II) \leq q_T Adv^{CDH}_{I}(B, q_{SC} + q_D + q_3 + 1)/2^k
\]

Where \( q_T = q_{PK} + q_{SK} + 2q_D + 2q_{SC} + 2 \). Here \( q_{PK} \) represents maximum queries which an adversary can place multiple request for public key oracles.

C. Unforgeability of Proof \( IN-CLGSC \)

**Theorem 03**: Against above proposed (signcryption or signature only mode) scheme if PPT adversary A-I has non negligible advantage to win game \( EUF - CLGSC - CMA - I \) in random oracle model then A-I must be used algorithm B to solve a hard CDH problem as:

\[
Adv^{EUF-CMA-I}_{CLGSC}(A - I) \leq q_T Adv^{CDH}_{I}(B, q_{DQ}^3 + 2q_{DQ}) + (q_{SC}(q_{SC} + q_D + q_3 + 1) + 2)/2^k
\]

Where \( q_T = q_1 + q_x + q_{SK} + 2q_D + 2q_{SC} + 1 \) and various \( q \)s are as . Against above proposed (signature or signcryption only mode) scheme if PPT adversary A-II has non negligible advantage to win game \( EUF - CLGSC - CMA - II \) in random oracle model then A-II must be used algorithm B to solve a hard CDH problem as:

\[
Adv^{EUF-CMA-II}_{CLGSC}(A - II) \leq q_T Adv^{CDH}_{I}(B, q_{DQ}^3 + 2q_{DQ}) + (q_{SC}(q_{SC} + q_D + q_3 + 1) + 2)/2^k
\]

Where \( q_T = q_1 + q_x + q_{SK} + 2q_D + 2q_{SC} + 1 \) and various \( q \)s are as .

**Theorem 04**: Against above proposed (signature or signcryption only mode) scheme if PPT adversary A-II has non negligible advantage to win game \( EUF - CLGSC - CMA - II \) in random oracle model then A-II must be used algorithm B to solve a hard CDH problem as:

\[
Adv^{EUF-CMA-II}_{CLGSC}(A - II) \leq q_T Adv^{CDH}_{I}(B, q_{DQ}^3 + 2q_{DQ}) + (q_{SC}(q_{SC} + q_D + q_3 + 1) + 2)/2^k
\]

Where \( q_T = q_{PK} + q_{SK} + 2q_D + 2q_{SC} + 1 \) and few others \( q \)s are as discussed before.

**Note**: The proofs of above theorems are similar to discussed in [4].
D. Cost Analysis

In public key cryptography, the standard notion of computational cost is the number of major operations like the elliptic curve scalar point multiplication (ECPM) in $G_1$, the modular exponentiation computation ($M - \text{Exp}$) in $G_2$ and the pairing computation ($PC$). The communication overhead is the ciphertext size in bits.

The security and cost comparison of proposed and existing schemes (only four CLGSC schemes are there in existing literature up-to date) are presented in the following Tables 1 and 2.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Security</th>
<th>Computational Cost</th>
<th>Cipher text Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ECPM $M - \text{Exp}$</td>
<td>$PC$</td>
</tr>
<tr>
<td>Huifang et al.[11]</td>
<td>No</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Kushwah and Lie. [12]</td>
<td>Yes</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Zhou et al.[1]</td>
<td>No</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Proposed IN-CLGSC</td>
<td>Yes</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

VII. CONCLUSION

Zhou et al. recently proposed a new certificateless generalized signcryption scheme and proved its security against IND − CCA2 and EUF − CMA in presence of Malicious-but-Passive Key Generation Center in random oracle model. We analyzed Zhou et al. scheme and unfortunately proved IND − CCA2 insecure in encryption and signcryption modes in their defined security model. We also presented an improved scheme, provable secure in presence of Malicious-but-Passive Key Generation Center in random oracle model. The improved scheme is same cost as Zhou et al. scheme and feasible for scarce resource environment.

REFERENCES