Improved Cryptanalysis of Provable Certificateless Generalized Signcryption

Abdul Waheed[1]
School of Electrical and Computer Engineering Seoul National University Korea Republic of
Department of Information Technology
Hazara University Mansehra, KP

Nizamud Din[3]
Department of Computer Science
University of Chitral, KP

Arif Iqbal Umar[5]
Department of Information Technology
Hazara University Mansehra, KP

Jawaid Iqbal[2]
Department of Information Technology
Hazara University Mansehra, KP

Shahab Ul Islam[4]
Department of Computer Science
IQRA National University

Noor Ul Amin[6]
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. Riyami and Paterson [6] first time gave Certificateless Public Key Cryptography ($CL-PKC$) 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 Certificatless (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 presents 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 $(G_1,+)$ and $(G_2,+)$ 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 Γ, such that $\mathcal{GBDH}$ assumption is hold if advantages of probabilistic polynomial time($\mathcal{PPT}$) intruder defined is considered negligible as below.

$$Adv\Gamma^{\mathcal{GBDH}}(A;q_{\mathcal{DBDH}})=Pr[T:=\hat{e}(P,P)^{\widetilde{xyz}} \mid \widetilde{x},\widetilde{y},\widetilde{z}\leftarrow Z_p; T\leftarrow A^{o_\Gamma(T,\widetilde{x}P,\widetilde{y}P,\widetilde{z}P)}] \quad (1)$$

By O_Γ point to the Decisional Bilinear Diffie Hellman oracle is used for tuple $(\widetilde{x}P,\widetilde{y}P,\widetilde{z}P,T)$. The result is 1, if the statement $T:=\hat{e}(P,P)^{\widetilde{xyz}}$ hold else 0 otherwise, and $q_{\mathcal{DBDH}}$ represents number of queries in $eq(1)$.

Let a bilinear group plan Γ such that in presence of Decisional Bilinear Diffie Hellman oracle assumption if the advantage of $\mathcal{PPT}$ attacker defined under below probability is consider negligible.

$$\mathrm{Adv}_\Gamma^{\mathcal{GDH}}(A,q_{DBDH})=Pr[Q=\widetilde{x}\widetilde{y}P|\widetilde{x},\widetilde{y}\leftarrow\mathcal{Z}_p, \mathcal{Q}\leftarrow A^{O_\Gamma}(\Gamma,\widetilde{x}P,\widetilde{y}P)] \quad (2)$$

O_Γ and q_{DBDH} define as above.

Let a bilinear group plan Γ, such that the assumption of Computational Diffie Hellman ($\mathcal{CDH}$) is hold if the advantage of any $\mathcal{PPT}$ attacker defined under below probability is negligible.

$$\mathrm{Adv}_\Gamma^{\mathcal{CDH}}(\mathrm{A}) = \Pr[\mathcal{Q}=\widetilde{x}\widetilde{y}P|\widetilde{x},\widetilde{y}\leftarrow\mathcal{Z}_p;\mathcal{Q}\leftarrow A(\Gamma,\widetilde{x}P,\widetilde{y}P)]. \quad (3)$$

A. Framework of N-CLGSC

The $N-CLGSC$ defined using five Probabilistic Polynomial Time ($\mathcal{PPT}$) and one Deterministic Polynomial Time ($\mathcal{DPT}$) algorithms.

1) *Setup ($1^{\mathbf{k}}$)*: Its is a $\mathcal{PPT}$ algorithm executed by $\mathcal{KGC}$, which takes security parameter ($1^{\mathbf{k}}$ 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 $\mathcal{PPT}$ algorithm executed by $\mathcal{KGC}$, which takes user identity $ID_i\in\{0,1\}^*$, params $(m_{sk},params)$ as input, and returns *partial-private-key D_i*.
3) *Generates user keys (ID, params)*: This $\mathcal{PPT}$ algorithm executed by user, which takes $(ID_i,params)$ as input and returns a secret key and public key pairs(x_i,P).
4) *Set-private-key (D, x, params)*: This $\mathcal{PPT}$ algorithm executed by the user, takes $(ID_i,x_i,params)$ as input and returns full private key S_i.
5) *GSC(m,S_A, ID_s,D_B, ID_B)*: This $\mathcal{PPT}$ algorithm executed by the user and run in three modes: signature, encryption and signcryption.
   - **Signature only mode**: If sender sign message $m\in M$ without definite receiver, it takes inputs (S_A,m,ID_ϕ), with null receiver identity ID_ϕ , and returns $\sigma = GSC(m,S_A,ID_\phi) = sign(m,S_A)$.
   - **Encryption only mode**: If Alice confidentially sends message m to receiver Bob, it takes inputs $(m,S_\phi,D_B,\ ID_B)$, with null sender identity S_ϕ, and returns $\sigma = GSC(S_\phi\ ,m,D_B,\ ID_B)$ = $encrypt$ $(m,D_B,\ ID_B)$.
   - **Signcryption only mode**: If Alice transmits a message m in an authenticated and confidential way to receiver, it takes inputs (m,S_A,ID_B), and returns σ = $GSC(m,S_A,ID_A,D_B,ID_B)$ = signcrypt (m,S_A,ID_A,D_B,ID_B)
6) *UGSC(σ)*: This $\mathcal{DPT}$ algorithm runs by receiver it takes received σ as input and validate if it is true then decrypts or unsigncrypts and returns message (m), otherwise return false $\perp$.

B. Security Analysis

Confidentiality

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

1) GAME 01: $(IND-CLGSC-CCA2-I)$:

- **Initialization:** Challenger $\mathcal{C}$ start this algorithm and take security parameters k as input and returns $params$ as output to adversary $\mathcal{A}$-I.
- **Find stage:** At this level adversary $\mathcal{A}$-I makes few oracles adaptively.
- **Challenge:** $\mathcal{A}$-I selects m_0 and m_1 equal length two distinct messages, ID_A^* is sender's ID and ID_B^*

receiver's ID using which he/she makes challenges. Adversary $\mathcal{A}$-I must have no private key for extraction query on ID_B^*, and also $ID_B^* \neq ID_\phi$ for confidentiality game. Challenger $\mathcal{C}$ selects a bit $\lambda \in \{0,1\}$ randomly, and runs GSC algorithm with message m_λ using ID_A^* and ID_B^* and returns output (σ^*) as a ciphertext to $\mathcal{A}$-I.

Guess stage: Just like find stage $\mathcal{A}$-I makes few queries adaptively. For private key extraction corresponding to ID_B^* does not allow to make UGSC query on ciphertext (σ^*) using private keys of sender and receiver ID_A^* and ID_B^* respectively until to replace with public keys (PK_A^*, PK_B^*) after a challenge. Eventually, $\mathcal{A}$-I wins the game after output a bit $\acute{\lambda}$ and if $\lambda := \acute{\lambda}$.

Advantage of adversary $\mathcal{A}$-I define as;

$$Adv_{\mathcal{A}-I}^{IND-CLGSC-CCA2-I} := 2Pr\left[\lambda := \acute{\lambda}\right] - 1$$

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

$\mathcal{C}$ executes $\mathcal{A}$-II on 1^k again with different tag makes above query adaptively and $\mathcal{A}$-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^* $\mathcal{A}$-II must has no choice to make private key.

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

$\sigma^* \leftarrow GSC(m\lambda,\text{ID}_A^*, ID_B^*)$

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

$$Adv_{\mathcal{A}-II}^{IND-CLGSC-CCA2-II} = 2Pr[\lambda = \acute{\lambda}] - 1$$

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 $\mathcal{PPT}$ adversary $\mathcal{A}$-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 ($\mathcal{C}$) and adversary ($\mathcal{A}$).

4) GAME 03 ($EUF - CLGSC - CMA - I$):

- **Initialization:** This phase is similar to game 01.
- **Queries:** Adversary $\mathcal{A}$-I makes polynomial time above phases oracles adaptively.
- **Forgery:** $\mathcal{A}$-I produces (ID_A, ID_B, σ) without exposed private key ID_A where ID_A = ID_ϕ for unforgeability game. If final results of UGSC (σ, ID_B, S_B, PK_B, ID_A, PK_A) is not $\perp$ $\mathcal{A}$-I succeed to win game. The advantage of $\mathcal{A}$-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 $\mathcal{PPT}$ adversary $\mathcal{A}$-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 $\mathcal{C}$ again invokes $\mathcal{A}$-II on 1^k with tag *forge*. $\mathcal{A}$-II makes above oracles polynomial time adaptively.
3) At final stage $\mathcal{A}$-II produces output (ID_A, ID_B, σ) without exposed private key ID_A where ID_A = ID_ϕ for unforgeability game.
4) If result of UGSC (σ, ID_B, S_B, PK_B, ID_A, PK_A) is not $\perp$ then $\mathcal{A}$-II succeed to win the game. $\mathcal{A}$-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 $\mathcal{PPT}$ adversary $\mathcal{A}$-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 ($1^{\mathbf{k}}$), 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 $\hat{e} : G_1 \times G_1 \rightarrow G_2$, 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 $s \in Z_q^*$

and computes $P_{Pub} = sP$ and then defines function like $f(ID_i), if ID_i \in \varphi, f(ID_i) = 0$ $else$ $f(ID_i)$=1 KGC publishes,$\{G_1, G_2, e, q, f(.), P, P_{Pub}, H_1, H_2, H_3, H_4\}$ as system parameters.

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

- **Extract partial private key:** For the given ith user identity ID_i , KGC computes partial private key as $D_i = sQ_i = sH_1(ID_i)$.
- **Generate user keys:** The ith user chooses random integer $x_i \in z_q^*$ and computes public key as $PK_i = x_iP$
- **Set private key:** The ith 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 $w := \hat{e}(P_{Pub}, QB)^{rf(ID_B)}$
  4) Computes $h = f(ID_B)H_2(w, U, r.PK_B, PK_B, PK_A ID_A, PK_A, PK_B itemComputesV := h \oplus m$
  5) Computes $H := H_3(U, V, ID_A, ID_B, PK_A, PK_B)$
  6) Computes $'H = H_4(V, U, ID_A, PK_A, ID_B, PK_B)$
  7) Computes $W = f(ID_A)D_A + rH + f(ID_A)x_A$ $'H$
  8) At the end returns c as $ciphertext = (U, V, W)$
- $UGSC(U, V, W, ID_A, ID_B, PK_A, x_B)$:
  1) Computes$f(ID_A), f(ID_B)$
  2) Computes $H = H_3(U, V, ID_A, PK_A, ID_B, PK_B)$
  3) Computes $'H = H_4(U, V, ID_A, ID_B, PK_A, PK_B)$
  4) If $\hat{e}(P, W) = \hat{e}(P_{Pub}, Q_A)^{f(ID_A)}\hat{e}(H, U)\hat{e}(PK_A), {'H}^{f(ID_A)}$ else return $\perp$.
  5) Computes $w = \hat{e}(U, D_B)^{f(ID_B)}$
  6) Computes $h = f(ID_B)H_2(U, w, x_BU, ID_A, PK_A, ID_B, PK_B)$
  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 $f(ID_B) = 0, V = m \oplus h = m, c = (U, m, W)$.
- **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 $f(ID_B) = 1, W = D_A + r.H + x_A$ $'H$ and $c = (U, V, W)$.

IV. Cryptanalysis 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 $\mathcal{C}$ represents a simulator and executes $\mathcal{A}$-II using 1^k and a master-key-generator. $\mathcal{A}$-II generates a master key pair (M_{SK}, M_{PK}) and params and atedthcalA$-II and$M$_{SK}$ to $\mathcal{C}$ without making any query to oracle.

Phase 1: Not to ask any queries.

Phase 2: $\mathcal{A}$-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^* $\mathcal{A}$-II must has no choice to make private key. $\mathcal{C}$ randomly chooses a bit $\lambda \in \{0, 1\}$ and $\mathcal{A}$-II runs a challenge where ciphertext σ^* and a tag guess where;

$\sigma^* \leftarrow GSC(m_\lambda, ID_A^*, ID_B^*)$

1) Computes $U^* = r^*P$
2) Computes $w^* = \hat{e}(P_{Pub}, QB)^{r^* f(ID_B)}$
3) Computes $h^* = f(ID_B, H_2, U^*, w^*, r^*, PK_A, PK_B)$
4) Computes $V^* = m_b^* \oplus h^*$
5) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$
6) Computes $\acute{H}^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$
7) Computes $W^* = 0.ID_A + r^*, H^* = r^*H^*$
8) Returns ciphertext c* =(U* , V* ,W*)

Sent $c^* = (U^*, V^*, W^*)$ to $\mathcal{A}$.

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

1) Computes $H^* = H_3(U^*, V^*, ID_B, PK_A, PK_B)$
2) Computes $r^* = \frac{W^*}{H^*}$
3) Chooses another equal length message m^+ as that of m_β^*
4) Computes V$^+ = V^* \oplus m^+$
5) Computes $H^+ = H_3(U^*, V^+, PK_A, ID_B, PK_B)$
6) Computes W$^+ = r^*H^+$

$\mathcal{A}$ can legally queries $c^+ = (U^*, V^+, W^+)$ to $\mathcal{C}$, as $c^* = c^+$. $\mathcal{C}$ will certainly return $m_\beta^* \oplus m^+$ to $\mathcal{A}$ and $\mathcal{A}$ can compute $m_\beta^* = m_\beta^* \oplus m^+ \oplus m^+$, guess the β 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 ($N-CLGSC$) is not $IND-CCA2$ secure in signcryption mode also.

Setup: Same as in encryption mode.

Phase 01: Same as in encryption mode.

Phase 02: $\mathcal{A}$-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. $\mathcal{A}$-II not to be allowed for private key extraction query on ID_B^*, as ID_B^* = ID using for confidentiality game. The challenger $\mathcal{C}$ picks a bit $\beta \in \{0,1\}$ randomly and runs $\mathcal{A}$-II takes a challenged ciphertext σ^* as input a challenged ciphertext $\sigma^* \leftarrow GSC(m_\beta, ID_A^*, ID_B^*)$.

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 $V^* = m_b^* \oplus h^*$
5) Computes $H^* = H_3(U^*, V^*, PK_A, ID, PK_B)$
6) Computes $\acute{H}^* = H_4, (U^*, V^*, PK_A, ID_B, PK_B)$
7) Computes $W^* = f(ID_A).D_A + r^*\mathrm{H}^* + f(ID_A)x_A \acute{H}^*$
8) At the end send ciphertext $c^* := (V^*, U^*, W^*)$

to $\mathcal{A}$. On the receiving challenged ciphertext $c^* = (U^*, V^*, W^*)$, In above generalized signcryption process $H^* = \acute{H}^*$ as $H_3 : \{0,1\}^* \rightarrow G_1, H_4 : \{0,1\}^* \rightarrow G_1$ and $H^* = H_3(U^*, V^*, PK_A, ID_B, PK_B), \acute{H}^* = H_4(U^*, V^*, PK_A, ID_B, PK_B)$, $\mathcal{A}$ computes

1) Computes$(r^* + x_A)$ $H^* = r^*H^* + x'_AH^* = W^* - f(ID_A).D_A$
2) Computes H*= H_3 *(U*,V*, PK$_A$, ID, PK$_B$)*
3) Computes $(r^* + x_A) = \frac{(r^*+x_A)\acute{H}^*}{\acute{H}^*}$
4) Chooses another equal length message m^+ as that of m_β^*
5) Computes $V^+ = V^* \oplus m^+$
6) Computes $H^+ = H_3(U^*, V^+, PK_A, PK_B, ID_B)$
7) Computes $W^+ = ID_A + (r^* + x_A)H^* = ID_A + r^*H^* + x_AH^*$

$\mathcal{A}$ can legally queries $c^+ = (U^*, V^+, W^+)$ to C, as $c^* = c^+$. C will certainly return $m_\beta^* \oplus m^+$ to $\mathcal{A}$ and $\mathcal{A}$ can compute $m_\beta^* = m_\beta^* \oplus m^+ \oplus m^+$, guess the β and wins the game.

Hence here also proved insecurity of $N-CLGSC$ under $IND-CCA2$ in signcryption only mode.

V. Improved N-CLGSC

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

- **Setup (1^k):** Given (1^k), two groups $(G_1, +)$ using generator P and $(G_2, *)$ respectively to be chosen by KGC using prime order n, a bilinear map , and 4 hash functions such that; $H_1 : \{0,1\}^* \rightarrow G_1, H_2 : \{0,1\}^* \rightarrow G_1, H_3 : \{0,1\}^* \rightarrow G_1, H_4 : \{0,1\}^* \rightarrow G_1$, KGC selects a random integer $s \in Z_q^*$ as a master key and computes $P_{Pub} = sP$ and then defines like function $f(ID) \mid if ID \in \varphi, f(ID) = 0$ else $f(ID) =$ 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 $x_i \in z_q^*$ and thus computes public key $PK_i = x_iP$.
- **Set private key:** The ith user sets $SK_i = \langle x_i, D_i \rangle$ as a private key.
- $IN-CLGSC(m, D_A, ID_A, ID_B, PK_B, PK_A,)$:

1) Computes $f(ID_A), f(ID_B)$
2) select a random integer value $r \in z_q^*$
3) Computes $U := r.P$,
4) Computes $w := \hat{e}(P_{Pub}, QB)^r f(ID_B)$,
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 $H := H_3(U, V, w, ID_A, PK_A, ID_B, PK_B)$,
8) Computes $\acute{H} := H_4(U, V, ID_A, PK_A, ID_B, PK_B)$,
9) Computes $W := f(ID_A)D_A + r.H + f(ID_A)x'_AH$
10) At the end returns ciphertext $c = (U, V, W)$ forward to receiver.

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

1) Computes $f(ID_A, f(ID_B)$,
2) Computes $w := \hat{e}(U, D_B), f(ID_B)$,
3) Computes $H := H_3(U, V, w, ID_A, ID_B, PK_A, PK_B)$
4) Computes $\acute{H} := H_4(U, V, ID_A, ID_B, PK_A, PK_B)$
5) If $\hat{e}(P, W) := \hat{e}(P_{Pub}, Q_A)f(ID_A)\hat{e}(U, H)\hat{e}(PK_A, \acute{H})$, $f(ID_A)$ else returns $\perp$.
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.

A. Variation

$IN-CLGSC$ works adaptively and impeccably switches on inputs of users, to three different modes according to the applications need without any other additional operation.

- Signature only mode: when $ID_A \neq \varphi$, and $ID_B = \varphi$ then the value of $f(ID_A) = 1$, and $f(ID_B) = 0, V = mh = m, c = (U, m, W)$.
- Encryption only mode: when $ID_A = \varphi$, and $ID_B \neq \varphi$ then the value of $f(ID_A) = 1$, and $f(ID_B) = 0$, $W = r.H$, and $c = (U, V, W)$.
- Signcryption only mode: when $ID_A \neq \varphi$, and $ID_B \neq \varphi$ then the value of $f(ID_A) = 1$ and $f(ID_B) = 1$, $W = D_A + r.H + x'_AH$, and $c = (U, V, W)$.

VI. Analysis of IN-CLGSC

This section of paper provides detail analysis. First part is correctness then security and cost analysis of our $IN-CLGSC$ scheme.

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, and $f(ID_A)=1$ then

$$\hat{e}(P,W)=\hat{e}(P,D_A+r.H+x'_AH)$$

$$=\hat{e}(P,D_A)\hat{e}(P,r.H)\hat{e}(P,x'_AH)$$

$$=\hat{e}(P,s.Q_A)\hat{e}(r.P,H)\hat{e}(x_AP,\acute{H})$$

$$=\hat{e}(sP,Q_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H})$$

$$=\hat{e}(P_{Pub},Q_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H})$$

$$=\hat{e}(P_{Pub},Q_A),f(ID_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H}),f(ID_A)$$

- Encryption only mode

If $ID_A=\varphi$,and $f(ID_A.h)=0$ then

$$\hat{e}(P,W)=\hat{e}(P,r.H)$$

$$=\hat{e}(rP,H)=\hat{e}(U,H)=1.\hat{e}(U,H).1$$

$$=\hat{e}(P_{Pub},Q_A),f(ID_A)\hat{e}(U,H)\hat{e}(PK_A,'H),f(ID_A)$$

- Signature only mode

$IfID_A\neq\varphi,andf(ID_A)=1$then

$$(P,W)=\hat{e}(P,D_A+r.H+x'_AH)$$

$$=\hat{e}(P,D_A)\hat{e}(P,r.H)\hat{e}(P,x'_AH)$$

$$=\hat{e}(P,sQ_A)\hat{e}(rP,H)\hat{e}(x_AP,\acute{H})$$

$$=\hat{e}(sP,Q_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H})$$

$$=\hat{e}(P_{Pub},Q_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H})$$

$$=\hat{e}(P_{Pub},Q_A),f(ID_A)\hat{e}(U,H)\hat{e}(PK_A,\acute{H}),f(ID_A)$$

B. Security Analysis

Confidentiality proof of $IN-CLGSC$

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

$$Adv^{IND-CCA2-I}_{CLGSC}(\mathcal{A}-I)\leq q_T\ Adv^{\mathcal{GBDH}}_{\Gamma}(B,q_D^2+2_{qDq2}+q_2)+q_{SC}(q_{SC}+q_D+q_3+1)/2^k \quad (4)$$

Where $q_T=q_1+q_x+q_{SK}+2q_D+2_qSC+2$. Here $q_1,q_2,q_3,q_X,q_K,q_{SC}$ and q_D 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 $\mathcal{PPT}$ adversary $\mathcal{A}-II$ has non negligible advantage to win game ($IND-CLGSC-CCA2-II$)* in random oracle model then $\mathcal{A}$-II must be used algorithm B to solve a hard CDH problem as;

$$Adv^{IND-CCA2-II}_{CLGSC}(\mathcal{A}-II)\leq q_T\ Adv^{\mathcal{CDH}}_{\Gamma}(B)+q_{SC}(q_{SC}+q_D+q_3+1)/2^k \quad (5)$$

Where $q_T=q_{PK}+q_{SK}+2_{qD}+2_{qSC}+2$. 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 :

$$Adv^{EUF-CMA-I}_{CLGSC}(\mathcal{A}-I)\leq q_TAdv^{\mathcal{GDH}}_{\Gamma}(B,q_{2D}+2_{qDq2})+(q_{SC}(q_{SC}+q_D+q_3+1)+2)/2^k \quad (6)$$

where $q_T=q_1+q_X+q_{SK}+2_{qD}+2_{qSC}+1$ and various $q's$ are as .Against above proposed (signature or signcryption only mode) scheme if $\mathcal{PPT}$ adversary $\mathcal{A}$-I has non negligible advantage to win game ($EUF-CLGSC-CMA-I$) in random oracle model then $\mathcal{A}$-I must be used algorithm B to solve a hard GDH problem as:

$$Adv^{EUF-CMA-I}_{CLGSC}(\mathcal{A}-I)\leq q_TAdv^{\mathcal{GDH}}_{\Gamma}(B,q_{2D}+2_{qDq2})+(q_{SC}(q_{SC}+q_D+q_3+1)+2)/2^k \quad (7)$$

where $q_T=q_1+q_X+q_{SK}+2_{qD}+2_{qSC}+1$ and various $q's$ are as .

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

$$Adv^{EUF-CMA-II}_{CLGSC}(\mathcal{A}-II)\leq q_TAdv^{CDH}_{\Gamma}(B)+(q_{SC}(q_{SC}+q_D+q_3+1)+2)/2^k \quad (8)$$

Where $q_T=q_{PK}+q_{SK}+2_{qD}+2_{qSC}+1$ 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 ($M - Exp$) 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 I. SECURITY COMPARISON

Scheme	Security		
	IND-CCA2	EUF-CMA	M-PKGC
Huifang et al.[11]	*No*	Yes	*No*
Kushwah and Lie. [12]	*Yes*	*Yes*	*No*
Zhou et al.[1]	*No*	*Yes*	*No*
Proposed IN-CLGSC	*Yes*	*Yes*	*Yes*

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

[1] C. Zhou, W. Zhou, and X. Dong, "Provable certificateless generalized signcryption scheme," Des. Codes, Cryptogr., vol. 71, no. July 2012, pp. 331–346, 2014.

[2] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644 – 654, 1976.

[3] R. L. Rivest, a. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[4] A. Shamir, "Identity-based cryptosystems and signature schemes," Adv. Cryptol. CRYPTO 84, LNCS, vol. 196, pp. 47–53, 1985.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Advances in Cryptology CRYPTO 2001, LNCS, 2001, vol. 2139, pp. 213–229.

[6] S. S. Al-Riyami and K. G. Paterson, "Certificateless Public Key Cryptography," in Advances in Cryptology-ASIACRYPT 2003, 2003, pp. 452–473.

[7] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)," in Advances in Cryptology, CRYPTO'97, 1997, pp. 165–179.

[8] M. Barbosa and P. Farshim, "Certificateless Signcryption," in ACM symposium on Information, computer and communications security ASIACCS '08, 2008, pp. 369–372.

[9] Y. Han, X. Yang, P. Wei, Y. Wang, and Y. Hu, "ECGSC: Elliptic Curve based Generalized Signcryption," in Ubiquitous Intelligence and Computing, LNCS-4159, 2006, pp. 956–965.

[10] S. Lal and P. Kushwah, "ID based generalized signcryption," in Cryptology ePrint Archive, Report 2008/084. http://eprint.iacr.org (2008), 2008, pp. 1–26.

[11] J. Huifang, H. Wenbao, and Z. Long, "Certificateless generalized signcryption," in Cryptology ePrint Archive, Report 2010/204. http://eprint.iacr.org, 2010.

[12] P. Kushwah, "Efficient Generalized Signcryption Schemes," Theor. Comput. Sci., vol. 412, no. 45, pp. 6382–6389, 2011.

[13] L.-D. Liu, H.-F. Ji, W.-B. Han, and L. Zhao, "Certificateless Generalized Signcryption Scheme," Phys. Procedia, no. 33, pp. 962 – 967, 2012.

[14] C. P. R. S. Sharmila Deva Selvi, S. Sree Vivek, "Cryptanalysis of Certificateless Signcryption Schemes and an Efficient Construction without Pairing," in Information Security and Cryptology, LNCS Volume 6151, 2010, pp. 75–92.

[15] M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang, "Malicious KGC attacks in certificateless cryptography," ASIACCS 2007 Proc. 2nd ACM Symp. Information, Comput. Commun. Secur., pp. 302–311, 2007.

[16] Y. H. Hwang, J. K. Liu, and S. S. M. Chow, "Certificateless public key encryption secure against malicious KGC attacks in the standard model," J. Univers. Comput. Sci., vol. 14, no. 3, pp. 463–480, 2008.

[17] H. Xiong, Z. Qin, and F. Li, "An Improved Certificateless Signature Scheme Secure in the Standard Model," Fundam. Informaticae, vol. 88, no. 1–2, pp. 193–206, 2008.

[18] J. Weng, G. Yao, R. H. Deng, M. R. Chen, and X. Li, "Cryptanalysis of a certificateless signcryption scheme in the standard model," Inf. Sci. (Ny)., vol. 181, no. 3, pp. 661–667, 2011.

[19] Li, Fagen, Hui Zhang, and Tsuyoshi Takagi. "Efficient signcryption for heterogeneous systems." IEEE Systems Journal 7.3 (2013): 420-429.

[20] Li, Fagen, Yanan Han, and Chunhua Jin. "Practical access control for sensor networks in the context of the Internet of Things." Computer Communications 89 (2016): 154-164.

[21] Niu, Shufen, et al. "An Efficient Heterogeneous Signcryption Scheme from Certificateless to Identity-based Cryptosystem." MATEC Web of Conferences. Vol. 139. EDP Sciences, 2017.

[22] Caifen, Wang, et al. "Efficient Heterogeneous Signcryption Scheme in the Standard Model." Journal of Electronics & Information Technology 39.4 (2017): 881-886.

TABLE II. COST COMPARISON

Scheme	Computational Cost						Cipher text Size
	CLGSC			*CLUGSC*			
	$ECPM$	$M-Exp$	PC	$ECPM$	$M-Exp$	PC	
Huifang et al.[11]	3	2	0	1	1	2	$\|m\|+2\|G_1\|+\|ID\|+\|G_2\|+\|P\|$
Kushwah and Lie. [12]	2	3	0	1	3	2	$\|m\|+2\|G_1\|+\|ID\|+\|G_2\|$
Zhou et al.[1]	1	4	0(+1)	0	1	4(+1)	$\|m\|+2\|G_1\|$
Proposed IN-CLGSC	1	4	0(+1)	0	1	4(+1)	$\|m\|+2\|G_1\|$