A Note on Obtain Confidentiality or/ and Authenticity in Big Data by ID-Based Generalized Signcryption

Nizamud Din[a,b] [1], Arif Iqbal Umar[a], Abdul Waheed[a], Noor ul Amin[a]

[a] *Department of Information Technology, Hazara University*

[b] *Department of Computer Science, IQRA National University Peshawar*

Abstract

$\mathcal{ID}$ based generalized signcryption can adaptively work as a signature scheme, an encryption scheme or a signcryption scheme and avoid weighty and complicated certificate management like Public Key Infrastructure. It has application in emerging paradigm big data security. Recently, Wei et al proposed a new $\mathcal{ID}$ based generalized signcryption scheme to obtain confidentiality or/and authenticity in big data, and claimed that their scheme is provably secure in standard model. Unfortunately, by giving substantial attack, we indicate that Wei et al scheme suffer from compromise of Private Key Generator ($\mathcal{PKG}$) master secret key and thus not hold the security of indistinguishability against adaptive chosen-ciphertext attacks ($\mathcal{IND}-\mathcal{CCA}$) and existential unforgeability against adaptive chosen-message attacks ($\mathcal{EUF}-\mathcal{CMA}$).

Key words: Cryptanalysis, Big Data, Confidentiality, Authenticity, Generalized signcryption, Standard model

1 Introduction

The identity is a natural link to a user, in his seminal paper Shamir [1] introduced the concept of Identity Based Cryptography ($\mathcal{IBC}$), where an entity's identity acts as public key and the corresponding private key is generated by a trusted third party entitled $\mathcal{PKG}$ to simplify public key certificate management. It is later on realized by Boneh and Franklin[2] using Weil pairing.

An alternative to sign-then-encrypt approach, Zheng [3] first proposed signcryption, a novel public key cryptographic primitive in Public Key Infrastructure ($\mathcal{PKI}$) having significant less computation and communication cost compare to sign-then-encrypt approach. Malone-Lee[4] extend the concept and designed an efficient ID based signcryption ($\mathcal{IBSC}$) scheme by merging the concepts of identity-based cryptography and signcryption.

However, in some cases of big data security, we sometimes need the confidentiality and authenticity separately and sometimes simultaneously. For exam-

[1] Corresponding Author e-mail: sahibzadanizam@yahoo.com

ple, we only care about the authenticity of statistic data from government, but the confidentiality and authenticity of sales data from companies. To achieve this special requirement, we can naively use three different schemes: a signature scheme, an encryption scheme, or a signcryption scheme costly in terms of implementation complexities, which makes it not suitable for big data. A novel primitive called Generalized Signcryption ($\mathcal{GSC}$) first proposed by Han [5] can adaptively work as a signature scheme, an encryption scheme, or a signcryption scheme with only one algorithm. Wang et al. [6] presented a security model and improved the scheme proposed in [5]. In 2008, Lal and Kushwah [7] proposed first ID based generalized signcryption ($\mathcal{IBGSC}$) scheme with a security model. However, Yu et al.[8] showed that Lal and Kushwah's security model is not complete, then they modified the security model and proposed their own scheme. Recently, Kushwah and Lal [9] simplified Yu et al.'s security model and proposed an efficient $\mathcal{IBGSC}$ scheme. Wei et al.[10] proposed a new $\mathcal{IBGSC}$ scheme for confidentiality or/and authenticity in big data, and claimed that their scheme is provably secure in standard model. However, in this paper,we analyzed and proved that Wei et al scheme is neither $\mathcal{IND}-\mathcal{CCA}$ nor $\mathcal{EUF}-\mathcal{CMA}$ secure in their defined security model.

2 Preliminaries

In this section, we briefly revise some of the definitions used in Wei et al $\mathcal{IBGSC}$ [10].

Let G and G_T be two multiplicative cyclic groups with same prime order q.

Definition 1 *A bilinear map* $e : G \times G \rightarrow G_T$ *satisfying the following properties:*

- Bilinearity: $\forall\ g_1, g_2 \in G$, and $a, b \in G_T; \hat{e}(g_1^a, bg_2^b) = \hat{e}(g_1, g_2)^{ab}$
- Non-degeneracy: $e(g_1, g_2)=1$
- Computable: The $e(g_1, g_2)$ can be efficiently computed

Definition 2 *Computational Diffie–Hellman Problem ($\mathcal{CDH}$): Let* G *be a group of prime order* q *and* g *be a generator of* G*. Given an instance* (g, g^a , g^b)*, it is intractable to compute* g^{ab} *.*

Definition 3 *$\mathcal{CDH}$ Assumption: If there is no t-time algorithm that can solve the $\mathcal{CDH}$ with probability at least ε , we say that the CDHP is (t,ε) hard in G.*

Definition 4 *Decisional bilinear Diffie–Hellman Problem ($\mathcal{DBDH}$): Given two groups* G *and* G_T*, a bilinear map* $e : G \times G \rightarrow G_T$ *and a generator*

g *of* G. *Given an instance (*g, g^a , g^b , g^c *) and* T $\in G_T$ *, it is intractable to decide whether* T= e(g, g)^{abc} .

Definition 5 *$\mathcal{DBDH}$ assumption: If there is no t-time algorithm that can solve the $\mathcal{DBDH}$ with probability at least ε ,we say that the $\mathcal{DBDH}$ is (t,ε) hard in G.*

3 Formal Framework of IBGSC Scheme

$\mathcal{IBGSC}$ scheme consists of three Probabilistic Polynomial Time *($\mathcal{PPT}$)* algorithms: *Setup;Ext*; $\mathcal{IBGSC}$ and one Deterministic Polynomial Time *($\mathcal{DPT}$)* algorithm: $\mathcal{IBGUSC}$.

Setup(1^λ)$\rightarrow$ (params; msk): It is a *($\mathcal{PPT}$)* algorithm that takes input security parameter k and returns the master key *msk* and system's public parameters *params*.

Ext(msk, u) $\rightarrow d_u$: It takes *(msk, u)* as input and generates the corresponding identity u private key d_u.

$\mathcal{IBGSC}$*(m,* u_a, u_b*)*$\rightarrow \sigma$: There are the following three situations:

We denote u_ϕ as the absence of the sender or the receiver, the sender's identity u_a and the receiver's identity u_b the message $m \in \mathcal{M}$ and signcrypted text $\sigma \in \mathcal{C}$. There are the following three situations:

- For encryption scheme, the $\mathcal{IBGSC}$ takes *(m,* u_ϕ*, ub)* as input and produces σ as output.
- For signature scheme, the $\mathcal{IBGSC}$ takes *(m,* u_a, u_ϕ *)* as input and produces the signature σ as output.
- For signcryption scheme, the $\mathcal{IBGSC}$ takes *(m,* u_a*,* u_b *)* as input and produces signcrypted text σ as output.

$\mathcal{IBGUSC}$ *(*σ*,* u_a*,* u_b*)* $\rightarrow$ *(m,* $\intercal$*,* $\perp$ *)*: There are the following three situations:

- For encryption scheme, the $\mathcal{IBGUSC}$ takes input (σ, u_ϕ, u_b) and generates m as output.
- For signature scheme, the $\mathcal{IBGUSC}$ takes input (σ, u_a, u_ϕ), and then checks If σ is valid, generates $\intercal$; otherwise, it generates $\perp$ as output.
- For signcryption scheme, the $\mathcal{IBGUSC}$ takes input (σ, u_a, u_b) and then checks If σ is valid, it produces message m ; otherwise $\perp$.

3.1 The $\mathcal{CCA}$ security model

In this section, we demonstrate the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$,taht guaranty the confidentiality of the message.

Setup: The challenger $\mathcal{C}$ runs the setup (1^λ) to generate systems' parameters and then forwards them to the adversary $\mathcal{A}$.

Phase 1: Following are the quires adaptively asked by $\mathcal{A}$:

- *Ext* $\mathcal{O}_{ext}$:Adversary $\mathcal{A}$ gives the identity u to $\mathcal{C}$ to compute private key d_u and returns back to $\mathcal{A}$
- $\mathcal{IBGSC}$ $\mathcal{O}_{ibgsc}$:$\mathcal{A}$ gives a chosen message m and identity keys u_a,u_b to $\mathcal{C}$. $\mathcal{C}$ returns value σ back to $\mathcal{A}$
- $\mathcal{IBGUSC}$ $\mathcal{O}_{ibgusc}$:$\mathcal{A}$ gives (σ, u_a, u_b) to $\mathcal{C}$ and $\mathcal{C}$ checks the validity of σ, as a result returns valid message to $\mathcal{A}$ else returns error symbol $\perp$.

Challenge:$\mathcal{A}$ chooses two messages of same size m_0, $m_1$and u_a^*,$\mathrm{u}_b^*(\neq \mathrm{u}_\varphi)$,(except asking the $\mathcal{O}_{ext}$ with input u_b^* previously), gives the instance (m_0,m_1,u_a^*,u_b^*) to $\mathcal{C}$. $\mathcal{C}$ generates a challenge σ^* using flips a coin b $\in \{1, 0\}$ for m_b^* and give it to the $\mathcal{A}$ finally.

Phase 2: $\mathcal{A}$ asks queries as in phase1 previously with input (σ^*, u_a^*, u_b^*),$\mathcal{O}_{ext}$,u_b^* except $\mathcal{O}_{ibgsc}$.

Guess: $\mathcal{A}$ produces a bit output $\acute{\mathrm{b}}$ of b. If the $\acute{\mathrm{b}}$=b then $\mathcal{A}$ wins the game. The wining probability of $\mathcal{A}$ in the said game is $Adv_{\mathcal{A}}^{CCA}\ (1^\lambda)=|Pr[b'=b]-\frac{1}{2}|$ and this scheme is said to be $\mathcal{CCA}$ secure if for all efficient adversaries $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{CCA}\ (1^\lambda)$ is negligible.

3.2 The EUF-CMA Security Model

The following $\mathcal{EUF}-\mathcal{CMA}$ game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ guarantees the existential unforgeability of the signature.

Setup: Identical to that in $\mathcal{CCA}$ security game.

Phase1 : Identical to that in $\mathcal{CCA}$ security game.

Forgery: On a message m^* , $\mathcal{A}$ produces a forgery (σ^* , u_a^* ($\neq u_\varphi$), u_b^*), where $\mathcal{A}$ has never asked $\mathcal{O}_{ibgsc}$ with input (m^* , u_a^* ($\neq u_\varphi$), u_b^*) and $\mathcal{O}_{ext}$ with input u_a before. $\mathcal{A}$ wins if (σ^* , u_a^* ($\neq u_\varphi$), u_b^*) is verified and valid. This scheme is said to be $\mathcal{EUFCMA}$ if the wining probability $Adv_{\mathcal{A}}^{CCA}\ (1^\lambda)$ of $\mathcal{A}$ in the said game is negligible.

4 Review of Wei et al $\mathcal{IBGSC}$ Scheme

In this section, we review Wei et al $\mathcal{IBGSC}$ for big data, consists of three $\mathcal{PPT}$ algorithms: *Setup; Ext;* $\mathcal{IBGSC}$ and one $\mathcal{DPT}$ algorithm: $\mathcal{IBGUSC}$.

Setup: Let G and G_T be two groups, e : G $\times$ G $\rightarrow$ G_T be an admissible bilinear map, $\mathcal{SIG}$=(G , *Sign Vrfy)* be one time signature, $\mathcal{SIG}.G(1^\lambda)$ can generate a signature and verification key pair *(ssk; svk)*. Let f(u) be the function, if u=$u_\phi$then *f(u)=0*; otherwise *f(u)= 1*. The *PKG* randomly chooses a secret $\alpha \in Z_q$ and computes $g_1 = g^\alpha$ It randomly chooses g_2 *ú,* $\tilde{m}'$, *v́* $\in G$ .and vector $U=u_i$, $M=\tilde{m}_j$ *and* $V=svk_k$ of length n_u , n_m *and* n_v respectively. Let λ be the security parameter, $H_1 : G_T \rightarrow \{0; 1\}^{n_m}$ and $H_2 : \{0; 1\}^* \rightarrow \{0; 1\}^{n_m}$ be two hash functions. It keeps the master key g_2^α secret and publishes system parameters (G, G_T, e, g, g_1, g_2, *ú,* $\tilde{m}'$, *v́*, U, M, V, H_1,H_2, *f(.))*

Ext: Let u be an identity of length n_u and *u[i]* be the *i-th* bit of u. Define $\mathcal{U} \subset$ {1,2,...n_u} to be the set of indices i such that u_i =*1*. To construct an identity *u's* private key d_u , the $\mathcal{PKG}$ randomly chooses a $r_u \in Z_q$ and computes d_u $=(d_{u1},\ d_{u2}\ )=(g_2^\alpha\ \ (u'\Pi_{\ i\in u}u_i\ )^{ru}\ , g^{r_u})$ then the private keys corresponding to identities u_a and u_b are

$d_a\ =(d_{a1},\ d_{a2}\ )=(g_2^\alpha\ (u'\Pi_{\ i\in u_a}u_i\ )^{ra}\ ,\ g^{r_a})$

$d_b\ =(d_{b1},\ d_{b2}\ )=(g_2^\alpha\ (u'\Pi_{\ i\in u_b}u_i\ )^{r_b}\ ,\ g^{r_b})$

$\mathcal{IBGSC}$: Let m$\in \{0,1\}^{n_m}$ be the message to be securely communicated, and the sender and the receiver's identities (u_a and u_b) respectively. Sender first runs $\mathcal{IG}.G(1^\lambda)$ to generate a signature and verification key pair *(ssk, svk)*, and randomly chooses two integers $r \in Z_q$; *ŕ*$\in Z_q$

- $\sigma_1 = g^r$
- $w = e(g_1,\ g_2)^r\ f(u_b)$
- $\sigma_2 = m \oplus H_1(w)\ f(u_b)$
- $\sigma_3 = (ú\Pi_{i\in ub}\ u_i)^r.f(u_b)$
- $\tilde{m} = H_2(m||svk)$
- $\sigma_4 = d_{a1}(\tilde{m}'\ \Pi_{\ j\in\mathcal{M}}\ \tilde{m}_j)^r\ \ d_{a1}(u'\ \Pi_{j\in ua}\ u_i)^{r'}\ f(u_a)$
- $\sigma_5 = d_{a2}\ (g)^{\acute{r}}\ f(u_a)$
- $\sigma_6 = (v\acute{\Pi}_{k\in v}\ svk_{_k})^r.f(u_b)$
- $\sigma_7 = SIG.Sign\ ((\sigma_1,\ \sigma_2, \sigma_3\ \sigma_4,\ \sigma_5,\ \sigma_6,), ssk).f(u_b)$
- $\sigma_8 = svk$

At last the sender sends $\sigma = (\sigma_1,\ \sigma_2, \sigma_3\ \sigma_4,\ \sigma_5,\ \sigma_6,\ \sigma_7,\ \sigma_8)$ to the receiver

(1) if $u_a = u_\varphi$ then *f(u_a)=0* and $\sigma = (\sigma_1, \sigma_2, \sigma_3\ 0, 0, \sigma_6, \sigma_7, \sigma_8)$ is a ciphertext
(2) if $u_b = u_\varphi$ then *f(u_b)=0* and $\sigma = (\sigma_1, \sigma_2, 0\ \sigma_4, \sigma_5, 0, 0, \sigma_8)$ is a signature
(3) if $u_a \neq u_\varphi$ and $u_b \neq u_\varphi$ and $\sigma = (\sigma_1,\ \sigma_2, \sigma_3\ \sigma_4,\ \sigma_5,\ \sigma_6,\ \sigma_7,\ \sigma_8)$ is a

signcryptext

$\mathcal{IBGUSC}$: Upon receiving σ , the receiver perform the following steps:

- If $\sigma_3 = \sigma_6 = \sigma_7 = 0$ then σ is a signature of the signature scheme. The receiver computes $\tilde{m}=H_2(\sigma_2||\sigma_8)$, and accepts the signature if $e(\sigma_4, g)=e(g_1, g_2)\ e(u'\Pi_{j\in\mathcal{M}}\ u_i, \sigma_5)\ e(\tilde{m}'\Pi_{j\in\mathcal{M}}\ \tilde{m}_j, \sigma_1)$ otherwise, the receiver perform the following steps.
- if $\mathcal{SIG}.Sign\ ((\sigma_1, \sigma_2, \sigma_3\ \sigma_4, \sigma_5, \sigma_6, \sigma_7), \sigma_8)=1,\ e(\sigma_1, u'\Pi_{i\in u_b}\ u_i)\neq e(g, \sigma_3)$ or $e(\sigma_3, v'\Pi_{k\in v}\ svk_k)\neq e(g, \sigma_6)$ the receiver returns an error $\perp$ otherwise computes $w=\frac{e(d_{b1}, \sigma_1)}{e(d_{b2}, \sigma_3)}$ and $m = \sigma_1 \oplus H_1(w)$
- If $\sigma_4 = \sigma_5 = 0$, then σ is a ciphertext of the encryption scheme. The receiver accepts the message; otherwise
- σ is a signcrypted text of the signcryption scheme, the receiver additionally has to check the authenticity of m. The receiver computes $\tilde{m} = H_2(m||\sigma_8)$, and accepts the message if $e(\sigma_4, g)=e(g_1, g_2)e(u'\Pi_{j\in\mathcal{M}}\ u_i, \sigma_5)\ e(\tilde{m}'\Pi_{j\in\mathcal{M}}\ \tilde{m}_j, \sigma_1)$

5 Cryptanalysis of Wei et al.'s Scheme

In this section, we disprove Wei et al. [10] claims, that their scheme is both semantically secure and existentially unforgeable; by giving three concrete attacks.

5.1 $\mathcal{PKG}$ Compromise Attack

We launch an attack on Wei et al.'s scheme such that given a σ generated by the sender, $\mathcal{A}$ can derive the $\mathcal{PKG}$ master secret key, leading to compromise of $\mathcal{PKG}$ and hence the whole system is compromised.

Setup: The $\mathcal{C}$ runs setup (1^λ) to generate systems parameters $(G;\ G_T;\ e,\ g;\ g_1\ ;\ g_2\ ;\ \acute{u},\ \tilde{m}'\ ,\ \acute{v},\ U\ ,\ M,\ V,\ H_1, H_2\ , f(.))$ and then forwards them to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ issues a signcryption query by submitting a messages m and $u_a\ , u_b$ with $u_a\ \neq\ u_\varphi$,and set $\tilde{m}' = (g)$, $\tilde{m}_j = (g)^{\tilde{m}_{j'}}$, $u' = (g)^{u_j}$ and $u_i = (g)^{u_{i'}}$ (except asking the $\mathcal{O}_{ext}$ with input u_a previously). At last $\mathcal{C}$ generate and sends $\sigma = (\sigma_1,\ \sigma_2, \sigma_3\ \sigma_4,\ \sigma_5,\ \sigma_6,\ \sigma_7,\ \sigma_8)$ to $\mathcal{A}$. $\mathcal{A}$ can compute $\mathcal{PKG}$ master secret key g_2^α as:

$$
\begin{aligned}
&\frac{\sigma_4}{(\sigma_1)^{(\tilde{m}+\sum_{j\in\mathcal{M}}\tilde{m}'_j)}\ (\sigma_5)^{(u+\sum_{j\ \in\ ua}u'_i)}}\\
=\ &\frac{d_{a1}\ (\tilde{m}'\prod_{j\ \in\ M}\tilde{m}_j)^r(u'\prod_{j\in ua}u_i)^{r'}}{(g^r)^{(\tilde{m}+\sum_{j\in\mathcal{M}}\tilde{m}'_j)}\ (g^{ra}.g^{\acute{r}})^{(u+\sum_{j\ \in\ ua}u'_i)}}\\
=\ &\frac{d_{a1}(\tilde{m}'\prod_{j\in\mathcal{M}}\tilde{m}_j)^r(u'\prod_{j\in ua}u_i)^{r'}}{(g)^{(\tilde{m}+\sum_{j\in\mathcal{M}}\tilde{m}'_j)^r}.(g)^{(u+\sum_{j\in ua}u'_i)^{(ra+\acute{r})}}}\\
&\frac{d_{a1}(\tilde{m}'\prod_{j\in\mathcal{M}}\tilde{m}_j)^r(u'\prod_{j\in ua}u_i)^{r'}}{(g)^{\tilde{m}}\Pi_{j\in M}(g)^{\tilde{m}_{j'}})^r.((g)^u\Pi_{j\in ua}(g)^{u_{i'}})^{(ra+\acute{r})}}\\
=\ &\frac{d_{a1}(\tilde{m}'\prod_{j\in\mathcal{M}}\tilde{m}_j)^r(u'\prod_{j\in ua}u_i)^{r'}}{(\tilde{m}'\Pi_{j\in\mathcal{M}}\tilde{m}_j)^r(u'.\Pi_{j\in ua}\ u_i)^{(ra+\acute{r})}}\\
=\ &\frac{d_{a1}(\tilde{m}'\prod_{j\in\mathcal{M}}\tilde{m}_j)^r(u'\prod_{j\in ua}u_i)^{r'}}{(\tilde{m}'\Pi_{j\in\mathcal{M}}\tilde{m}_j)^r(u'.\Pi_{j\in ua}\ u_i)^{\acute{r}}(u'.\Pi_{j\in ua}\ u_i)^{ra}}\\
=\ &\frac{d_{a1}}{(u'.\Pi_{j\in ua}\ u_i)^{ra}}\\
=&\frac{g_2^{\alpha}\ \ (u'\Pi_{\ i\in u_a}u_i\ )^{ra}}{(u'.\Pi_{j\in ua}\ u_i)^{ra}}\\
=&\ g_2^{\alpha}
\end{aligned}
$$

With $\mathcal{PKG}$ master key g_2^{α} , $\mathcal{A}$ can certainly computes the sender and the receiver's private keys d_a d_b and can signcrypt on behalf of the sender and unsigncrypt on the behalf of the receiver and thus can always win $\mathcal{IND}-\mathcal{CCA}$ and $\mathcal{EUF}-\mathcal{CMA}$ games.

5.2 Attack Against Semantic Security

Wei et al. [10] claims that their scheme is semantically secure even in the standard model. Unfortunately, this is not true, since there exists a polynomial time $\mathcal{A}$ which can always win the below game as:

Setup: $\mathcal{C}$ runs the setup (1^{λ}) to generate systems parameters (G; G_T ; e, g, g_1, g_2, $\acute{u}$, $\tilde{m}'$, $\acute{v}$, U , M, V, H_1,H_2 ,,$f(.)$) and then forwards them to $\mathcal{A}$.

Phase 1: $\mathcal{A}$ needs not issue any query.

Challenge:$\mathcal{A}$ first launches attack on $\mathcal{PKG}$ and obtains master secret key g_2^{α} of $\mathcal{PKG}$. $\mathcal{A}$ randomly chooses two random number r_{a^*} $r_{b^*}\in Z_q$ and constructs the private key of user having identities u_a^*,u_b^* as:

d_{a^*} $=(d_{a^*1}\ ,\ d_{a^*2}\ )=(g_2^{\alpha}\ \ (u'\Pi_{\ i\in u_a}u_i\ )^{r_{a^*}}\ , g^{r_{a^*}})$

$d_{b^*} = (d_{b^*1}\ ,\ d_{b^*2}\ ) = (g_2^{\alpha}\ \ (u' \Pi_{\ i \in u_b} u_i\ )^{r_{b^*}}\ , g^{r_{b^*}})$

$\mathcal{A}$ chooses two messages of same size m_0, $m_1$and u_a^*,$u_b^*(\neq u_\varphi)$,(except asking the $\mathcal{O}_{ext}$ with input u_b^* previously), gives the instance (m_0,m_1,u_a^*,u_b^*) to $\mathcal{C}$. $\mathcal{C}$ flips a coin $b \in \{\ 1\ ,\ 0\ \}$ and for m_b^* generates a challenge σ^*as following: and gives σ^* to the $\mathcal{A}$. Recall that $\mathcal{A}$'s goal is to correctly guess the value b. $\mathcal{C}$ first runs $\mathcal{SIG}.G(1^\lambda)$ to generate a signature and verification key pair *(ssk; svk)*, and randomly chooses two integers $r \in Z_q$; $\acute{r} \in Z_q$and computes σ^* .

- $\sigma_1^* = g^{r*}$
- $w^* = e(g_1,\ g_2)^{r*}\ f(u_{b^*}\ )$
- $\sigma_2^* = m_b^* \oplus H_1(w)\ f(u_{b^*}\ )$
- $\sigma_3^* = (\acute{u} \Pi_{i \in ub}\ u_i)^{r*}.f(u_{b^*}\ )$
- $\tilde{m}^* = H_2(m_b^*\ ||\ svk\ )$
- $\sigma_4 = d_{a^*1}(\tilde{m}^{*\prime}\ \Pi_{\ j \in \mathcal{M}}\ \tilde{m}_j^*)^r\ d_{a1}(u'\ \Pi_{j \in ua}\ u_i)^{r*\prime}\ f(u_{b^*}\ )$
- $\sigma_5 = d_{a^*2}\ (g)^{r*\prime}\ f(u_{b^*}\ )$
- $\sigma_6^* = (\acute{v} \Pi_{k \in v}\ svk_{\ k})^{r*}.f(u_{b^*}\ )$
- $\sigma_7^* = \mathcal{SIG}.Sign\ ((\sigma_1^*\ ,\ \sigma_2^*\ ,\sigma_3^*\ \ \sigma_4^*\ ,\ \sigma_5^*\ ,\ \sigma_6^*\ ), ssk).f(u_{b^*}\ )$
- $\sigma_8^* = svk$

At last $\mathcal{C}$ sends $\sigma^* = (\sigma_1^*\ ,\ \sigma_2^*\ ,\sigma_3^*\ ,\sigma_4^*\ ,\ \sigma_5^*\ ,\ \sigma_6^*\ ,\ \sigma_7^*\ ,\ \sigma_8^*\ )$ to $\mathcal{A}$

Phase 2: $\mathcal{A}$ has private keys of the sender and the receiver, hence computes $w = \frac{e(d_{b1},\ \sigma_1)}{e(d_{b2},\ \sigma_3)}$, further $\mathcal{A}$, surely computes the underlying message $m_b^* = \sigma_1 \oplus H_1(w)$ and knows the value b, and thus wins the game. Therefore, Wei et al.'s scheme is semantically insecure against chosen-ciphertext attacks.

5.3 Attack Against Existential Unforgeability

We disprove the Wei et al.'s claim that their scheme is not existentially unforgeable, as $\mathcal{A}$ can certainly generate a valid generalized signcrypted text and there exists a $\mathcal{PPT}$ $\mathcal{A}$ which can always win the following $\mathcal{EUF} - \mathcal{CMA}$ game between $\mathcal{C}$ and $\mathcal{A}$ as:

Setup: Identical to that in $\mathcal{CCA}$ security game.

Phase1: Identical to that in $\mathcal{CCA}$ security game.

Forgery: $\mathcal{A}$ first launches attack on $\mathcal{PKG}$ and obtains master secret key of $\mathcal{PKG}$. $\mathcal{A}$ randomly chooses two random number $r_{a^*}\ r_{b^*} \in Z_q$ and constructs the private key an identity u_a^*,u_b^* as:

$d_{a^*} = (d_{a^*1}\ ,\ d_{a^*2}\ ) = (g_2^{\alpha}\ \ (u' \Pi_{\ i \in u_a} u_i\ )^{r_{a^*}}\ , g^{r_{a^*}})$

$d_{b^*} = (d_{b^*1}\ ,\ d_{b^*2}\ ) = (g_2^{\alpha}\ \ (u' \Pi_{\ i \in u_b} u_i\ )^{r_{b^*}}\ , g^{r_{b^*}})$

On a message m^* , $\mathcal{A}$ certainly produces a forgery $(\sigma^*\ ,\ \mathrm{u}_a^*\ (\neq u_\varphi\ ),\ \mathrm{u}_b^*\ )$, as $\mathcal{A}$ has private keys of the sender and the receiver, where $\mathcal{A}$ has never asked $\mathcal{O}_{ibgsc}$ with input $(m^*\ ,\ \mathrm{u}_a^*\ (\neq u_\varphi\ ),\ \mathrm{u}_b^*\ )$ and $\mathcal{O}_{ext}$ with input u_a before. $\mathcal{A}$ certainly wins as $(\sigma^*\ ,\ \mathrm{u}_a^*\ (\neq u_\varphi\ ),\ \mathrm{u}_b^*\ )$ is verified and valid, and thus always wins the game.

6 Conclusion

In this paper, we analyzed Wei et al [10] scheme. The formal model, security model and review are presented. The security attacks are launched on the mentioned scheme that result security flaws as: First, the master secret key of $\mathcal{PKG}$ can be compromised that lead to system insecurity. Second, it is neither $\mathcal{IND} - \mathcal{CCA}$ secure nor $\mathcal{EUF} - \mathcal{CMA}$ secure in their defined standard security model.

References

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

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

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

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

[5] 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.

[6] X. A. Wang, X. Yang, and J. Zhang, "Provable secure generalized signcryption," J. Comput., vol. 5, pp. 807–814, 2010.

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

[8] G. Yu, X. Ma, Y. Shen, and W. Han, "Provable secure identity based generalized signcryption scheme," Theor. Comput. Sci., vol. 411, pp. 3614–3624, 2010.

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

[10] G. Wei, J. Shao, Y. Xiang, P. Zhu, and R. Lu, "Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption," In Press, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.05.034