Article

Cryptanalysis of an Authentication Scheme Using an Identity Based Generalized Signcryption

Abdul Waheed ^{1,2,*}, Arif Iqbal Umar ^{1,†}, Nizamud Din ^{3,†}, Noor Ul Amin ^{1,†},
Saleem Abdullah ^{4,†} and Poom Kumam ^{5,†}

¹ Department of Information Technology, Hazara University, Mansehra 21120, KP, Pakistan

² Department of Computer Science, IQRA National University, Peshawar 25124, KP, Pakistan

³ Department of Computer Science, University of Chitral, Chitral 17200, KP, Pakistan

⁴ Department of Mathematics, AWKUM University, Mardan 23200, KP, Pakistan

⁵ Department of Mathematics, King Mungkut's University of Technology Thonburi, Bangkok 10140, Thailand

* Correspondence: abdul@netlab.snu.ac.kr

† These authors contributed equally to this work.

Received: 7 May 2019; Accepted: 30 July 2019; Published: 24 August 2019

Abstract: Secure data transmission is a challenging issue in modern data communication. ID based generalized signcryption is a cost effective security primitive which provides authentication or confidentiality, or jointly confidentiality and authentication. Wei's proposed an ID based generalized signcryption scheme for authentication and confidentiality of big data in a standard model, claiming that their scheme holds the security of indistinguishability against adaptive chosen-ciphertext attacks and existential unforgeability against adaptive chosen message attacks. In this paper, we analyzed Wei's scheme by launching security attacks on the scheme to check its validity. As a result, it became clear and proved that the master secret key generated in the scheme is compromisable. Similarly, the mentioned scheme does not hold the security of indistinguishability against adaptive chosen-ciphertext attacks and existential unforgeability against adaptive chosen message attacks. Consequently, Wei's schemes is prone to attacks and is insecure.

Keywords: cryptanalysis; encryption; digital signature; malicious-but-passive; Key Generation Center (KGC); ID based generalized signcryption; security model; standard model

1. Introduction

In 1984, Shamir [1] introduced the concept of Identity Based Cryptography (IBC) for the first time, where an identity is used as a public key and the corresponding private key is generated by a trusted third party entitled PKG. The objective of identity based cryptography is to simplify public key certificate management in public key cryptography. It was later on improved by Boneh and Franklin [2].

To overcome the drawbacks of the traditional cryptographic approaches, Zheng proposed a novel cryptographic primitive called signcryption [3], which is an alternative to the signature then encryption approach with significantly less computation and communication cost. In 2002, Malone-Lee [4] merged identity-based cryptography with signcryption and designed a new ID based signcryption (IBSC) scheme. This IBSC scheme [4] provides foundation for some other identity based signcryption and its variant [5–14].

In big data security, we need the data confidentiality and data authentication separately and in some cases we use both simultaneously. Likewise, authentication security approach is used by government sectors to authenticate statistical data. And different companies use two security attributes

like confidentiality and authentication to both authenticate and keep confidential sales related data. This type of operations require generalized signcryption (GSC) approach proposed by Han et al. [15].

GSC works in three different modes such as; pure encryption mode, pure signature mode and signcryption mode and can be used for data confidentiality, data authenticity or both respectively. For the requirement of a single security parameter either data confidentiality or data authentication, signcryption is not feasible due to greater computational cost and algorithmic complexities. Thus, in this case, signcryption scheme is not suitable for big data and other resources constraint environment.

Now, to fulfill the multi option security requirements of big data we refer the use of generalized signcryption a flavor of simple signcryption suitable for big data and other resources constraints environment instead of signcryption. Wang et al. [16] improved Han et al. [15] scheme and presented a new security model for generalized signcryption. In 2008, Lal and Kushwah [17] contributed the first ID based generalized signcryption (IBGSC) scheme with a new security model. Later on Yu et al. [18] proved that Lal and Kushwah's security model was not fulfilling the basic security needs, and improved the existing security model with minimal computational cost. In 2011, Kushwah and Lal [19] also simplified same Yu et al. [18] security model and proposed a new efficient IBGSC scheme. In 2019, Waheed et al. [20] analyzed the Zhou et al. [21] certificateless generalized scheme and proposed improved scheme comparatively more secure with the same cost.

Wei et al. [22] proposed a novel IBGSC scheme for pure encryption or pure signature to ensure the confidentiality and authenticity as per requirements in big data with the claim that this scheme is provably secure in standard model. However, in this paper, we analyze Wei's authentication scheme and prove that Wei's scheme is prone to attacks and neither IND-CCA nor EUF-CMA secure in the standard model. Therefore we use cryptanalysis approach to analyze and check the Wei's authentication scheme security and vulnerabilities.

Cryptanalysis approach uses mathematical formulas to search vulnerabilities of an algorithm to prove security limitations or it decrypts ciphertext without knowing session's key or key related information. Figure 1 reflects the cryptanalysis approach over a simple signcryption.

Figure 1. Cryptanalysis of a signcryption scheme.

2. Preliminaries

This section of the paper describes definitions used in Wei's authentication scheme IBGSC [22]. Let us assume that $\mathbb{G}$ and $\mathbb{G}_T$ be the two cyclic multiplicative groups of order q .

Definition 1. A bilinear map such as: $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, where a bilinear map satisfies the following properties as:

- **Bi-linearity:** For all g_1 and $g_2 \in \mathbb{G}$, and $x, y \in \mathbb{G}_T$, where $\hat{e}(g_1^x, g_2^y) = \hat{e}(g_1, g_2)^{xy}$.
- **Computability:** The $\hat{e}(g_1, g_2)$ is efficiently computable.
- **Non-degeneracy:** $\hat{e}(g_1, g_2) = 1$.

Definition 2. Computational Diffie-Hellman (CDH) Problem: Let g be a generator of multiplicative group $\mathbb{G}$ of prime order q and it is intractable to compute g^{xy} if input (g, g^x, g^y) is given.

Definition 3. Computational Diffie-Hellman (CDH) Assumption: We can say CDH is (t, ζ) hard in $\mathbb{G}$ if any t -time algorithm can not solve CDH with at least ζ probability.

Definition 4. Decisional Bi-linear Diffie-Hellman (DBDH) Problem: Let $\mathbb{G}$ and $\mathbb{G}_T$ have two groups, a bilinear map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, having generator g of group $\mathbb{G}$, such that input (g, g^x, g^y, g^z) is given and $T \in \mathbb{G}_T$, it is also difficult to define $T = \hat{e}(g, g)^{xyz}$.

Definition 5. Decisional Bi-linear Diffie-Hellman (DBDH) assumption: We can say DBDH is (t, ζ) hard in $\mathbb{G}$ if any t -time algorithm can not solve DBDH with at least ζ probability.

2.1. IBGSC Formal Framework

IBGSC scheme consists of three Probabilistic Polynomial Time (PPT) algorithms titled as; Setup; Ext; IBGSC and IBGUSC a Deterministic Polynomial Time (DPT) algorithm.

- **Setup** $(1^\lambda) \mapsto (params; msk)$:- A PPT algorithm takes security parameter k and returns the master key (msk) and public parameters $(params)$.
- **Ext** $(msk; u) \mapsto d_u$:- It takes $(msk; u)$ to generate identity u and private key d_u .
- **IBGSC** $(m; u_a; u_b) \mapsto \sigma$:- Sender or receiver absence denoted by u_ϕ , sender's and receiver identities denoted by u_a, u_b respectively, message denoted by $m \in \mathcal{M}$ and signcrypted text denoted by $\sigma \in \mathcal{C}$.

Further three situations are as:

1. In pure encryption mode, the IBGSC takes (m, u_ϕ, u_b) as input and produces σ as output in the absence of sender private key.
 2. In pure signature mode, the IBGSC collects (m, u_a, u_ϕ) and produces the signature σ as output in the absence of receiver private key.
 3. In signcryption mode $(sign + enc)$, the IBGSC collects (m, u_a, u_b) and produces signcrypted text σ .
- **IBGUSC** $(\sigma, u_a, u_b) \mapsto (m, \top, \perp)$:- Output of this algorithm depends on three different situations:
 1. In pure encryption mode, on receiver end IBGUSC collects input (m, u_ϕ, u_b) , and generates m as output.
 2. In pure signature mode, on receiver end IBGUSC collects input (m, u_a, u_ϕ) , and checks σ validity, generates $\top$; else generates $\perp$ as output.
 3. In signcryption mode $(sign + enc)$, on receiver end IBGUSC collects input (m, u_a, u_b) , and then checks validity of σ , it produces message m , else $\perp$.

2.2. The CCA Security Model

This section of the paper defines CCA security model to check the data confidentiality. Adversary A and Challenger C played a game that guarantee the confidentiality of the message.

Setup:- In this stage challenger C runs setup algorithm with (1^λ) and send to A to generate system's parameters.

Phase 01:- A asked following queries adaptively;

- **Ext $\mathcal{O}_{ext}$:-** After receiving identity u , challenger C calculate private key d_u and returns back to A.
- **IBGSC $\mathcal{O}_{ibgsc}$:-** A gives a chosen message m and identities u_a, u_b to C and in response C returns value σ to A.
- **IBGUSC $\mathcal{O}_{ibgusc}$:-** A sends (σ, u_a, u_b) to C and C first checks σ validity, and returns valid message to A or returns error symbol $\perp$.

Challenge:- A chooses two messages (m_0, m_1) with same size and $u_a^*, u_b^* (\neq u_\phi)$, (except to ask $\mathcal{O}_{ext}$ for input u_b^* previously), and (m_0, m_1, u_a^*, u_b^*) forward to C. C generates a challenge σ^* using flips a coin $b \in \{1, 0\}$ for m_b^* and finally gives it to A back.

Phase 02:- A asks queries as practiced in phase 1st using input (σ^*, u_a^*, u_b^*) , $\mathcal{O}_{ext}, u_b^*$ except $\mathcal{O}_{ibgsc}$.

Guess:- A produces output ρ' of ρ and compares if $\rho' = \rho$ then A wins the game. The winning probability of A in this game is $Adv_A^{CCA}(1^\lambda) = |Pr[\rho' = \rho] - \frac{1}{2}|$ and thus the scheme is to be CCA secured against all efficient adversaries A, and advantages $Adv_A^{CCA}(1^\lambda)$ will be considered negligible.

2.3. The EUF-CMA Security Model

This section of the paper define security model to authenticate message contents. Using following game between challenger C and adversary A make sure the existential unforgeability of message signature.

Setup:- This step same as CCA security game.

Phase 01:- Like CCA security game.

Forgery:- On a message m^* , A produces a forgery $(\sigma^*, u_a^* (\neq u_\phi), u_b^*)$, where A has never asked $\mathcal{O}_{ibgsc}$ for input $(m^*, u_a^* (\neq u_\phi), u_b^*)$ and $\mathcal{O}_{ext}$ for input u_a before. A wins game if $(\sigma^*, u_a^* (\neq u_\phi), u_b^*)$ is valid and verified. The scheme will be EUF-CMA secure if the winning probability $Adv_A^{CCA}(1^\lambda)$ of A in the game is negligible.

3. Review of Wei's IBGSC Scheme

This section, presents review of Wei's IBGSC scheme for big data, which consists of three PPT algorithms such as: Setup; Ext; IBGSC and one DPT algorithm is IBGUSC.

Setup:- Let $\mathbb{G}$ and $\mathbb{G}_T$ be two groups, $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a bilinear map, $SIG = (\mathbb{G}, Sign, Vrfy)$ be a one time signature, $SIG \cdot \mathbb{G}(1^\lambda)$ used to generate a signature and verification key pair $(ssk; svk)$. Let $f(u)$ be a function, if $u = u_\phi$ then $f(u) = 0$, otherwise $f(u) = 1$. The PKG chooses a secret value $\alpha \in \mathbb{Z}_q$ randomly and then computes $g_1 = g^\alpha$. It also randomly chooses $g_2 u', \tilde{m}', v' \in \mathbb{G}$, vector $U = u_i, M = \tilde{m}_j, V = svk_k$ of length n_u, n_m and n_v respectively. Let λ be security parameter, $H_1 : \mathbb{G}_T \rightarrow (0; 1)^{n_m}$ 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 $(\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, u', \tilde{m}', v', U, M, V, H_1, H_2, f(\cdot))$.

Ext:- Let u be the length of n_u , where $u[i]$ be the i -th bit of u . Let us define $\mathcal{U}$, which is a subset $\{1, 2, \dots, n_u\}$ such that $u[i] = 1$. To construct an identity u 's private key d_u , the PKG chooses an $r_u \in \mathbb{Z}_q$ randomly and computes $d_u = (d_{u1}, d_{u2}) = (g_2^\alpha (u' \prod_{i \in \mathcal{U}} u_i)^{r_u}, g^{r_u})$. The identities u_a and u_b private keys are: $d_a = (d_{a1}, d_{a2}) = (g_2^\alpha (u' \prod_{i \in u_a} u_i)^{r_a}, g^{r_a})$ $d_b = (d_{b1}, d_{b2}) = (g_2^\alpha (u' \prod_{i \in u_b} u_i)^{r_b}, g^{r_b})$.

IBGSC:- Let message $m \in \{0, 1\}^{n_m}$, sender and the receiver's identities (u_a and u_b) securely communicated. Sender runs the algorithm $SIG \cdot \mathbb{G}(1^\lambda)$ to generate signature and verification key pair $(ssk; svk)$, and then chooses two integers $r \in \mathbb{Z}_q; r' \in \mathbb{Z}_q$ randomly.

- $\sigma_1 = g^r$

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

At the end 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 signcrypted text.

IBGUSC:- After collecting σ , receiver of message goes through the following stages:

1. If $\sigma_3 = \sigma_6 = \sigma_7 = 0$ mean message σ comprises upon signature contents of the pure signature mode. The message receiver computes $\tilde{m} = H_2(\sigma_2 || \sigma_8)$ then verifies and accepts signature if $\hat{e}(\sigma_4, g) = \hat{e}(g_1, g_2) \hat{e}(u' \Pi_{j \in \mathcal{M}} u_i, \sigma_5) \hat{e}(\tilde{m}' \Pi_{j \in \mathcal{M}} \tilde{m}_j, \sigma_1)$; otherwise, the receiver goes through the following algorithmic steps.
2. If $\text{SIG} \cdot \text{Verify}(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8) = 1$, $\hat{e}(\sigma_1, u' \Pi_{i \in ub} u_i) \neq \hat{e}(g, \sigma_3)$ or $\hat{e}(\sigma_3, v' \Pi_{k \in v} svk_k) \neq \hat{e}(g, \sigma_6)$ returns error $\perp$; otherwise computes $w = \frac{e(d_{b1}, \sigma_1)}{e(d_{b2}, \sigma_3)} \sigma_3$ and $m = \sigma_1 \oplus H_1(w)$.
3. If $\sigma_4 = \sigma_5 = 0$, mean σ is a ciphertext of pure encryption mode. The receiver accepts the message contents, otherwise.
4. σ is a signcrypted text of the signcryption mode ($sign + enc$), in this case the message receiver checks message m authenticity with the encryption additionally. The receiver also computes $\tilde{m} = H_2(m || \sigma_8)$, accepts message if $\hat{e}(\sigma_4, g) = \hat{e}(g_1, g_2) \hat{e}(u' \Pi_{j \in \mathcal{M}} u_i, \sigma_5) \hat{e}(\tilde{m}' \Pi_{j \in \mathcal{M}} \tilde{m}_j, \sigma_1)$.

4. Cryptanalysis of Wei's Authentication Scheme

In this section of the paper, we disprove the Wei's authentication scheme [22], after launching following three concrete attacks.

4.1. PKG Compromise Attack

We launch an attack on Wei's authentication scheme such that given σ generated by the sender, A can derive the PKG master secret key, leading to compromise PKG and thus the whole system is compromised.

Setup:- The C runs setup (1^λ) to generate systems parameters $(\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, u' \tilde{m}', v', U, M, V, H_1, H_2, f(\cdot))$ and then forward to A.

Phase 01:- A put a signcryption query by submitting a messages m and u_a, u_b with $u_a \neq u_\varphi$, and set $\tilde{m}' = g^{\tilde{m}}, \tilde{m}_j = g^{\tilde{m}_j'}, u' = g_j^u$ and $u_i = g^{u_i'}$ (except asking the $\mathcal{O}_{ext}$ for input u_a previously). C generates $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6, \sigma_7, \sigma_8)$ and send to A. A can compute PKG master secret key g_2^α as:

$$\begin{aligned}
& \frac{\sigma_4}{(\sigma_1)^{(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)} (\sigma_5)^{(u + \sum_{j \in ua} u'_i)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in M} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'} f(u_a)}{(g^r)^{(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)} (d_{a2} g^f f(u_a))^{(u + \sum_{j \in ua} u'_i)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in M} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'} f(u_a)}{(g^r)^{(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)} (g^{ra} g^f f(u_a))^{(u + \sum_{j \in ua} u'_i)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in M} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{(g^r)^{(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)} (g^{ra} g^f)^{(u + \sum_{j \in ua} u'_i)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in M} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{g^{r(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)} (g^{ra+f})^{(u + \sum_{j \in ua} u'_i)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in \mathcal{M}} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{(g)^{(\tilde{m} + \sum_{j \in \mathcal{M}} \tilde{m}'_j)^r} \cdot (g)^{(u + \sum_{j \in ua} u'_i)(ra+f)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in \mathcal{M}} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{(g)^{\tilde{m} \prod_{j \in M} (g)^{\tilde{m}'_j r} \cdot ((g)^u \prod_{j \in ua} (g)^{u'_i})^{(ra+f)}}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in \mathcal{M}} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{(\tilde{m}' \prod_{j \in \mathcal{M}} \tilde{m}_j)^r (u' \cdot \prod_{j \in ua} u_i)^{(ra+f)}} \\
&= \frac{d_{a1} (\tilde{m}'_{j \in \mathcal{M}} \tilde{m}_j)^r (u'_{j \in ua} u_i)^{r'}}{(\tilde{m}' \prod_{j \in \mathcal{M}} \tilde{m}_j)^r (u' \cdot \prod_{j \in ua} u_i)^f (u' \cdot \prod_{j \in ua} u_i)^{ra}} \\
&= \frac{d_{a1}}{(u' \cdot \prod_{j \in ua} u_i)^{ra}} \\
&= \frac{g_2^\alpha (u' \prod_{i \in ua} u_i)^{ra}}{(u' \cdot \prod_{j \in ua} u_i)^{ra}} \\
&= g_2^\alpha.
\end{aligned}$$

With PKG master key g_2^α , A can certainly compute 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 IND-CCA and EUF-CMA games.

4.2. Attack on Semantic Security

Wei et al. [22] claim that the scheme is also secure semantically in standard model. But there exists a polynomial time adversary A which has always high probability to win the game as:

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

Phase 01:- A does not need to issue any query.

Challenge:- A first launches attack on PKG and obtain master secret key g_2^α . A randomly chooses two numbers $r_{a^*}, r_{b^*} \in Z_q$ and computes private keys of user having identities u_a^*, u_b^* as: $d_{a^*} = (d_{a^*1}, d_{a^*2}) = (g_2^\alpha (u' \prod_{i \in ua} u_i)^{r_{a^*}}, g^{r_{a^*}})$, $d_{b^*} = (d_{b^*1}, d_{b^*2}) = (g_2^\alpha (u' \prod_{i \in ub} u_i)^{r_{b^*}}, g^{r_{b^*}})$

A chooses two messages of same size m_0, m_1 with identities $u_a^*, u_b^* (\neq u_\phi)$, (except asking the $\mathcal{O}_{ext}$ for input u_b^* previously), and send (m_0, m_1, u_a^*, u_b^*) to C. Challenger C flips coin $b \in \{1, 0\}$ and for m_b^* generates a challenge σ^* using following steps and then forward σ^* to A. Recall that A's goal is to correctly guess the value b . C runs SIG. $\mathbb{G}(1^\lambda)$ to compute $(ssk; svk)$ for sign and verification keys pair, chooses two integers $r \in Z_q, r' \in Z_q$ randomly and then computes σ^* .

- $\sigma_1^* = g^{r^*}$
- $w^* = e(g_1, g_2)^{r^*} \cdot f(u_b^*)$

- $\sigma_2^* = m_b^* \oplus H_1(w) \cdot f(u_b^*)$
- $\sigma_3^* = (u' \Pi_{i \in u_b} u_i)^{r^*} \cdot f(u_b^*)$
- $\tilde{m}^* = H_2(m_b^* || svk)$
- $\sigma_4^* = d_a^* 1 (\tilde{m}^* \Pi_{j \in \mathcal{M}} \tilde{m}_j^*)^r d_{a1} (u' \Pi_{j \in u_a} u_i)^{r^*} \cdot f(u_b^*)$
- $\sigma_5^* = d_a^* 2 (g)^{r^*} \cdot f(u_b^*)$
- $\sigma_6^* = (v \Pi_{k \in v} svk_k)^{r^*} \cdot f(u_b^*)$
- $\sigma_7^* = \text{SIG} \cdot \text{Sign}(\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*), ssk) \cdot f(u_b^*)$
- $\sigma_8^* = svk$

At the end C sends $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*, \sigma_7^*, \sigma_8^*)$ to A.

Phase 02:- 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 A, computes the underlying message $m_b^* = \sigma_1^* \oplus H_1(w)$ and knows the value b , and thus wins the game. After above computation it has proved that existing scheme is semantically insecure against chosen-ciphertext attack.

4.3. Attack against Existential Unforgeability

We disprove Wei's authentication scheme and proved that A can certainly generate a valid generalized signcrypted text and there exists an PPT Adversary can always win the following EUF-CMA game between C and A as:

Setup:- Like CCA security game.

Phase 01:- Like CCA security game.

Forgery:- A first launches attack on PKG, and obtains master secret key of PKG and choose two random numbers $r_{a^*}, r_{b^*} \in \mathbb{Z}_q$ with identities u_a^*, u_b^* respectively 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^* , A certainly produces a forgery $(\sigma^*, u_a^* (\neq u_\varphi), u_b^*)$, as A has private keys of the sender and the receiver, and never asked before from $\mathcal{O}_{ibgsc}$ for input $(m^*, u_a^* (\neq u_\varphi), u_b^*)$ and $\mathcal{O}_{ext}$ for input u_a before. A computes $(\sigma^*, u_a^* (\neq u_\varphi), u_b^*)$ if verified and valid, thus always wins the game.

5. Conclusions

Wei et al. presented an authenticated identity based generalized signcryption scheme for big data. In this paper, we have analyzed the mentioned scheme using a formal model and security model. Security attacks were launched on the Wei's scheme to check whether the scheme is secure or not. In first attack, it is proved that master secret key is compromised. The subsequent attacks proved that the scheme is neither IND-CCA secure nor EUF-CMA secure in the standard model. Thus, Wei's scheme is susceptible and insecure.

Author Contributions: conceptualization, A.W. and N.D.; methodology, N.D.; validation, A.W., N.D. and N.U.A.; formal and security analysis, A.W. and N.D.; investigation, A.W.; resources, S.A. and P.K.; writing—original draft preparation, A.W.; writing—review and editing, A.W., and N.U.A.; supervision, A.I.U.; project administration, N.D.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 47–53.
2. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. *SIAM J. Comput.* **2003**, *32*, 586–615. [[CrossRef](#)]

3. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption) cost (signature)+ cost (encryption). In Proceedings of the 17th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997; pp. 165–179.
4. Malonee-Lee, J. Identity Based Signcryption. Available online: <https://eprint.iacr.org/2002/098.pdf> (accessed on 25 July 2019).
5. Libert, B.; Quisquater, J.J. A new identity based signcryption scheme from pairings. In Proceedings of the 2003 IEEE Information Theory Workshop (Cat. No.03EX674), Paris, France, 31 March–4 April 2003; pp. 155–158.
6. Chow, S.S.; Yiu, S.M.; Hui, L.C.; Chow, K.P. *Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity*; Springer: Berlin/Heidelberg, Germany, 2003.
7. Boyen, X. Multipurpose Identity-Based Signcryption. In Proceedings of the 23rd Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 2003; pp. 383–399.
8. Chen, L.; Malonee-Lee, J. Improved Identity-Based Signcryption. In Proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, 23–26 January 2005; pp. 362–379.
9. Barreto, P.S.; Libert, B.; McCullagh, N.; Quisquater, J.J. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps. In Proceedings of the 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, 4–8 December 2005; pp. 515–532.
10. Selvi, S.S.; Vivek, S.S.; Rangan, C.P. Identity Based Public Verifiable Signcryption Scheme. In Proceedings of the 4th International Conference on Provable Security, Malacca, Malaysia, 13–15 October 2010; pp. 244–260.
11. Yu, Y.; Yang, B.; Sun, Y.; Zhu, S.L. Identity based signcryption scheme without random oracles. *Comput. Stand. Interfaces* **2009**, *31*, 56–62. [[CrossRef](#)]
12. Jin, Z.; Wen, Q.; Du, H. An improved semantically-secure identity-based signcryption scheme in the standard model. *Comput. Electr. Eng.* **2010**, *36*, 545–552. [[CrossRef](#)]
13. Li, F.; Muhaya, F.B.; Zhang, M.; Takagi, T. Efficient Identity-Based Signcryption in the Standard Model. In Proceedings of the 5th International Conference on Provable Security 2011, Xi'an, China, 16–18 October 2011; pp. 120–137.
14. Shen, X.; Ming, Y.; Feng, J.; Shen, X.; Ming, Y.; Feng, J. Identity Based Generalized Signcryption Scheme in the Standard Model. *Entropy* **2017**, *19*, 121. [[CrossRef](#)]
15. Han, Y.; Yang, X.; Wei, P.; Wang, Y.; Hu, Y. ECGSC: Elliptic Curve Based Generalized Signcryption. In Proceedings of the 3rd International Conference on Ubiquitous Intelligence and Computing, Wuhan, China, 3–6 September 2006; pp. 956–965.
16. Wang, X.A.; Yang, X.; Zhang, J. Provable secure generalized signcryption. *J. Comput.* **2010**, *5*, 807–814. [[CrossRef](#)]
17. Lal, S.; Kushwah, P. ID Based Generalized Signcryption. Available online: <https://eprint.iacr.org/2008/084.pdf> (accessed on 25 July 2019).
18. Yu, G.; Ma, X.; Shen, Y.; Han, W. Provable secure identity based generalized signcryption scheme. *Theor. Comput. Sci.* **2010**, *411*, 3614–3624. [[CrossRef](#)]
19. Kushwah, P.; Lal, S. An efficient identity based generalized signcryption scheme. *Theor. Comput. Sci.* **2011**, *412*, 6382–6389. [[CrossRef](#)]
20. Waheed, A.; Iqbal, J.; Din, N.; Ul, S.; Iqbal, A.; Ul, N. Improved Cryptanalysis of Provable Certificateless Generalized Signcryption. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [[CrossRef](#)]
21. Zhou, C.; Zhou, W.; Dong, X. Provable certificateless generalized signcryption scheme. *Des. Codes Cryptogr.* **2014**, *71*, 331–346. [[CrossRef](#)]
22. Wei, G.; Shao, J.; Xiang, Y.; Zhu, P.; Lu, R. Obtain confidentiality or/and authenticity in Big Data by ID-based generalized signcryption. *Inf. Sci.* **2015**, *318*, 111–122. [[CrossRef](#)]