entropy

MDPI

Article

Identity Based Generalized Signcryption Scheme in the Standard Model

Xiaoqin Shen [1], Yang Ming [2,*] and Jie Feng [2]

[1] School of Sciences, Xi'an University of Technology, Xi'an 710054, China; xqshen@xaut.edu.cn
[2] School of Information Engineering, Chang'an University, Xi'an 710064, China; jiefengcl@163.com
* Correspondence: yangming@chd.edu.cn; Tel.: +86-29-8233-4720

Academic Editor: Raúl Alcaraz Martínez
Received: 10 January 2017; Accepted: 13 March 2017; Published: 17 March 2017

Abstract: Generalized signcryption (GSC) can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm. It is more suitable for the storage constrained setting. In this paper, motivated by Paterson–Schuldt's scheme, based on bilinear pairing, we first proposed an identity based generalized signcryption (IDGSC) scheme in the standard model. To the best of our knowledge, it is the first scheme that is proven secure in the standard model.

Keywords: generalized signcryption; identity based cryptography; bilinear pairings; standard model

1. Introduction

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements simultaneously is to sign-then-encrypt or encrypt-then-sign. To enhance efficiency, Zheng [1] proposed the concept of signcryption in 1997. The main idea of this primitive is to perform signature and encryption simultaneously in a logical step. Compared with traditional methods [2], signcryption reduces the computational costs and communication overheads. Since then, many public key signcryption schemes have been proposed [3–5].

In 1984, Shamir [6] first proposed the idea of identity-based (ID-based) public key cryptography (ID-PKC) to simplify key management procedures of traditional certificate-based public key cryptography. The main idea of ID-PKC is that the user's public key can be calculated directly from his/her identity such as email addresses rather than being extracted from a certificate issued by a certificate authority (CA). Private keys are generated for the users by a trusted third party, called a Private Key Generator (PKG) using some master key related to the global parameters for the system. The direct derivation of public keys in ID-PKC eliminates the need for certificates and some of the problems associated with them. The first identity based signature scheme was given by Shamir [6], but the first identity based encryption scheme was presented by Boneh and Fanklin [7] in 2001. The first identity based signcryption scheme was proposed by Malone Lee [8] in 2002, and they also gave the security model for signcryption in identity based settings. Since then, many identity based signcryption schemes have been proposed [9–17].

The signcryption scheme was used in these application environments, which need simultaneous confidentiality and authenticity. However, it is not all application environments requiring both confidentiality and authenticity. If only one of the two functionalities is required, then the signcryption scheme is not efficient. To achieve this, we can use an encryption/signature scheme. However, in the low bandwidth environment, we have to afford to use three different cryptographic algorithms—encryption, signature and signcryption—to achieve confidentiality and authenticity separately or simultaneously. In 2006, to decrease implementation complexity, Han et al. [18] proposed the concept of generalized signcryption, which can work as an encryption scheme or a signature

scheme or a signcryption scheme as required. They also proposed a concert construction based on the Elliptic Curve Digital Signature Algorithm (ECDSA) . Wang et al. [19] gave the security model of a generalized signcryption scheme and modified the scheme proposed in [18]. In 2008, Lal et al. [20] presented the first identity based generalized signcryption (IDGSC) scheme. However, Yu et al. [21] showed that the security model in [20] is not complete. They modified the security model and gave a new scheme that is secure in this model. In 2011, Kushwah et al. [22] simplified the security model for IDGSC and proposed an efficient scheme.

Provable security is the basic requirement for ID-based generalized signcryption schemes. The security of all of the schemes [20–22] described above was only proven secure in the random oracle model. The random oracle model was introduced by Bellare and Rogaway in [23]. The model is a formal model in analyzing cryptographic schemes, where a hash function is considered as a black box that contains a random function. Although the model is efficient and useful, it has received a lot of criticism that the proofs in the random oracle model are not proven. Canetti et al. [24] have shown that security in the random oracle model does not imply security in the real world, in that a scheme can be secure in the random oracle model and yet be broken without violating any particular intractability assumption, and without breaking the underlying hash functions.

Therefore, to design a provable secure ID-based generalized signcryption scheme in the standard model (without random oracles) remains an open and interesting research problem.

In this paper, we first proposed an ID-based generalized signcryption scheme in the standard model. Using the Paterson–Schuldt scheme [25], we give a concrete scheme. We also prove its semantic security under the hardness of the Decisional Bilinear Diffie–Hellman problem and its unforgeability under the computational Diffie–Hellman assumption.

2. Preliminaries

In this section, we briefly review the basic concepts on bilinear pairings and some related complexity assumptions.

2.1. Bilinear Pairings

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of prime order q and let g be a generator of $\mathbb{G}_1$. The map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is said to be an admissible bilinear pairing with the following properties:

- *Bilinearity:* For all $u, v \in \mathbb{G}_1$, and $a, b \in \mathbb{Z}_q$, $e(u^a, v^b) = e(u, v)^{ab}$.
- *Non-degeneracy:* $e(g, g) \neq 1$.
- *Computability:* There exists an efficient algorithm to compute $e(u, v)$ for all $u, v \in \mathbb{G}_1$.

We note that the modified Weil and Tate pairings associated with supersingular elliptic curves are examples of such admissible pairings.

2.2. Complexity Assumptions

2.2.1. Decisional Bilinear Diffie–Hellman (DBDH) Problem

Given $g, g^a, g^b, g^c \in \mathbb{G}_1$, for unknown $a, b, c \in \mathbb{Z}_q^*$ and $Z \in \mathbb{G}_2$, decide whether $Z = e(g, g)^{abc}$.
Defining the advantage ε of a polynomial algorithm $\mathcal{A}$ against the DBDH problem is

$$|\Pr[\mathcal{A}(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[\mathcal{A}(g, g^a, g^b, g^c, Z) = 1]| \geq \varepsilon,$$

where the probability is over the randomly chosen a, b, c and the random bits consumed by $\mathcal{A}$.

Definition 1. *The (t, ε) DBDH assumption holds if no t-time adversary has at least ε advantage in solving the DBDH problem.*

2.2.2. Computational Diffie–Hellman (CDH) Problem

Given $g, g^a, g^b \in \mathbb{G}_1$, for unknown $a, b \in \mathbb{Z}_q^*$, compute g^{ab}.
The success probability δ of a polynomial algorithm $\mathcal{A}$ in solving the CDH problem is denoted as

$$Succ_{\mathcal{A}}^{CDH} = \Pr[\mathcal{A}(g, g^a, g^b) = g^{ab},] \geq \delta$$

where the probability is over the randomly chosen a, b and the random bits consumed by $\mathcal{A}$.

Definition 2. *The (t, δ) CDH assumption holds if no t-time adversary has at least δ in solving the CDH problem.*

3. Formal Model of Identity-Based Generalized Signcryption Schemes

3.1. Generic Scheme

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

- *Setup*: Given a security parameter k, the private key generator (PKG) generates system parameters *params* and a master key s. *params* is made public while s is kept secret.
- *Extract*: Given an identity ID, the PKG computes the corresponding private key d_{ID} and transmits it to the ID via a secure channel.
- *Generalized Signcrypt*: Given the sender's identity ID_A and private key d_A, the receiver's identity ID_B and a message m, the sender outputs the ciphertext σ.
- *Generalized Unsigncrypt*: Given the sender's identity ID_A, the receiver's identity ID_B and private key d_B and the ciphertext σ, the receiver with identity ID_B outputs m or the symbol $\perp$ if σ is an invalid ciphertext under ID_A and ID_B.

There is no special sender (or receiver) when we encrypt (or sign) a message using IDGSC. We denote the absence of sender (or receiver) by ID_Φ. If $ID_B = ID_\Phi$, the IDGSC scheme becomes a signature scheme and output of the IDGSC is a signature of sender ID_A on the message m. If $ID_A = ID_\Phi$, the IDGSC scheme becomes an encryption scheme and output of the IDGSC is merely an encryption of message m for receiver ID_B. If $ID_A \neq ID_\Phi$ and $ID_B \neq ID_\Phi$, then IDGSC works as the signcryption scheme and output of IDGSC is the signcryption of message m for sender ID_A and receiver ID_B. Thus, the IDGSC scheme works in three models via signcryption mode, encryption mode and signature mode.

3.2. Security Model

According to Yu et al.'s scheme [21], the abilities of an adversary are formally modeled by queries issued by adversities. Each adversary may issue the following queries:

- *Private-Key-Extract*: The adversary submits an identity, and the challenger responds with the private key of that identity.
- *Sign*: The adversary submits a sender's identity and a message, and the challenger responds with the signature of the signer on the message.
- *Verify*: The adversary submits a signer's identity and a message/signature pair, and the challenger responds with 1 if the signature is accepted and 0 otherwise.
- *Encrypt*: The adversary submits a receiver's identity and a message, and the challenger responds with the ciphertext on this message for the receiver.
- *Decrypt*: The adversary submits a receiver's identity and a ciphertext, and the challenger decrypts the ciphertext under the private key of the receiver and returns the corresponding plaintext.
- *Signcrypt*: The adversary submits a sender's and receiver's identities and a message, and the challenger responds with the ciphertext under the sender's private key and the receiver's public key.

- *Unsigncrypt*: The adversary submits a ciphertext and a receiver's identity, and the challenger decrypts the ciphertext under the private key of the receiver and verifies that the resulting decryption is a valid message/signature pair under the public key of the decrypted identity. Then, the challenger returns the message.

The identity based generalized signcryption can work in three modes: *encryption mode*, *signature mode* and *signcryption mode*, denoted IDGSC-EN, IDGSC-SG and IDGSC-SC, respectively.

For the *confidentiality*, we define the following two games (Game 1 and Game 2) under IDGSC-EN and IDGSC-SC, respectively.

Game 1. Indistinguishability (IND)-(IDGSC-EN)-CCA2 Secure

Consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- *Initial*: The challenger $\mathcal{C}$ takes security parameters k and runs the *Setup* algorithm to generate system parameters *params* and the master key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$ and keeps s secret.
- *Phase 1*: The adversary $\mathcal{A}$ can perform a polynomially bounded number of seven above types of queries. These queries may be made adaptively, i.e., each query may depend on the answers to the previous queries.
- *Challenge*: The adversary $\mathcal{A}$ decides when Phase 1 ends, and chooses two equal length plaintexts m_0, m_1 and two identities $ID_A = ID_\Phi, ID_B \neq ID_\Phi$ on which to be challenged. The identity ID_B should not appear in any private key extract queries in Phase 1. $\mathcal{C}$ chooses randomly a bit b, encrypts m_b and then sends the ciphertext σ to $\mathcal{A}$.
- *Phase 2*: The adversary $\mathcal{A}$ makes a polynomial number of queries adaptively again as in Phase 1 with the restriction that it cannot make private key extract queries on ID_B and cannot make an unsigncrypt query on σ.
- *Guess*: The adversary $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Adv^{IND-CCA2}_{IDGSC-EN}(A) = |2\Pr[b' = b] - 1|$, where $\Pr[b' = b]$ denotes the probability that $b' = b$.

Definition 3 (Confidentiality-IDGSC-EN)**.** *An IDGSC scheme is said to have the indistinguishability against chosen adaptive ciphertext attacks (IND-(IDGSC-EN)-CCA2) or semantic security if no polynomially bounded adversary has a non-negligible advantage in Game 1.*

Game 2. IND-(IDGSC-SC)-CCA2 Secure

Consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- *Initial*: The challenger $\mathcal{C}$ takes security parameters k and runs the *Setup* algorithm to generate system parameters *params* and the master key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$ and keeps s secret.
- *Phase 1*: The adversary $\mathcal{A}$ can perform a polynomially bounded number of the seven types of queries above. These queries may be made adaptively, i.e., each query may depend on the answers to the previous queries.
- *Challenge*: The adversary $\mathcal{A}$ decides when phase 1 ends, chooses two equal length plaintexts m_0, m_1 and two identities $ID_A \neq ID_\Phi, ID_B \neq ID_\Phi$ on which to be challenged. The identity ID_B should not appear in any private key extract queries in Phase 1. $\mathcal{C}$ chooses randomly a bit b, encrypts m_b and then sends the ciphertext σ to $\mathcal{A}$.
- *Phase 2*: The adversary $\mathcal{A}$ makes a polynomial number of queries adaptively again as in Phase 1 with the restriction that it cannot make private key extract queries on ID_B and cannot make an unsigncrypt query on σ.
- *Guess*: The adversary $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Adv^{IND-CCA2}_{IDGSC-SC}(A) = |2\Pr[b' = b] - 1|$, where $\Pr[b' = b]$ denotes the probability that $b' = b$.

Definition 4 (Confidentiality-IDGSC-SC)**.** *An IDGSC scheme is said to have the indistinguishability against adaptive chosen ciphertext attacks (IND-(IDGSC-SC)-CCA2) or semantic security if no polynomially bounded adversary has a non-negligible advantage in Game 2.*

For the *unforgeability*, we define the following two games (Game 3 and Game 4) under IDGSC-SG and IDGSC-SC, respectively.

Game 3. EF-(IBGSC-SG)-Adaptive Chosen Message Attack (ACMA) Secure

Consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- *Initial*: The challenger $\mathcal{C}$ runs the *Setup* algorithm with a security parameter k and obtains system parameters *params* and the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.
- *Queries*: The adversary $\mathcal{A}$ performs a polynomially bounded number of queries adaptively just like in Game 1.
- *Forgery*: Finally, the adversary $\mathcal{A}$ produces two identities $ID_A \neq ID_\Phi, ID_B = ID_\Phi$ and a ciphertext (signature) σ. The adversary wins the game if $ID_A \neq ID_\Phi$; σ was a valid ciphertext (signature) on m, ID_A; no private key extract query was made on ID_A; σ did not result from signature query on m, ID_A.

The advantage of $\mathcal{A}$ is defined as $Adv^{EF-ACMA}_{IDGSC-SG}(A) = \Pr[Awins]$.

Definition 5 (Unforgeability-IDGSC-SG)**.** *An IDGSC scheme is said to have the existential unforgeability against chosen adaptive message attacks (EF-(IDGSC-SG)-ACMA) if no polynomially bounded adversary has a non-negligible advantage in Game 3.*

Game 4. EF-(IDGSC-SC)-ACMA Secure

Consider the following game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- *Initial*: The challenger $\mathcal{C}$ runs the *Setup* algorithm with a security parameter k and obtains system parameters *params* and the master secret key s. $\mathcal{C}$ sends *params* to $\mathcal{A}$.
- *Queries*: The adversary $\mathcal{A}$ performs a polynomially bounded number of queries adaptively just like in Game 1.
- *Forgery*: Finally, the adversary $\mathcal{A}$ produces a new tuple (σ, ID_A, ID_B). Let m be the result of unsigncryption σ under the private key of ID_B. The adversary wins the game if $ID_A \neq ID_\Phi, ID_B \neq ID_\Phi$; no private key extract query was made on ID_A; σ is a valid signature under m, ID_A; (σ, ID_A, ID_B) was not output by a signcrypt query.

The advantage of $\mathcal{A}$ is defined as $Adv^{EF-ACMA}_{IDGSC-SC}(A) = \Pr[Awins]$.

Definition 6 (Unforgeability-IDGSC-SC)**.** *An IDGSC scheme is said to have the existential unforgeability against chosen adaptive message attacks (EF-(IDGSC-SC)-ACMA) if no polynomially bounded adversary has a non-negligible advantage in Game 4.*

4. The Proposed Scheme

Our IDGSC scheme is described as the following algorithms.

- *Setup*: Given a security parameter k, the PKG chooses groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q, a generator g of $\mathbb{G}_1$, a admissible bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, and hash functions $H : \{0,1\}^* \to \{0,1\}^l$ and $H_m : \{0,1\}^* \to \{0,1\}^{n_m}$. The PKG chooses a random value $\alpha \in \mathbb{Z}^*_q$, computes $g_1 = g^\alpha$ and selects $g_2 \in \mathbb{G}_1$. Furthermore, the PKG computes $z = e(g_1, g_2)$ and picks $u', m' \in \mathbb{G}_1$ and vectors $\mathrm{u} = \{u_i\}$, $\mathrm{m} = \{m_i\}$ of length n_u and n_m, respectively, whose entries are random elements from $\mathbb{G}_1$. The system parameters are $params = \{G_1, G_2, e, p, g, g_1, g_2, H, H_m, z, u', m', \mathrm{u}, \mathrm{m}\}$ and the master secret key g_2^α.

Let $f(ID)$ be a special function, where $ID \in \{0,1\}^{n_u}$. If identity is vacant, that is $ID = ID_\Phi$, $f(ID) = 0$, otherwise $f(ID) = 1$.

- *Extract*: Let ID be a bit string of length n_u, representing an identity and let $ID[i]$ be the i-th bit of ID. Define $U_{ID} \subset \{1, 2, \cdots, n_u\}$ to be the set of indices i such that $ID[i] = 1$. A private key d_{ID} for identity ID is generated as follows. The PKG picks $r_{ID} \in \mathbb{Z}_q^*$ and computes

$$d_{ID} = (d_{ID1}, d_{ID2}) = \left(g_2^\alpha (u' \prod_{i \in U_{ID}} u_i)^{r_{ID}}, g^{r_{ID}} \right).$$

Therefore, the sender with identity ID_A and the receiver with identity ID_B private keys are

$$d_A = (d_{A1}, d_{A2}) = \left(g_2^\alpha (u' \prod_{i \in U_A} u_i)^{r_A}, g^{r_A} \right),$$
$$d_B = (d_{B1}, d_{B2}) = \left(g_2^\alpha (u' \prod_{i \in U_B} u_i)^{r_B}, g^{r_B} \right).$$

- *Generalized Signcrypt*: Suppose the sender A with identity ID_A wants to send a message $m \in \{0,1\}^l$ to the receiver B with identity ID_B, A picks randomly $r \in \mathbb{Z}_q^*$ and does the following:

1. Compute $\sigma_1 = g^r$.
2. Compute $w = z^{rf(ID_B)}$.
3. Compute $c = m \oplus H(w)$.
4. Compute $\sigma_2 = (d_{A2})^{f(ID_A)}$.
5. Compute $\sigma_3 = (u' \prod_{i \in U_B} u_i)^{rf(ID_B)}$.
6. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$. Here π is an n_m bit string and $\pi[j]$ denotes the j-th bit of π, and $M \subset \{1, 2, \cdots, n_m\}$ denotes the set of j for which $\pi[j] = 1$.
7. Compute $\sigma_4 = (d_{A1})^{f(ID_A)} \cdot \sigma_3 \cdot (m' \prod_{j \in M} m_j)^r$.

The ciphertext is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, c)$.

- *Generalized Unsigncrypt*: When receiving σ, the receiver with identity ID_B follows the steps below:

1. Compute $f(ID_B)$.
2. Compute $w = e(d_{B1}, \sigma_1^{f(ID_B)}) \cdot e(d_{B2}, \sigma_3)^{-1}$.
3. Compute $m = c \oplus H(w)$.
4. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$ and generate the corresponding set M, the set of all j for which $\pi[j] = 1$.
5. Accepted the message if and only if the following equality holds:
$e(\sigma_4, g) = e(g_2, g_1)^{f(ID_A)} e(u' \prod_{i \in U_A} u_i, \sigma_2) e(u' \prod_{i \in U_B} u_i, \sigma_1)^{f(ID_B)} e(m' \prod_{j \in M} m_j, \sigma_1)$.

Remark 1. *Our* Setup, Extract *algorithm in our scheme is from the existing work, i.e., Paterson–Schuldt's scheme [25]. However, our Setup algorithm has some differences from [25], and we added some parameters: H and H_m. Other algorithms such as* Generalized Signcrypt *and* Generalized Unsigncrypt *are new designs.*

5. Analysis

5.1. Correctness

$$\frac{e\left(d_{B1}, \sigma_1^{f(ID_B)}\right)}{e(d_{B2}, \sigma_3)} = \frac{e\left(g_2^\alpha (u' \prod_{i \in U_B} u_i)^{r_B}, g^{rf(ID_B)}\right)}{e\left(g^{r_B}, (u' \prod_{i \in U_B} u_i)^{rf(ID_B)}\right)} = \frac{e\left(g_2^\alpha, g^{rf(ID_B)}\right) e\left((u' \prod_{i \in U_B} u_i)^{r_B}, g^{rf(ID_B)}\right)}{e\left(g^{r_B}, (u' \prod_{i \in U_B} u_i)^{rf(ID_B)}\right)} = e(g_1, g_2)^{rf(ID_B)}$$

$$\begin{aligned} e(\sigma_4, g) &= e((g_2^{\alpha f(ID_A)} \cdot (u' \prod_{i \in U_A} u_i)^{r_A f(ID_A)} \cdot (u' \prod_{i \in U_B} u_i)^{r f(ID_B)} \cdot (m' \prod_{j \in M} m_j)^r, g)) \\ &= e(g_2^{\alpha f(ID_A)}, g) e((u' \prod_{i \in U_A} u_i)^{r_A f(ID_A)}, g)) e(((u' \prod_{i \in U_B} u_i)^{r f(ID_B)}, g)) e(((m' \prod_{j \in M} m_j)^r, g)) \\ &= e(g_2, g_1)^{f(ID_A)} e(u' \prod_{i \in U_A} u_i, g^{r_A f(ID_A)}) e(u' \prod_{i \in U_B} u_i, g^{r f(ID_B)}) e(m' \prod_{j \in M} m_j, g^r) \\ &= e(g_2, g_1)^{f(ID_A)} e(u' \prod_{i \in U_A} u_i, \sigma_2) e(u' \prod_{i \in U_B} u_i, \sigma_1)^{f(ID_B)} e(m' \prod_{j \in M} m_j, \sigma_1). \end{aligned}$$

There are three cases to be considered.

Case 1. In the IDGSC-SC Model

In this case, there is $ID_A \neq ID_\Phi, ID_B \neq ID_\Phi$, so $f(ID_A) = f(ID_B) = 1$. The generalized signcryption scheme in signcryption model is as follows:

- *Signcrypt:*

  1. Compute $\sigma_1 = g^r$.
  2. Compute $w = z^r$.
  3. Compute $c = m \oplus H(w)$.
  4. Compute $\sigma_2 = d_{A2}$.
  5. Compute $\sigma_3 = (u' \prod_{i \in U_B} u_i)^r$.
  6. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$. Here π is an n_m bit string and $\pi[j]$ denotes the j-th bit of π, and $M \subset \{1, 2, \cdots, n_m\}$ denotes the set of j for which $\pi[j] = 1$.
  7. Compute $\sigma_4 = d_{A1} \cdot \sigma_3 \cdot (m' \prod_{j \in M} m_j)^r$.

  The ciphertext is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, c)$.
- *Unsigncrypt*:

  1. Compute $w = e(d_{B1}, \sigma_1) \cdot e(d_{B2}, \sigma_3)^{-1}$.
  2. Compute $m = c \oplus H(w)$.
  3. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$ and generate the corresponding set M, the set of all j for which $\pi[j] = 1$.
  4. Accepted the message if and only if the following equality holds:

$$e(\sigma_4, g) = e(g_2, g_1) e(u' \prod_{i \in U_A} u_i, \sigma_2) e(u' \prod_{i \in U_B} u_i, \sigma_1) e(m' \prod_{j \in M} m_j, \sigma_1).$$

Case 2. In the IDGSC-SG Model

In this case, there is $ID_A \neq ID_\Phi, ID_B = ID_\Phi$, so $f(ID_A) = 1, f(ID_B) = 0$. The generalized signcryption scheme in the signature model is as follows:

- *Sign*:

  1. Compute $\sigma_1 = g^r$.
  2. Compute $w = z^{r f(ID_B)} = 1$.
  3. Compute $c = m \oplus H(w)$.
  4. Compute $\sigma_2 = (d_{A2})^{f(ID_A)} = d_{A2}$.
  5. Compute $\sigma_3 = (u' \prod_{i \in U_B} u_i)^{r f(ID_B)} = 1$.
  6. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$. Here π is an n_m bit string and $\pi[j]$ denotes the j-th bit of π , and $M \subset \{1, 2, \cdots, n_m\}$ denotes the set of j for which $\pi[j] = 1$.
  7. Compute $\sigma_4 = d_{A1} \cdot \sigma_3 \cdot (m' \prod_{j \in M} m_j)^r$.

  The signature is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, c \oplus H(w)) = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, m)$.

- *Verify*:

  1. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$ and generate the corresponding set M, the set of all j for which $\pi[j] = 1$.
  2. Accepted the signature if and only if the following equality holds:

$$e(\sigma_4, g) = e(g_2, g_1)e(u' \prod_{i \in U_A} u_i, \sigma_2)e(u' \prod_{i \in U_B} u_i, \sigma_1)e(m' \prod_{j \in M} m_j, \sigma_1).$$

Case 3. In the IDGSC-EN Model

In this case, there is $ID_A = ID_\Phi, ID_B \neq ID_\Phi$, so $f(ID_A) = 0, f(ID_B) = 1$. The generalized signcryption scheme in the encryption model as follows:

- *Encrypt*:

  1. Compute $\sigma_1 = g^r$.
  2. Compute $w = z^{rf(ID_B)} = z^r$.
  3. Compute $c = m \oplus H(w)$.
  4. Compute $\sigma_2 = (d_{A2})^{f(ID_A)} = 1$.
  5. Compute $\sigma_3 = (u' \prod_{j \in U_B} u_i)^{rf(ID_B)} = (u' \prod_{i \in U_B} u_i)^r$.
  6. Compute $\pi = H_m(m, \sigma_1, \sigma_2, \sigma_3, w)$. Here π is an n_m bit string and $\pi[j]$ denotes the j-th bit of $\pi[j]$, and $M \subset \{1, 2, \cdots, n_m\}$ denotes the set of j for which $\pi[j] = 1$.
  7. Compute $\sigma_4 = (d_{A1})^{f(ID_A)} \cdot \sigma_3 \cdot (m' \prod_{j \in M} m_j)^r = (u' \prod_{i \in U_B} u_i)^r \cdot (m' \prod_{j \in M} m_j)^r$.

  The ciphertext is $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, c)$.
- *Decrypt*:

  1. Compute $w = e(d_{B1}, \sigma_1) \cdot e(d_{B2}, \sigma_3)^{-1}$.
  2. Compute $m = c \oplus H(w)$.
  3. Compute $\pi = H_m(M, \sigma_1, \sigma_2, \sigma_3, w)$ and generate the corresponding set M, the set of all j for which $\pi[j] = 1$.
  4. Accepted the message if and only if the following equality holds:

$$e(\sigma_4, g) = e(u' \prod_{i \in U_B} u_i, \sigma_1)e(m' \prod_{j \in M} m_j, \sigma_1).$$

5.2. Security Proof

Theorem 1. *(Confidentiality in the IDGSC-EN model) Assume there is an adversary IND (IBGSC-EN) CCA2 $\mathcal{A}$ that is able to distinguish two valid ciphertexts during the defined in Game 1 with an advantage ε when running in a time t, then there exists an algorithm $\mathcal{D}$ that can break Waters' identity based encryption scheme in a time $t' = t$ with an advantage $\varepsilon' = \varepsilon$.*

Proof. When the IDGSC scheme works as an encryption scheme, it is a actually the identity based encryption proposed by Waters [26] and one-time signature. Owing to the theorem proposed by Canetti et al. [27], this scheme is secure against the normal adaptive chosen-ciphertext attack. Considering the signcrypt/unsigncrypt query, the adversary cannot transform the target encryption ciphertext into a valid signcryption ciphertext. This conclusion is based on the EF-ACMA security of PS. So IDGSC scheme in encryption model is IND-CCA2 secure. Thus, the theorem follows. □

Theorem 2. *(Confidentiality in the IDGSC-SC model). Assume there is an adversary IND (IDGSC-SC) CCA2 $\mathcal{A}$ that is able to distinguish two valid ciphertexts during the defined in Game 2 with an advantage ε when running in a time t and making at most q_k private key extract queries, q_s sign queries, q_v verify queries, q_e encrypt queries, q_d decrypt queries, q_{sc} signcrypt queries and q_{us} unsigncrypt queries. Then, there exists a distinguisher that can solve an instance of the DBDH problem in a time $t' = t + (5q_k + 2q_s + 4q_e + 4q_{sc})t_e + (4q_d + 7q_{us} + 4q_v)t_p$ with an advantage $\varepsilon' = \frac{\varepsilon}{8(q_k+q_d+q_s+q_{sc}+q_{us})(n_u+1)q_{sc}(n_m+1)}$, where t_e denotes the time of an exponentiation in $\mathbb{G}_1$ and t_p denotes the time of a pairing in (G_1, G_2).*

Proof. Assume that there is a polynomially bounded adversary $\mathcal{A}$ that is able to break the semantic security of our scheme. Then, there exists a distinguisher $\mathcal{D}$ that can decide whether $Z = e(g,g)^{abc}$ or not with a non-negligible advantage when receiving a random instance g, g^a, g^b, g^c, Z. $\mathcal{D}$ runs $\mathcal{A}$ as the subroutine and acts as the challenger in Game 2 and interacts with $\mathcal{A}$ as described below. □

- *Initial*. $\mathcal{D}$ chooses randomly as follows:

  1. Two integers $0 \leqslant l_u \leqslant q$ and $0 \leqslant l_m \leqslant q$.
  2. Two integers $0 \leqslant k_u \leqslant n_u$ and $0 \leqslant k_m \leqslant n_m$ ($l_u(n_u+1) < q$, $l_m(n_m+1) < q$).
  3. An integer $x' \in \mathbb{Z}_{l_u}$ and n_u-dimensional vector $(x_1, \cdots, x_{n_u}) \in \mathbb{Z}_{l_u}$.
  4. An integer $y' \in \mathbb{Z}_{l_m}$ and n_m-dimensional vector $(y_1, \cdots, y_{n_m}) \in \mathbb{Z}_{l_m}$.
  5. An integer $z' \in \mathbb{Z}_q$ and n_u-dimensional vector $(z_1, \cdots, z_{n_u}) \in \mathbb{Z}_q$.
  6. An integer $\omega' \in \mathbb{Z}_q$ and n_m-dimensional vector $(\omega_1, \cdots, \omega_{n_m}) \in \mathbb{Z}_q$.

  To make the notation easy to follow, we define four functions:

  $$F(ID) = x' + \sum_{i \in \mathrm{U}} x_i - l_u k_u,\ J(ID) = z' + \sum_{i \in \mathrm{U}} z_i,$$
  $$K(M) = y' + \sum_{i \in \mathrm{M}} y_i - l_m k_m,\ L(M) = \omega' + \sum_{i \in \mathrm{M}} \omega_i.$$

  $\mathcal{D}$ sets system parameters as follows:

  1. $g_1 = g^a$ and $g_2 = g^b$.
  2. $u' = g_2^{-l_u k_u + x'} g^{z'}$ and $u_i = g_2^{x_i} g^{z_i}$ $(1 \leqslant i \leqslant n_u)$, which means that, for any identity ID, we have $u' \prod_{i \in U_{ID}} u_i = g_2^{F(ID)} g^{J(ID)}$.
  3. $m' = g_2^{-l_m k_m + y'} g^{\omega'}$ and $m_i = g_2^{y_i} g^{\omega_i}$ $(1 \leqslant i \leqslant n_m)$, which means that, for any π, we have $m' \prod_{i \in M} m_i = g_2^{K(\pi)} g^{L(\pi)}$.

  Finally, $\mathcal{D}$ returns all parameters to $\mathcal{A}$. We can see that all distributions are identical to that in the real world.
- *Phase 1*. $\mathcal{D}$ answers the queries as follows:

  – *Private key extract queries*: When the adversary $\mathcal{A}$ issues a private key extract query on an identity ID, $\mathcal{D}$ acts as follows:

    1. If $F(ID) = 0 \bmod l_u$, $\mathcal{D}$ aborts and reports failure.
    2. If $F(ID) \neq 0 \bmod l_u$, $\mathcal{D}$ can construct a private key by picking a random $r_{ID} \in \mathbb{Z}_q^*$ and computing:

    $$d_{ID} = (d_{ID1}, d_{ID2}) = (g_1^{-\frac{J(ID)}{F(ID)}} (g_2^{F(ID)} g^{J(ID)})^{r_{ID}}, g_1^{-\frac{1}{F(ID)}} g^{r_{ID}}).$$

  – *Encrypt queries*: At any time, the adversary $\mathcal{A}$ can perform an encrypt query on a plaintext m for the receiver ID_B, and $\mathcal{D}$ runs the encrypt algorithm in the encryption model to answer $\mathcal{A}$'s query.
  – *Decrypt queries*: At any time, the adversary $\mathcal{A}$ can perform a decrypt query on a ciphertext σ for the receiver ID_B, and $\mathcal{D}$ acts as follows:

    1. If $F(ID_B) = 0 \bmod l_u$, $\mathcal{D}$ aborts and reports failure.
    2. If $F(ID_B) \neq 0 \bmod l_u$, $\mathcal{D}$ first obtains the private key for ID_B as he does in response to the private key extract query, and then runs a decrypt algorithm in the encryption model to answer $\mathcal{A}$'s query.

  – *Sign queries*: At any time, the adversary $\mathcal{A}$ can perform a sign query on a message m for the sender ID_A, $\mathcal{D}$ acts as follows:

    1. If $F(ID_A) = 0 \bmod l_u$, $\mathcal{D}$ aborts and reports failure.
    2. If $F(ID_A) \neq 0 \bmod l_u$, $\mathcal{D}$ first obtains the private key for ID_A as he does in response to the private key extract query, and then runs a sign algorithm in the signature model to answer $\mathcal{A}$'s query.

- *Verify queries*: At any time, the adversary $\mathcal{A}$ can perform a verify query on a message/signature pair (m, σ) for the sender ID_A, and $\mathcal{D}$ runs a verify algorithm in the signature model to answer $\mathcal{A}$'s query.
- *Signcrypt queries*: At any time, the adversary $\mathcal{A}$ can perform a signcrypt query on a plaintext m for the sender identity ID_A and the receiver identity ID_B, and $\mathcal{D}$ acts as follows:
  1. If $F(ID_A) = 0 \bmod l_u$, $\mathcal{D}$ aborts and reports failure.
  2. If $F(ID_A) \neq 0 \bmod l_u$, $\mathcal{D}$ first obtains the private key for ID_A as he does in response to the private key extract query, and then runs the signcrypt algorithm in the signcryption model to answer $\mathcal{A}$'s query.
- *Unsigncrypt queries*: At any time, the adversary $\mathcal{A}$ can perform an unsigncrypt query on a ciphertext σ for the sender identity ID_A and the receiver identity ID_B, and $\mathcal{D}$ acts as follows:
  1. If $F(ID_B) = 0 \bmod l_u$, $\mathcal{D}$ aborts and reports failure.
  2. If $F(ID_B) \neq 0 \bmod l_u$, $\mathcal{D}$ first obtains the private key for ID_B as he does in response to the private key extract query, and then runs the unsigncrypt algorithm in the signcryption model to answer $\mathcal{A}$'s query.

- *Challenge*. After a polynomially bounded number of queries, the adversary $\mathcal{A}$ ID_A^*, ID_B^* on which he wishes to be challenged. Note that $\mathcal{D}$ fails if $\mathcal{A}$ has made a private key extract query on ID_B^* during Phase 1. Then, $\mathcal{A}$ submits two messages $m_0, m_1 \in \{0,1\}^l$ and ID_A^*, ID_B^* to $\mathcal{D}$. $\mathcal{D}$ will abort if $F(ID_B^*) \neq 0 \bmod l_u$. *Otherwise*, $\mathcal{D}$ flips a fair binary coin $\gamma \in \{0,1\}$ and constructs ciphertext m_γ as follows.

  $\mathcal{D}$ randomly chooses a number $r^* \in \mathbb{Z}_q^*$ and computes

$$\pi_\gamma^* = H(m_\gamma, g^c, g_1^{-\frac{1}{F(ID_A^*)}} g^{ID_A^*}, (g^c)^{J(ID_B^*)}, m_\gamma \oplus H(Z)).$$

  M_γ^* denoted the set of 1 for which $\pi_\gamma^*[j] = 1$. If $K(M_\gamma^*) \neq 0 \bmod q$, $\mathcal{D}$ aborts. Otherwise, $\mathcal{D}$ sets the ciphertext as:

$$\sigma^* = \left(g^c, g_1^{-\frac{1}{F(ID_A^*)}} g^{ID_A^*}, (g^c)^{J(ID_B^*)}, g_1^{-\frac{J(ID_A^*)}{F(ID_A^*)}} (g_2^{F(ID_A^*)} g^{J(ID_A^*)})^{r^*} (g^c)^{J(ID_B^*)} (g^c)^{L(\pi_\gamma^*)} \right).$$

- *Phase* 2. The adversary $\mathcal{A}$ then performs a second series of queries which are treated in the same as Phase 1. It is not allowed to make the private key extract query on ID_B^* and an unsigncrypt query on σ^* under ID_B^*.
- *Guess*. At the end of the simulations, the adversary $\mathcal{A}$ outputs a guess γ'. If $\gamma' = \gamma$, $\mathcal{D}$ answers 1, indicating that $Z = e(g,g)^{abc}$; otherwise, $\mathcal{D}$ answers 0 to the DBDH problem.

This completes the description of simulation. Analyzing the probability of $\mathcal{D}$ not aborting still needs to be analyzed. $\mathcal{D}$ will not abort if all the following conditions are fulfilled:

1. $F(ID) \neq 0 \bmod l_u$ during the private key extract queries.
2. $F(ID_B) \neq 0 \bmod l_u$ during the decrypt queries.
3. $F(ID_A) \neq 0 \bmod l_u$ during the sign queries.
4. $F(ID_A) \neq 0 \bmod l_u$ during the signcrypt queries.
5. $F(ID_B) \neq 0 \bmod l_u$ during the unsigncrypt queries.
6. $F(ID_B^*) = 0 \bmod q$ and $K(M_\gamma^*) = 0 \bmod q$ during the challenge phase.

Let $ID_1, \cdots, ID_{q_{ID}}$ be the identity appearing in all queries not involving the challenge identity. Clearly, we will have $q_{ID} \leqslant q_k + q_d + q_s + q_{sc} + q_{us}$. Define the following events:

$\mathrm{A}_i : F(ID_i) \neq 0 \bmod l_u$ where $i = 1, \cdots, q_{ID}$.
$\mathrm{B} : F(ID_B^*) = 0 \bmod q$.

$$\mathrm{C}: K(M_\gamma^*) = 0 \bmod q.$$

The success probability of $\mathcal{D}$ is $\Pr[\neg abort] = \Pr[\bigwedge_{i=1}^{q_{ID}} \mathrm{A}_i \wedge \mathrm{B} \wedge \mathrm{C}]$.

The functions F and K are selected independently; therefore, the events $(\bigwedge_{i=1}^{q_{ID}} \mathrm{A}_i \wedge \mathrm{B})$ and C are independent. According to $l_u(n_u+1) < q$, it is easy to see that $F(u) = 0 \bmod q \Rightarrow F(u) = 0 \bmod l_u$. Furthermore, this implies that, if $F(u) = 0 \bmod l_u$, there will be a unique k_u with $0 \leqslant k_u \leqslant n_u$, such that $F(u) = 0 \bmod q$. For the randomness of $k_u, x', x_1, \cdots, x_{n_u}$, we have

$$\begin{aligned}\Pr[\mathrm{B}] &= \Pr[F(ID_B^*) = 0 \bmod q] \\ &= \Pr[F(ID_B^*) = 0 \bmod l_u] \Pr[F(ID_B^*) = 0 \bmod q | F(ID_B^*) = 0 \bmod l_u] \\ &= (\frac{1}{l_u}\frac{1}{n_u+1}).\end{aligned}$$

On the other hand, for any i, the event A_i and B are independent, so we have

$$\begin{aligned}\Pr[\bigwedge_{i=1}^{q_{ID}} \mathrm{A}_i \wedge \mathrm{B}] &= \Pr[\mathrm{B}] \Pr[\bigwedge_{i=1}^{q_{ID}} \mathrm{A}_i | \mathrm{B}] = \Pr[\mathrm{B}] \left(1 - \Pr[\bigvee_{i=1}^{q_{ID}} \neg \mathrm{A}_i | \mathrm{B}]\right) \\ &\geqslant \Pr[\mathrm{B}] \left(1 - \sum_{i=1}^{q_{ID}} \Pr[\neg \mathrm{A}_i | \mathrm{B}]\right) = \left(\frac{1}{l_u(n_u+1)}\right)\left(1 - \frac{q_{ID}}{l_u}\right).\end{aligned}$$

Similarly, we have $\Pr[\mathrm{C}] = \Pr[K(M_\gamma^*) = 0 \bmod q] = \frac{1}{l_m}\frac{1}{n_m+1}$.
Let $l_u = 2(q_k + q_d + q_s + q_{sc} + q_{us})$ and $l_m = 2q_{sc}$. Then, we have

$$\begin{aligned}\Pr[\neg abort] &= \Pr[\bigwedge_{i=1}^{q_{ID}} \mathrm{A}_i \wedge \mathrm{B} \wedge \mathrm{C}] = \left(\frac{1}{l_u(n_u+1)}\right)\left(1 - \frac{q_{ID}}{l_u}\right)\left(\frac{1}{l_m}\frac{1}{n_m+1}\right) \\ &= \frac{1}{8(q_k + q_d + q_s + q_{sc} + q_{us})(n_u+1)q_{sc}(n_m+1).}\end{aligned}$$

If the simulation does not abort, the adversary $\mathcal{A}$ will win Game 2 with the advantage at least ε. Thus, $\mathcal{D}$ can solve for the DBDH problem instance with the advantage $\varepsilon' = \frac{\varepsilon}{8(q_k+q_d+q_s+q_{sc}+q_{us})(n_u+1)q_{sc}(n_m+1)}$.

Algorithm $\mathcal{D}$'s running time is the same as $\mathcal{A}$'s running time plus the time it takes to respond to q_k private key extract queries, q_s sign queries, q_v verify queries, q_e encrypt queries, q_d decrypt queries, q_{sc} signcrypt queries and q_{us} unsigncrypt queries. Each private key extract query requires five exponentiation operations in $\mathbb{G}_1$. Each sign query needs two exponentiation operations in $\mathbb{G}_1$. Each verify query needs four pairing operations in $(\mathbb{G}_1, \mathbb{G}_2)$. Each encrypt query needs four exponentiation operations in $\mathbb{G}_1$. Each decrypt query needs four pairing operations in $(\mathbb{G}_1, \mathbb{G}_2)$. Each signcrypt query requires four exponentiation operations in $\mathbb{G}_1$. Each unsigncrypt query requires seven pairing operations in $(\mathbb{G}_1, \mathbb{G}_2)$. If we assume each that exponentiation takes time t_e and each pairing takes time t_p, the total running time is at most $t + (5q_k + 2q_s + 4q_e + 4q_{sc})t_e + (4q_d + 7q_{us} + 4q_v)t_p$. Thus, the theorem follows.

Theorem 3. *(Unforgeability in the IDGSC-SG Model) Assuming that there is an adversary EF (IDGSC-SG) ACMA $\mathcal{A}$ that breaks our scheme with the probability δ when running in a time t, then there exists an algorithm $\mathcal{B}$ that can forge a valid signature of Paterson–Schuldt in a time $t' = t$ with the probability $\delta' = \delta$.*

Proof. When the IDGSC scheme works as a signature scheme, it is actually the identity based signature proposed by Paterson and Schuldt [25]. This signature scheme itself is EF-ACMA secure. Considering the signcrypt/unsigncrypt query that is absent in the normal signature scheme, these queries are useless to the adversary of EF-(IDGSC-SG)-ACMA. The identities of sender and receiver are included in the signature. Hence, an adversary can break the Paterson and Schuldt scheme if he can break our scheme in the signature model. Then, the theorem follows. □

Theorem 4. *(Unforgeability in the IDGSC-SC Model) Assume that there is an adversary EF (IDGSC-SC) ACMA $\mathcal{A}$ that breaks our scheme with the probability δ when running in a time t and making at most q_k private key extract queries, q_s sign queries, q_v verify queries, q_e encrypt queries, q_d decrypt queries, q_{sc} signcrypt queries and q_{uc} unsigncrypt queries. Then, there exists a algorithm $\mathcal{B}$ that can solve an instance of the CDH problem in a time $t' = t + (5q_k + 2q_s + 4q_e + 4q_{sc})t_e + (4q_d + 7q_{us} + 4q_v)t_p$ with the probability $\delta' = \frac{\delta}{16(q_k+q_d+q_s+q_{sc}+q_{us})^2(n_u+1)^2q_{sc}(n_m+1)}$, where t_e denotes the time of an exponentiation in $\mathbb{G}_1$ and t_p denotes the time of a pairing in $(\mathbb{G}_1, \mathbb{G}_2)$.*

Proof. Assume that there is a polynomially bounded adversary $\mathcal{A}$ that is able to break the unforgeability of our scheme. Then, there exists an algorithm $\mathcal{B}$ that can compute g^{ab} with a non-negligible advantage when receiving a random CDH problem instance (g, g^a, g^b). $\mathcal{B}$ runs $\mathcal{A}$ as the subroutine and acts as the challenger in Game 4 and interacts with $\mathcal{A}$ as described below. □

- *Initial*: $\mathcal{B}$ sets the system parameter using the initial phase described in Theorem 1. Note that $\mathcal{B}$ assigns $g_1 = g^a$ and $g_2 = g^b$.
- *Queries*: $\mathcal{A}$ can perform a polynomially bounded number of queries including private key extract queries, sign queries, verify queries, encrypt queries, decrypt queries, signcrypt queries and unsigncrypt queries. $\mathcal{B}$ answers the adversary $\mathcal{A}$ in the same way as that of Theorem 2.
- *Forgery*: Finally, $\mathcal{A}$ outputs a forgery ciphertext $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, c^*)$ on the message m^* under the receivers ID_B^* and the sender ID_A^* such that

  1. σ^* is a valid ciphertext.
  2. ID_A^* has not been submitted as one of the private key extract queries.
  3. m^* has not been submitted as one of the signcrypt queries under the ID_A^*, ID_B^*.

Now, $\mathcal{B}$ can unsigncrypt σ^* and obtain m^* under the ID_A^*, ID_B^*. $\mathcal{B}$ computes $\pi^* = H_m(m^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, w^*)$ and generates M^*, the set of all i for which $\pi^*[j] = 1$. If $F(ID_A^*) \neq 0 \bmod q$, $F(ID_B^*) \neq 0 \bmod q$ and $K(\pi^*) \neq 0 \bmod q$, $\mathcal{B}$ will abort. Otherwise, $F(ID_A^*) = 0 \bmod q$, $F(ID_B^*) = 0 \bmod q$ and $K(\pi^*) = 0 \bmod q$, $\mathcal{B}$ can obtain the following case:

$$\begin{aligned} e(\sigma_4^*, g) &= e(g_2, g_1)e(u' \prod_{i \in U_A^*} u_i, \sigma_2^*)e(u' \prod_{i \in U_B^*} u_i, \sigma_1^*)e(m' \prod_{j \in M^*} m_j, \sigma_1^*) \\ &= e(g^a, g^b)e(g^{J(ID_A^*)}, \sigma_2^*)e(g^{J(ID_B^*)}, \sigma_1^*)e(g^{L(\pi^*)}, \sigma_1^*). \end{aligned}$$

Thus, we have $g^{ab} = \frac{\sigma_4^*}{(\sigma_1^*)^{J(ID_B^*)}(\sigma_2^*)^{J(ID_A^*)}(\sigma_1^*)^{L(\pi^*)}}$, which is the solution to the given CDH problem.

Analogous to Theorem 1, we can obtain that $\mathcal{B}$ solves for the CDH problem instance with the probability $\delta' = \frac{\delta}{16(q_k+q_d+q_s+q_{sc}+q_{us})^2(n_u+1)^2q_{sc}(n_m+1)}$, with time being $t' = t + (5q_k + 2q_s + 4q_e + 4q_{sc})t_e + (4q_d + 7q_{us} + 4q_v)t_p$. Thus, the theorem follows.

5.3. Efficiency

We compare the efficiency and security of our scheme with those of three identity based generalized signcryption schemes, including Lal et al.'s scheme [20], Yu et al.'s scheme [21] and Kushwah et al.'s scheme [22]. We denote the modular exponentiation and the pairing computation by E, P, respectively. Other operations are omitted in the following analysis since their computation cost is trivial. We consider the pre-computation here and do not take hash function evaluations into account.

To compare the computation cost of related schemes, we compute the execution time of the cryptographic operations above using MIRACL [28], which is a famous cryptographic library and has been widely used to implement cryptographic operations in many environments. Our hardware platform consists of an Intel I7-4770 processor with 3.40 GHz clock frequency, 4 gigabytes memory and runs the Windows 7 operating system. A bilinear pairing P operation needs 4.211 milliseconds and a modular exponentiation E operation needs 1.709 milliseconds.

We summarize the comparisons of the four schemes in Table 1. The Generalized Signcrypt column and the Generalized Unsigncrypt column demonstrate the computational costs of each identity based generalized signcryption scheme. The Security Model column specifies the security model that the schemes rely on, where RO and SM represent Random Oracle and Standard Model, respectively.

Table 1. Comparison of identity based generalized signcryption schemes.

Schemes	Generalized Signcrypt	Generalized Unsigncrypt	Security Model
Lal et al. [20]	$6E + 1P = 14.456$ ms	$3P + 1E = 14.342$ ms	RO
Yu et al. [21]	$4E + 1P = 11.047$ ms	$3P + 3E = 17.76$ ms	RO
Kushwah et al. [22]	$4E = 6.836$ ms	$2P + 3E = 13.549$ ms	RO
Ours	$6E = 10.254$ ms	$5P + 2E = 24.473$ ms	SM

From Table 1, in Generalized Signcrypt, the computation cost of our scheme is less than Lal et al.'s scheme [20] and Yu et al.'s scheme [21] and more than Kushwash et al.'s scheme [22]. Our scheme has slightly higher computation costs than other schemes [20–22] in Generalized Unsigncrypt, whereas our scheme is proven secure in the standard model. To the best of our knowledge, it is the first scheme that is proven secure in the standard model. All previous schemes mentioned above have proven their security on the random oracle model. For some special applications that require very high security, it is believed that only those schemes that can be proven in the standard model must be employed. Thus, our scheme is suitable for secure e-mail and electronic commerce, where the confidentiality and authenticity are simultaneously or separately required to enable a secure and trustable communication environment.

6. Conclusions

The main purpose of identity based generalized signcryption is to reduce implementation complexity. According to different application environments, identity based generalized signcryption can fulfill the function of identity based signature, encryption or signcryption, respectively. In this paper, we proposed a concrete, ID-based generalized signcryption scheme based on the Paterson–Schuldt scheme. To the best of our knowledge, this is the first ID-based generalized signcryption scheme that can be proven secure in the standard model.

Acknowledgments: This work was supported by the National Natural Science Foundation of China (No. 61202438), the Key Project of Industry Science and Technology of Shaanxi Province (Nos. 2015GY021, 2015GY014) and the Project of Technology Transfer Promoting Engineering of Xi'an City (No. CXY1437(10)).

Author Contributions: Y. Ming conceived and designed the generalized signcryption scheme; X. Shen provided the secure proof and completed the paper writing; J. Feng performed the experiments and numerical analysis. All authors have read and approved the final manuscript.

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

References

1. Zheng, Y. Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption). In Proceedings of the Advances in Cryptology-Crypto'97, LNCS 1294, Santa Barbara, CA, USA, 17–21 August 1997.
2. Linn, J. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. Available online: https://www.rfc-editor.org/rfc/pdfrfc/rfc1421.txt.pdf (accessed on 14 March 2017).
3. Zheng, Y.; Imai, H. How to construct efficient signcryption schemes on elliptic curves. *Inf. Process. Lett.* **1998**, *68*, 227–233.

4. Bao, F.; Deng, R.H. A signcryption scheme with signature directly verifiable by public key. In Proceedings of the Public Key Cryptography-PKC'98, LNCS 1431, Yokohama, Japan, 5–6 February1998; pp. 55–59.
5. Malone-Lee, J.; Mao, W. Two birds one stone: Signcryption using RSA. In Proceedings of the Topics in Cryptology-CT-RSA'03, LNCS 2612, San Francisco, CA, USA, 13–17 April 2003; pp. 210–224.
6. Shamir, A. Identity-based cryptosystems and signature schemes. In Proceedings of the Advances in Cryptology-CRYPTO'84, LNCS 196, Santa Barbara, CA, USA, 19–22 August 1984; pp. 47–53.
7. Boneh, D.; Franklin, M. Identity-based encryption from the weil pairing. In Proceedings of the Advances in Cryptology-CRYPTO'01, LNCS 2139, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
8. Malone-Lee, J. Identity Based Signcryption. Cryptology ePrint Archive, Report 2002/098, 2002. Available online: http://eprint.iacr.org/2002/098 (accessed on 14 March 2017).
9. Libert, B.; Quisquator, J.J. A new identity based signcryption scheme from pairings. In Proceedings of the IEEE Information Theory Workshop-ITW'03, Paris, France, 31 March–4 April 2003; pp. 155–158.
10. Chow, S.S.M.; Yiu, S.M.; Hui, L.C.K.; Chow, K.P. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity. In Proceedings of the Information Security and Cryptology-ICISC'03, LNCS 2971, Seoul, Korea, 27–28 November 2004; pp. 352–369.
11. Boyen, X. Multipurpose identity based signcryption: A Swiss army knife for identity based cryptography. In Proceedings of the Advance in Cryptology-CRYPTO'03, LNCS 2729, Santa Barbara, CA, USA, 17–21 August 2003; pp. 383–399.
12. Chen, L.; Malone-Lee, J. Improved identity-based signcryption. In Proceedings of the Public Key Cryptography-PKC'05, LNCS 3386, Les Diablerets, Switzerland, 23–26 January 2005; pp. 362–379.
13. Barreto, P.S.L.M.; Libert, B.; McCullagh, N.; Quisquater, J.J. Efficient and provably-secure identity based signatures and signcryption from bilinear maps. In Proceedings of the Advance in Cryptology-ASIACRYPT'05, LNCS 3788, Chennai, India, 4–8 December 2005; pp. 515–532.
14. Selvi, S.S.D.; Vivek, S.S.; Rangan, C.P. Identity based public verifiable signcryption scheme. In Proceedings of the ProvSec'10, LNCS 6402, Malacca, Malaysia, 13–15 October 2010; pp. 244–260.
15. Yu, Y.; Yang, B.; Sun, Y.; Zhu, S. Identity based signcryption scheme without random oracles. *Comput. Stand. Interfaces* **2009**, *31*, 56–62.
16. 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.
17. Li, F.; Muhaya, F.B.; Zhang, M.; Takagi, T. Efficient identity-based signcryption in the standard model. In Proceedings of the ProvSec'11, LNCS 6980, Xi'an, China, 16–18 October 2011; pp. 120–137.
18. Han, Y.; Yang, X. ECGSC: Elliptic Curve Based Generalized Signcryption Scheme. Cryptology ePrint Archive, Report 2006/126, 2006. Available online: http://eprint.iacr.org/2006/126 (accessed on 14 March 2017).
19. Wang, X.; Yang, Y.; Han, Y. Provable Secure Generalized Signcryption. Cryptology ePrint Archive, Report 2007/173, 2007. Available online: http://eprint.iacr.org/2007/173 (accessed on 14 March 2017).
20. Lal, S.; Kushwah, P. ID Based Generalized Signcryption. Cryptology ePrint Archive, Report 2008/084, 2008. Available online: http://eprint.iacr.org/2008/084 (accessed on 14 March 2017).
21. Yu, G.; Ma, X.; Shen, Y.; Han, W. Provable secure identity based genrealized signcryption schem. *Theor. Comput. Sci.* 2010, 411, 3614–3624.
22. Kushwah, P.; Lal, S. An efficient identity based generalized signcryption scheme. *Theor. Comput. Sci.* 2011, 412, 6382–6389.
23. Bellare, M.; Rogaway, P. The exact security of digital signatures-how to sign with RSA and Rabin. In Proceedings of the Advances in Cryptology-EUROCRYPT'96, LNCS 0950, Kenmare, Ireland, 9–12 May 1996; pp. 399–416.
24. Canetti, R.; Goldreich, O.; Halevi, S. The random oracle methodology, revisited. In Proceedings of the Annual Symposium on the Theory of Computing-STOC'98, Dallas, TX, USA, 23–26 May 1998; pp. 209–218.
25. Paterson, K.G.; Schuldt, J.C.N. Efficient identity based signatures secure in the standard mode. In Proceedings of the Information Security and Privacy-ACISP'06, LNCS 4058, Melbourne, Australia, 3–5 July 2006; pp. 207–222.
26. Waters, R. Efficient identity based encryption without random oracles. In Proceedings of the Advance in Cryptology-Eurocrypt'05, LNCS 3494, Aarhus, Denmark, 22–26 May 2005; pp. 114–127.

27. Canetti, R.; Halevi, S.; Kate, J. Chosen-ciphertext security from identity-based encryption. In Proceedings of the Advance in Cryptology-Eurocrypt'04, LNCS 3027, Interlaken, Switzerland, 2–6 May 2004; pp. 207–222.
28. Shamus Software Ltd. MIRACL Library. Available online: http://www.shamus.ie/index.php?page=home (accessed on 1 May 2015).