A Survey on ID based and Certificateless Generalized Signcryption Scheme

DEEPA MISHRA\textsuperscript{*}  
Computer Science and Engineering,  
Acropolis Institute of Technology and Research  
SNIGDH SINGH  
Computer Science and Engineering,  
Acropolis Institute of Technology and Research

Abstract—Signcryption is basically a cryptographic primitive which provides both signature and encryption functions simultaneously, but it is not useful when only one of the function is required. Generalized Signcryption (GSC) is a special cryptographic primitive which can provide Signcryption function when security and authenticity are needed simultaneously, and can also provide encryption or signature function separately when any one of them is needed. Generalized signcryption (GSC) scheme can adaptively work as an encryption scheme, a signature scheme or a signcryption scheme with only one algorithm. It is very suitable for storage-constrained environments. In this paper we have surveyed the existing Generalized Signcryption (GSC) schemes and compare their security properties and efficiency. Along with this we also have proposed two schemes of which first one is an Identity based Generalized Signcryption Scheme and second one is a Certificateless Generalized Signcryption scheme which is a variation of Certificateless Signcryption scheme by Barbosa et al. We begin by giving formal definition of Generalized Signcryption (GSC) primitive and complete with comparative study with other models.

Keywords—Signcryption, Unsigncryption, PKG (Private Key Generator), Hash function, bilinear pairing, public key cryptography.

1. INTRODUCTION

Confidentiality and authenticity are two logically independent primitives of cryptography. To achieve confidentiality, an encryption scheme is used and authenticity is achieved through a signature scheme. There are scenarios where both the primitives are required. In this situation we use signcryption a primitive proposed by Zheng [1] in 1997. Signcryption performs encryption and signature both in a single logical step. However, in the low bandwidth environment we cannot afford to use three different schemes to achieve confidentiality or authenticity or both. In [2] Han et al. proposed the concept of generalized signcryption which can work as an encryption scheme, a signature scheme and a signcryption scheme as per need. Wang et al. [4] gave the first security model for a generalized signcryption scheme and modified the scheme proposed in [2]. Identity based cryptography was introduced by Shamir [3] in 1984. In the identity based cryptosystem public key of users are their identities and secret keys of user are created by a trusted third party called private key generator (PKG). First identity based signature scheme was given by Shamir [3] in 1984, but the first identity based encryption scheme was given by Boneh and Franklin [5] in 2001. The first identity based signcryption scheme was proposed by Malone Lee [6] in 2002. They also gave the security model for signcryption in identity based setting. Since then, many identity based signcryption schemes have been proposed in literature. The first identity based generalized signcryption along with a security model was proposed by Lal and Kushwah [7] in 2008. However, Yu et al. [8] show that security model for identity based generalized signcryption proposed in [7] is not complete. They modified the security model and proposed a concrete scheme which is secure in this model. In 2003, Al-Riyami and Paterson [9] proposed a new cryptographic primitive, certificateless public key cryptosystem, which avoid the key escrow problem and the need of certificate in public key cryptography. Barbosa and Frashim [10] in 2008 proposed a signcryption scheme in the certificateless setting. Recently, Ji et al. [11] modeled a security notion of generalized signcryption in certificateless setting and proposed a concrete scheme. However they have not given any security proof of their scheme. In this paper we surveyed an efficient identity based generalized signcryption and also an improved certificateless generalized Signcryption scheme.

II. PRELIMINARIES

A. Bilinear Pairing

Let \( G_1 \) be a cyclic additive group and \( G_2 \) be a cyclic multiplicative group both of the same prime order \( q \). Let \( P \) be an arbitrary generator of \( G_1 \) and \( a, b \) be the elements of \( \mathbb{Z}_q \). A function \( e: G_1 \times G_1 \rightarrow G_2 \) is called a bilinear pairing if it satisfies the following properties:

1. Bilinearity: for every \( P, Q, R \in G_1 \), we have \( e(P, Q + R) = e(P, Q)e(P, R) \) and \( e(P + Q, R) = e(P, R)e(Q, R) \).

Consecutively, for any \( a, b \in \mathbb{Z}_q \):

\[
\begin{align*}
    e(aP, bQ) &= e(P, Q)^{ab} = e(abP, Q) = e(P, abQ) = e(bP, Q)^a \\
    e(kP, Q) &= e(P, kQ) = e(P, Q)^k
\end{align*}
\]

2. Non-Degeneracy: If everything maps to the identity, thats obviously not desirable. If \( P \) is a generator of \( G_1 \), then \( e(P, P) \) is a generator of \( G_2 \). In other words there exist \( P \in G_1 \) such that \( e(P, P) \neq 1 \) where 1 is the identity element of \( G_2 \).

3. Computability: There exist an efficient algorithm to compute \( e(P, Q) \) for every \( P, Q \in G_1 \).
The pairing map $e$ is sometimes called an admissible pairing. A pairing is admissible if the mapping is also non-degenerate and computable ($e^*$).

B. Definition

Let be $e^*$: $G_1 \times G_2 \rightarrow G_3$ be a bilinear map. Let $g_1, g_2$ be two generators of $G_1, G_2$ respectively. The map $e$ is an admissible bilinear map if $e(g_1, g_2)$ generates $G_3$ and $e$ is efficiently computable.

III. ID BASED GENERALIZED SIGNCRIPTION SCHEME

A. Framework

An identity based generalized signcryption (IBGSC) consist the following algorithms:

1. Setup ($1^k$): This is a randomized algorithm run by PKG. This algorithm takes input a security parameter $k$ and outputs the system parameter params and a master secret key $s$ and master public key $mpk$.

2. Key Generation (mpk, msk, ID): On input ID, PKG uses it to compute a pair of corresponding public/private keys $(S_U, Q_U)$.

3. GSC: If sender $S$ wants to send a message $m$ to receiver $R$. This algorithm takes input $(S_U, ID_R, m)$ and outputs a signcrypted text $\sigma = \text{GSC}(S_U, m)$.

   - When $ID_R \neq ID_S$, $ID_R \neq ID_P$, $\sigma \leftarrow \text{GSC}(S_U, m) = \text{SC}(S_U, m)$.
   - When $ID_R \neq ID_S$, $ID_R = ID_P$, $\sigma \leftarrow \text{GSC}(S_U, m) = \text{Sign}(S_U, m)$.
   - When $ID_R = ID_S$, $ID_R \neq ID_P$, $\sigma \leftarrow \text{GSC}(S_U, m) = \text{Encrypt}(Q_R, m)$.

4. GUSC: This is unsigncryption algorithm. It takes input $(ID_S, S_R, \sigma)$ and outputs $m$ if $\sigma$ is valid Generalized signcryption done by sender $S$ for receiver $R$, otherwise output $\bot$ (false) if is not valid.

   - When $ID_R \neq ID_S$, $ID_R \neq ID_P$, $m \leftarrow \text{GUSC}(Q_S, m) = \text{SC}(Q_S, m)$.
   - When $ID_R \neq ID_S$, $ID_R = ID_P$, $(T, \bot) \leftarrow \text{GUSC}(Q_S, m) = \text{verify}(S_U, \sigma)$.
   - When $ID_R = ID_S$, $ID_R \neq ID_P$, $m \leftarrow \text{GUSC}(Q_S, m) = \text{Decrypt}(Q_S, m)$.

   There is no specific sender (or receiver) when we only encrypt (or sign) a message $m$ using IBGSC. We denote the absence of sender (or receiver) by $ID_P$. Thus to only sign or encrypt a message $m$, use $ID_R = ID_S$ or $ID_S = ID_P$. When there is no specific sender we only encrypt the message $m$ using MIDGSC, when information about sender is not needed MIDGSC, when information about sender is not needed MIDGSC becomes signature scheme and when both are there it will work as Signcryption scheme.

B. Description

Set up: Given a security parameter $1^k$, the PKG chooses two groups $G_1$ and $G_2$ of prime order $p$, a random generator $P$ of $G_1$ and a bilinear map $e: G_1 \times G_2 \rightarrow G_3$, three cryptographic hash functions as:

- $H_0: \{0,1\}^* \rightarrow Z_p^*$
- $H_1: G_1 \rightarrow Z_p^*$
- $H_2: \{0,1\}^* \rightarrow Z_p^*$

Where $n$ denotes the number of bits to represent a message. PKG chooses a random $msk \epsilon Z_p^*$ as master secret key and set $mpk = msk \times P$. A special function $f$ is defined as $f(ID) = 0$ if $ID = ID_S$, otherwise $f(ID) = 1$. (Assumptions $H_1(1) = 1$, $H_2(ID_S) = 0$). Also it is assumed that $Q_R = 0$. PKG publishes the system parameters as $\langle G_1, G_2, p, n, P, mpk, f, H_1, H_2, H_3 \rangle$.

Key Generation: Given a user with identity $ID_U$, its public key is $Q_U = H_0(ID_U)$ is a simple transformation of its identity. The private key is generated by the PKG as $S_U = s \cdot Q_U$.

Generalized Signcryption (GSC): If the sender $S$ with identity $ID_S$ has to send a message to the receiver $R$ with identity $ID_R$, it does as follows:

- Compute $f(ID_S)$ and $f(ID_R)$.
- Select $r$ uniformly from $Z_p^*$ and computes
  - $U \leftarrow r^p$
  - $W \leftarrow e(mpk, Q_R)^{f(ID_R)}$
  - $h_1 \leftarrow H_1(W)$
  - $h_2 \leftarrow H_2(U, W, m, Q_S, Q_R, ID_S, ID_R)$
  - $V \leftarrow h_2 P + f(ID_S) h_1 S_S$
  - $X \leftarrow r V$
  - $Q_R \leftarrow H_0(ID_R)$
  - $y \leftarrow m \parallel ID_S \parallel X \oplus h_1 f(ID_R)$
- Return $(U, y)$

Generalized Unsighncryption (GUSC): After receiving $(U, y)$ the receiver computes

- $f(ID_R)$
- $W \leftarrow e(U, S_R)^{f(ID_R)}$
- $h_1 \leftarrow H_1(W)$
- $m \parallel ID_S \parallel X \leftarrow h_1 f(ID_R) \oplus y$
- $h_2 \leftarrow H_2(U, W, m, Q_S, Q_R, ID_S, ID_R)$
The basic purpose of generalized signcryption is to reduce implementation complexity. As per need in different application environments, generalized signcryption can fulfill the function of signature, encryption or signcryption respectively. However, the computational and communication cost may increase compared with the normal signcrytion schemes.

### IV. EFFICIENCY ANALYSIS

The proposed scheme significantly reduces the extra computations and has comparable efficiency as compared to the existing efficiency identity based signcryption schemes [12,13,14]. In Table 1 we compare the computational complexity of our scheme with several other efficient existing signcryption schemes. Moreover, we compare our efficiency with other existing identity based generalized signcryption schemes [15,8]. Our scheme gives better performance as compared to IDGSC [15], and gives comparable efficiency as compared to NIDGSC [8]. Also, the proposed scheme uses less number of schemes as compared to other ID based generalized signcryption.

The Table 1 shows that the proposed scheme has comparable efficiency as compared to other existing signcryption schemes. Almost with same computational cost, the proposed can work as a signcryption scheme when both confidentiality and authentication are needed and as an encryption scheme or a signature scheme when anyone them is needed.

The Table 2 shows that the proposed scheme has better efficiency as compared to the IDGSC, and the comparable efficiency with respect NIDGSC. Overall as compared to all the existing scheme the proposed scheme uses less no of Hashing and hence it has got better efficiency than other schemes.

### V. CERTIFICATELESS GENERALIZED SIGNCRYPTION SCHEME

#### A. Framework

A certificateless generalized signcryption (CLGSC) consists of the following algorithms:

1. Setup(\(1^k\)): This is a global set up algorithm, which takes input the security parameter \(1^k\) and outputs the KGC’s secret key msk and global parameters params including a master public key mpk. This algorithm is executed by the KGC, which publishes params.

2. Extract-Partial-Private-Key (ID\(_i\), msk, params): Given input params, msk (master secret key) and a user’s identity ID\(_i\) \(\in [0,1]\), it outputs a partial private key D\(_i\). This algorithm is run by KGC, after verifying the users identity.

3. Generate User Key (ID\(_i\), params): An algorithm which takes input as an identity and the public parameters and outputs a secret value x and a public key PK. This algorithm is run by a user to obtain a public key and a secret value which will be used for constructing full private key. The public key is published without certification.
4. Set Private Key (D_{U}, x, params): A deterministic algorithm which takes as input a partial secret key D_{U} and secret value x and outputs the full private key S_{U}. This algorithm is run by a user to construct a full private key.

5. CLGSC (m,S_{U}, D_{U}): This algorithm has three scenarios:

- **Signcryption Mode**: If sender S wants to transmit a message m to receiver B such that both confidentiality and authentication need to be maintained then the input is (m,S_{U}, D_{U}), output is \( \sigma = CLGSC(m,S_{U}, D_{U}) = \text{Signcrypt}(m,S_{U}, D_{U}) \).
- **Signature only Mode**: If sender S wants to send message m without definite receiver, the input is (m,S_{U}, D_{U}), where D_{U} means receiver is null, the output is \( \sigma = CLGSC(m,S_{U}, D_{U}) = \text{sign}(m, S_{U}) \).
- **Encryption only Mode**: If someone wants to send a message m to a definite receiver R confidentially and private key S_{R}, the signature on m by S, \( (m,S_{R}) \), after receiving \( \sigma \), if it is valid, the receiver R decrypts the cipher text and returns the message m and the signature on m by S, otherwise return false (⊥).

There is no specific sender (receiver) when we only encrypt (only sign) a message & using

**B. Description**

In this section we proposed a new CLGSC scheme based on the certificateless signcryption scheme proposed in [10] scheme.

Set up(1^{st}) : Given a security parameter k, the KGC chooses two groups G_{1}, G_{2} of prime order p, a random generator P of G_{1}, a bilinear map e: G_{1} x G_{1} → G_{2}, four cryptographic hash function as:

- \( H_{1}: \{0,1\}^{*} \rightarrow G_{1} \)
- \( H_{2}: \{0,1\}^{*} \rightarrow \{0,1\}^{n} \)
- \( H_{3}: \{0,1\}^{*} \rightarrow G_{1} \)

Where n denotes the number of bits to represent a message. A special function f is defined as f(ID)=0, if ID = ID_{φ} otherwise f(ID)=1. \( ID_{φ}, PK_{φ} \) and \( S_{φ} \) are parsed as strings of zero. KGC chooses a random \( msk \in Z_{p}^{*} \) as master secret key and set mpk = msk x P. KGC publishes the system parameters as < G_{1}, G_{2}, p, n, P, mpk, f, H_{1}, H_{2}, H_{3}>.

Extract Private Key: Given a user with identity ID_{U}, the partial private key is computed by KGC as D_{U} = mskQ_{U} = mskH_{1}(ID_{U}).

Generate User Keys: Given D_{U}, the user with identity ID_{U} chooses a random \( x_{U} \in Z_{p}^{*} \) and sets its public key \( PK_{U} = x_{U}P \) and private key \( S_{U} = \langle x_{U}, D_{U} \rangle \).

**CLGSC(m, ID_{S}, S_{U}, IS, PK_{S}, PK_{R}, mpk):**

1. Computes f(ID_{S}) and f(ID_{R}), Selects r uniformly from \( Z_{p}^{*} \).
2. Compute
   - \( U \leftarrow rP, T \leftarrow e(mpk, Q_{U})f(ID_{R}) \)
   - \( h \leftarrow H_{2}(U, TrPK_{S}, ID_{S}, ID_{R}, PK_{S}, PK_{R}) \cdot f(ID_{R}) \)
   - \( V \leftarrow m \oplus h \)
   - \( H \leftarrow H_{1}(U, V, ID_{S}, ID_{R}, PK_{S}, PK_{R}) \)
   - \( W \leftarrow f(ID_{S}) \cdot (D_{U} + x_{S}H) + rH \)
3. Return \( \sigma = (U,V,W) \)

**CLDGSC(σ, ID_{S}, IS, IS, PK_{S}, PK_{R}, mpk):** After receiving σ from sender S, the receiver R parses σ as U,V,W and

1. Computes f(ID_{R}), f(ID_{S})
2. Computes H \( \leftarrow H_{1}(U, V, ID_{S}, ID_{R}, PK_{S}, PK_{R}) \)
3. Check if e(P,W) \( \neq f(ID_{S}) \cdot e(U + PK_{S}, H) \) return ⊥, else computes
   - \( T \leftarrow (U, D_{R}), \) parse \( S_{R} \) as \( (x_{R}, D_{R}) \)
   - \( h \leftarrow H_{2}(U, Trx_{R}U, ID_{S}, ID_{R}, PK_{S}, PK_{R}) \)
   - \( m \leftarrow V \oplus h \)
4. Return m

Consistency:
- \( T = e(U, D_{U}) = e(P, mskQ_{U}) = e(rP, Q_{U})^{msk} = e(r \cdot msk \cdot P, Q_{U}) = e(r \cdot MPkH_{1}(ID_{S})) \cdot e((r + x_{S}H)P, H) = e(mskP, H_{1}(ID_{S}))e(U + PK_{S}, H) = e(mpk, Q_{U})e(U + PK_{S}, H) \)

VI. EFFICIENCY ANALYSIS

Computation time and cipher text size are two important parameters affecting the efficiency of a cryptographic scheme. We present a comparison of our scheme with other existing CLGSC schemes with respect to these parameters. The Table 3 shows that Barbosa et. al.’s signcryption scheme[10] has the same cipher text size and efficiency as our scheme. That means both the schemes have the same computation and communication complexity. But in terms of implementation complexity our scheme is better than first one because, Barbosa et. al.’s certificateless signcryption[10] scheme cannot work as signature only or encryption only mode, but our scheme can adaptively work as a signcryption scheme when both confidentiality and authentication are needed and as an encryption scheme or a signature scheme when anyone them is needed.


In this paper we proposed two generalized signcryption schemes, first is identity based and second is certificateless. Generalized Signcryption is a multi-functional subroutine which can adaptively work as an encryption scheme or signcryption scheme. According to the comparison to other schemes, the proposed schemes are efficient. Due to the computation of the pairing being still time consuming the schemes can be further improved by reducing the number of pairing operations at the same time maintaining the efficiency.

| Schemes          | Ciphertext size | | | | Signcryption | | | | | | Designcryption | | | |
|------------------|-----------------|---|---|---|---|---|---|---|---|---|---|---|---|
|                  |                 | E | M | P | H | E | M | P | H |
| Barbosa et. Al   | $2G_1 + m$      | 1 | 4 | 0(+1) | 3 | 0 | 1 | 4(+1) | 3 |
| Proposed Scheme  | $2G_1 + m$      | 1 | 4 | 0(+1) | 3 | 0 | 1 | 4(+1) | 3 |

Table 3

Here, M: number of point multiplications in $G_1$; E: number of exponentiation in $G_2$; P: number of pairing of computations; H: number of hash function; (+): pre-computation of pairing; $|G_1|$: size of an element in $G_1$; $|G_2|$: size of an element in $G_2$; $|m|$: length of message m; $|ID|$: length of Identity; $|P|$: size of an element in $Z_p$.

Table 4 shows that the proposed scheme has smaller text size as compared to first two schemes but has same size as third scheme. But as compared to all the existing scheme our scheme uses less no of hashing and hence it has got better efficiency than other schemes.

VII. CONCLUSIONS

In this paper we proposed two generalized signcryption scheme, first is identity based and second is certificateless. Generalized Signcryption is a multi-functional subroutine which can adaptively work as an encryption scheme or signcryption scheme. According to the comparison to other schemes, the proposed schemes are efficient. Due to the computation of the pairing being still time consuming the schemes can be further improved by reducing the number of pairing operations at the same time maintaining the efficiency.

REFERENCES


