International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163
Issue 11, Volume 2 (November 2015) www.ijirae.com

A Survey on ID based and Certificateless Generalized Signcryption Scheme

DEEPA MISHRA*
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 authencity 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.

I. 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 a 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 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 $e(P,Q + R) = e(P,Q)e(P,R)$, $e(P+Q,R) = e(P,R)e(Q,R)$

Consecutively, for any $a,b \in Z_q^*$:

$e(aP,bQ) = e(P,Q)^{ab} = e(abP,Q) = e(P,abQ) = e(bP,Q)^a$

$e(kP,Q) = e(P,kQ) = e(P,Q)^k$

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 $P,Q \in G_1$.

© 2014- 15, IJIRAE- All Rights Reserved

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^: $G_1 \times G_2 \rightarrow G_t$ 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_t and e is efficiently computable.

III. *ID BASED GENERALIZED SIGNCRYPTION 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_S, ID_R, m) and outputs a signcrypted text σ = MIDGSC(S_s, ID_R, m).
   - When $ID_S \neq ID_\phi$, $ID_R \neq ID_\phi$, $\sigma \leftarrow$ GSC(S_s, Q_R, m) = SC(S_s, Q_R, m).
   - When $ID_S \neq ID_\phi$, $ID_R = ID_\phi$, $\sigma \leftarrow$ GSC(S_s, Q_R, m) = Sign(S_s, m).
   - When $ID_S = ID_\phi$, $ID_R \neq ID_\phi$, $\sigma \leftarrow$ GSC(S_s, Q_R, m) = Encrypt(Q_R, m).
4. GUSC: This is unsigncryption algorithm. It takes input (ID_S, S_R, σ) and outputs m if σ is valid Generalized signcryption done by sender S for receiver R, otherwise output $\perp$ (false) if is not valid.
   - When $ID_S \neq ID_\phi$, $ID_R \neq ID_\phi$, m $\leftarrow$ GUSC(Q_s, S_R, δ) = USC(Q_s, S_R, δ).
   - When $ID_S \neq ID_\phi$, $ID_R = ID_\phi$, (T,$\perp$) $\leftarrow$ GUSC(Q_s, S_R, δ) = verify(S_s, δ).
   - When $ID_S = ID_\phi$, $ID_R \neq ID_\phi$, m $\leftarrow$ GUSC(Q_s, S_R, δ) = Decrypt(Q_R, δ).

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_ϕ. Thus to only sign or encrypt a message m, use $ID_R = ID_\phi$ or $ID_S = ID_\phi$. 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: $G_1 \times G_2 \rightarrow G_1$, three cryptographic hash functions as:

- $H_0 : \{0,1\}^* \rightarrow Z_p^*$
- $H_1 : G_2 \rightarrow Z_p^*$
- $H_2 : \{0,1\}^* \rightarrow Z_p^*$

Where n denotes the number of bits to represent a message. PKG chooses a random msk $\in Z_p^*$ as master secret key and set mpk = msk x P. A special function f is defined as f(ID) = 0 if ID = ID_ϕ, otherwise f(ID) = 1.(Assumptions $H_1(1) = 1$, $H_0(ID_\phi) = 0$). Also it is assumed that $Q_\phi = 0$. PKG publishes the system parameters as <G_1, G_2, p, n, P, mpk, f, H_1, H_2, H_3>.

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 $S_U = s\, Q_U$.

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 s, r uniformly from Z_p^* and computes
  - $U \leftarrow rP$
  - $W \leftarrow e(mpk, Q_R)^{rf(IDR)}$
  - $h_1 \leftarrow H_1(W)$
  - $h_2 \leftarrow H_2(U, W, m, Q_s, Q_R, ID_S, ID_R)$
  - $V \leftarrow h_2P + f(ID_S)\, h_1S_S$
  - $X \leftarrow rV$
  - $Q_R \leftarrow H_0(ID_R)$
  - $y \leftarrow m \| ID_S \| X \oplus h_1 f(ID_R)$
- Return (U,y)

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

- f(ID_R)
- $W \leftarrow e(U, S_R)^{f(IDR)}$
- $h_1 \leftarrow H_1(W)$
- $m \| ID_S \| X \leftarrow h_1 f(ID_R) \oplus y$
- $h_2 \leftarrow H_2(U, W, m, Q_s, Q_R, ID_S, ID_R)$

© 2014- 15, IJIRAE- All Rights Reserved

Checks if $e(P,X) \neq e(U,P)^{h2}\, e(r \cdot mpk, Q_S)^{h1f(IDR)}$ return $\perp$, else return m.

Consistency:

- $W = e(mpk, Q_R)^{rf(IDR)} = e(sP. Q_R)^{rf(IDR)}$
  $= e(sP. Q_R)^{rf(IDR)} = e(rP,S_R)^{f(IDR)}$
  $= e(U, S_R)^{f(IDR)}$
- $e(P,X) = e(P,rV) = e(rP,V)$
  $= e(rP,h_2P + f(ID_S)h_1S_S)$
  $= e(rP,h_2P)\, e(rP, f(ID_S)h_1S_S)$
  $= e(U,P)^{h2}\, e(rP, S_S)^{f(IDS)h1}$
  $= e(U,P)^{h2}\, e(rP, sQ_S)^{f(IDS)h1}$
  $= e(U,P)^{h2}\, e(rsP, Q_S)^{f(IDS)h1}$
  $= e(U,P)^{h2}\, e(r\ mpk, Q_S)^{f(IDS)h1}$

IV. EFFICIENCY ANALYSIS

The basic purpose of generalized signcryption is to reduce implementation complexity. As per need in different application environments, generalized signcryption can fulfil the function of signature, encryption or signcryption respectively. However, the computational and communication cost may increase compared with the normal signcryption schemes.

Schemes	*Signcryption*			*Unsigncryption*		
	M	*E*	*P*	*M*	*E*	*P*
Malone Lee's	*3*	*0*	*0(+1)*	*0*	*1*	*3(+1)*
Libert Quisqater's	*2*	*2*	*0(+2)*	*0*	*2*	*3(+2)*
X Boyen's	*3*	*1*	*0(+1)*	*2*	*0*	*3(+1)*
Chow et al's	*2*	*0*	*0(+2)*	*1*	*0*	*4*
Proposed Scheme	*3*	*1*	*0(+1)*	*1*	*2*	*2(+2)*

Table 1

Schemes	*Generalized Signcryption*				*Generalized Unsigncryption*			
	M	*E*	*P*	*H*	*M*	*E*	*P*	*H*
IDGSC	*5*	*0*	*0(+1)*	*3*	*1*	*0*	*3(+1)*	*3*
NIDGSC	*3*	*1*	*0(+1)*	*4*	*0*	*2*	*2(+2)*	*3*
Proposed Scheme	*3*	*1*	*0(+1)*	*3*	*1*	*2*	*2(+2)*	*2*

Table 2

Here, M:number of point multiplications in G_1; E: number of exponentiation in G_2; P: number of pairing computations; (+): pre-computation of pairing and H: number of hash function.

The proposed scheme significantly reduces the extra computations and has comparable efficiency as compared to the existing efficient 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 SIGNCRYTION 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_U, msk, params): Given input params, msk (master secret key) and a user's identity $ID_U \in \{0,1\}$, it outputs a partial private key D_U. This algorithm is run by KGC, after verifying the users identity.
3. Generate User Key (ID_U, 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.

© 2014- 15, IJIRAE- All Rights Reserved

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_S, ID_R): This algorithm has three scenario-

- Signcryption Mode: If sender S wants to transmit a message m to receiver B such that both confidentially and authentication need to be maintained then the input is (m,S_S, ID_R), output is σ = CLGSC(m,S_S, ID_R) = Signcrypt(m,S_S, ID_R).
- Signature only Mode: If sender S wants to send message m without definite receiver, the input is (m,S_S, ID_ϕ), where ID_ϕ means receiver is null, the output is σ = CLGSC(m,S_S, ID_ϕ) = sign(m, S_S).
- Encryption only Mode: If someone wants to send a message m to a definite receiver R confidentially, the input is (m,S_ϕ, ID_R), where S_ϕ means the receiver is null, the output is σ = encrypt(m, ID_R).

5. CLDGSC (σ, ID_s, ID_R): After receiving σ, 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 certicateless signcryption scheme proposed in [10] scheme.

Set up(1^k): 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 $G_1 \rightarrow G_2$, 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 ∈ 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 Partial Private key: Given a user with identity ID_U, the partial private key is computed by KGC as D_U = mskQ_U = msk$H_1(ID_U)$.

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 $S_U = < x_U, D_U >$.

CLGSC(m, ID_S, ID_R, S_S, PK_S, PK_R, mpk):

1. Computes f(ID_s) and f(ID_R), Selects r uniformaly from Z_p^*.
2. Compute
   - $U \leftarrow rP$, $T \leftarrow e(mpk, Q_R)^r f(ID_R)$
   - $h \leftarrow H_2(U, T, rPK_R, ID_s, ID_R, PK_S, PK_R)\, f(ID_R)$
   - $V \leftarrow m \oplus h$
   - $H \leftarrow H_3(U, V, ID_s, ID_R, PK_S, PK_R)$
   - $W \leftarrow f(ID_s)[D_s + x_S H] + rH$
3. Return $\sigma \leftarrow (U,V,W)$

CLDGS(σ, ID_S, ID_R, S_S, 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 $H \leftarrow H_3(U, V, ID_s, ID_R, PK_S, PK_R)^{f(IDR)}$
3. Check if $e(P,W) \neq e(mpk, Q_S)^{f(IDS)}\, e(U + PK_S, H)$ return ⊥ else computes
   - $T \leftarrow (U, D_R)$, parse S_R as (x_R, D_R)
   - $h \leftarrow H_2(U, T, x_R U, ID_s, ID_R, PK_S, PK_R)$
   - $m \leftarrow V \oplus h$
4. return m

Consistency:

- $T = e(U, D_R) = e(rP, msk\, Q_R) = e(rP, Q_R)^{msk} = e(r \cdot msk \cdot P, Q_R) = e(r \cdot mpk \cdot P, Q_R)$ $e = (mpk, Q_R)^r$
- $e(P,W) = e(P, D_S + x_S \cdot H + rH) = e(P, mskH_1(ID_S))e((r+x_S)P, H) = e(mskP, H_1(ID_S))e(U+PK_S, H) = e(mpk, Q_S)e(U+PK_S, H)$

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.

© 2014- 15, IJIRAE- All Rights Reserved

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

Table 3

Schemes	Ciphertext size	GSC				GDSC			
		E	M	P	H	E	M	P	H
Ji et. al.[11]	$2\|G_1\|+\|m\|+\|ID\|+\|G_2\|+\|P\|$	3	2	0	4	1	1	2	4
Kushwah et. al.[16]	$2\|G_1\|+\|m\|+\|ID\|+\|G_2\|$	2	3	0	3	1	3	2	3
Zhou et al. [17]	$2\|G_1\|+\|m\|$	1	4	0(+1)	3	0	1	4(+1)	3
Proposed Scheme	$2\|G_1\|+\|m\|$	1	4	0(+1)	2	0	1	4(+1)	2

Table 4

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 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 comparision 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 no of pairing operations at the same time maintaining the efficiency.

REFERENCES

[1] Y. Zheng: Digital signcryption or how to achieve cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption), CRYPTO'97, LNCS # 1294, pp. 165-179, Springer-Verlag, 1997.
[2] Y. Han and X. Yang: ECGSC: Elliptic curve based generalized signcryption scheme. Cryptology ePrint Archive, Report 2006/126, 2006, http:/eprint.iacr.org/.
[3] A. Shamir: Identity-based cryptosystems and signature schemes. CRYPTO 84, LNCS # 196, pp 47-53 Springer-Verlag, 1984.
[4] X. Wang, Y. Yang and Y. Han: Provable secure generalized signcryption. Cryptology ePrint Archive, Report 2007/173, 2007, http:/eprint.iacr.org/.
[5] D. Boneh and M. Franklin: Identity–based encryption scheme from Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 2001, 213-229.
[6] J. Malone-Lee: Identity-based signcryption, Cryptology ePrint Archive Report 2002/098.
[7] S. Lal and P. Kushwah: ID based generalized signcryption. Cryptology ePrint Archive, Report 2008/84, http://eprint.iacr.org/ 2008/84.pdf, 2008.
[8] G. Yu, X. Ma, Y. Shen and W. Han: Provable secure identity based generalized signcryption scheme. Available at arXiv:1004.1304v1 [cs.CR], (to appear in Theoretical Computer Science), 2010.
[9] S. S. Al-Riyami and K. G. Paterson: Certificateless public key cryptography. ASIACRYPT 2003, LNCS # 2894, pp. 452-473 Springer-Verlag, 2003.
[10] M. Barbosa and P. Farshim: Certificateless signcryption. Proceedings of the 2008 ACM Symposium on Information, Computer and Communication Security, pp. 369-372, 2008.
[11] H. Ji, W. Han and L. Zhao: Certificateless generalized signcryption. Cryptology ePrint Archive, Report 2010/204, http://eprint.iacr.org/ 2010/204.pdf, 2010.
[12] B. Libert and Jean-Jacques Quisquater. A new identity based signcryption scheme from pairings. In Information Theory Workshop, 2003. Proceedings. 2003 IEEE, pages 155–158.IEEE, 2003.
[13] J. Malone-Lee. Identity-based signcryption, 2002.
[14] S. SM Chow, Siu-Ming Yiu, L. CK Hui, and KP Chow. Efficient forward and provably secure id-based signcryption scheme with public verifiability and public ciphertext authenticity. In Information Security and Cryptology-ICISC 2003, pages 352–369. Springer,2004.
[15] S. Lal and P. Kushwah. Id based generalized signcryption, 2008.
[16] P. Kushwah and S. Lal. Efficient generalized signcryption schemes, 2010.
[17] C. Zhou, W. Zhou, and X. Dong. Provable certificateless generalized signcryption scheme. Designs, Codes and Cryptography, pages 1–16, 2012.

© 2014- 15, IJIRAE- All Rights Reserved