International Journal of Theoretical & Applied Sciences, **1**(2)**:** 88-92(2009) **ISSN : 0975-1718**

An efficient and publicly verifiable Id-based multi-signcryption scheme

Munendra Aggarwal, Prashant Kushwah and Sunder Lal*

Department of Mathematics, Dr. B.R. Ambedkar University Agra, (UP) INDIA
**Professor and Pro-Vice Chancellor, Dr. B.R. Ambedkar University Agra, (UP) INDIA*

ABSTRACT : Multi-signcryption is used when different senders wants to authenticate a single message without revealing it. This paper proposes a multi signcryption scheme in which no pairing is computed on the signcryption stage and the signatures can be verified publicly.

Keywords : Identity based cryptography, Signcryption, Multi-Signcryption, Bilinear pairing

INTRODUCTION

Secure message transmission over an insecure channel, require both confidentiality and authenticity, which may be achieved through 'signature then encryption' approach. However, in 1997 Zheng [17] proposed a cryptographic primitive "Signcryption" which achieves both confidentiality and authenticity in a single logical step with much lower computational cost than signature then encryption approach. Beak *et. al.,* [2] gave formal security model for signcryption scheme and provided security proof for Zheng's scheme in random oracle model.

1984, Shamir [14] introduced the concept of identity based cryptography and gave the first identity based signature scheme. The idea of identity based cryptography is to enable a user to use any arbitrary string that uniquely identifies him as his public key. Identity based cryptography serves as an efficient alternative to Public Key Infrastructure (PKI) based system. In 2001, Boneh and Franklin [5] gave the first identity based encryption scheme and in 2003 Malone-Lee [9] gave the first identity based signcryption scheme. He also considered security notions of signcryption in identity based setting. Since then many signcryption schemes have been proposed.

In 1989, Boyed [5] defined multi signature scheme the scenario where more than one user authenticate a single message in such a way that a verifier verify only a single compact signature on that message. An identity based version of multi-signature was given by Gentry et al. [7] in 2006. Mitomi *et. al.,* [10] include confidentiality in multi-signature by signcrypting the message. Zhang et al. [15] gave an identity based multi-signcryption scheme. However, S. Deva *et. al.,* [12] find some flaw and fix them. Recently Zhang *et. al.,* [16] came up with a new multi-signcryption scheme in identity based setting which to the best our knowledge is most efficient scheme till date.

The concept of multi-receiver setting was first given by Bellare *et. al.,* [3] for public key encryption where, there are n receivers numbered by $1,\ldots,n$ and each of them generates for itself a private key and public key pair denoted by (sk_i, pk_i). A sender encrypts a message m using pk_i to obtain C_i for $i = 1,\ldots,n$ and then sends $(C_1,\ldots,C_n)$ as a ciphertext. Upon receiving the ciphertext, receiver i extract C_i and decrypt it using sk_i. Beak *et. al.,* [1] formalized identity based encryption to the multiple receivers setting. Duan and Cao [6] consider the situation where there is not only multiple receiver but also multiple senders. As an example, consider that there are several managers, each of whom wants to securely broadcast an e-mail to the employees of the company independently. Once an employee receives several ciphertexts from different managers, an issue of message authentication will arise. In such case confidentiality and authenticity required simultaneously. Motivated by this Duan and Cao [6] gave the first multi-receiver identity based signcryption scheme. Later on some more multi-receiver identity based signcryption schemes were proposed [8, 11, 13].

In this paper, we propose an identity based multi-signcryption scheme which is more efficient then the schemes S. Deva et. al [12] and Zhang *et. al.,* [16]. Our scheme needs no pairing computation on the signcryption stage. The scheme also possesses public verifiability for signature. We also convert our proposed scheme for multiple receivers, which we believe is the first multi-signcryption scheme for multiple receivers.

PRELIMINARIES

Let G_1 be an additive group and G_2 be a multiplicative group, of the same prime order q. A function $e : G_1 \times G_1 \rightarrow G_2$ is called a **bilinear pairing** if it satisfies the following properties :

(*i*) $\forall P, Q \in G_1, \forall a, b \in Z^*_q$, $e(aP, bQ) = e(P, Q)^{ab}$

(*ii*) For any point $P \in G_1$,$e(P, Q) = 1$ for all $Q \in G_1$, if only if $P = O$, the identity of G_1.

(*iii*) There exists an efficient algorithm to compute $e(P, Q)$ $\forall P, Q \in G_1$.

Given $(P, aP, bP) \in G_1$ for unknown $a, b \in Z^*$, the Computational Diffie-Hellman Problem **(CDH Problem)** in G_1 is to compute abP.

Given two groups G_1 and G_2 of the same prime order q, a bilinear map $e : G_1 \times G_1 \to G_2$, a generator P of G_1, three elements aP, bP, cP of G_1 and an element $H \in G_2$, the Decisional Bilinear Diffie-Hellman Problem **(DBDH Problem)** is to decide whether $H = e(P, P)^{abc}$.

Before giving the proposed multi-signcryption scheme, first we formalize **Identity based Multi-Signcryption**

An Identity based Multi- Signcryption scheme consists of the following algorithms :

(*i*) **Setup.** Given a security parameter k, the Private Key Generator (PKG) chooses a secret value randomly and generates master secret key *msk* and the public parameters *params* of the system.

(*ii*) **Key Extract.** Given a user identity $ID \in \{0, 1\}^*$, the PKG computes the corresponding private key S and transmits it to the user in a secure way.

(*iii*) **Signcrypt.** Different users with identities $L = \{ID_1, ..., ID_n\}$ run this algorithm to signcrypt a message m to the receiver's identity ID_B to obtain signcryption σ.

(*iv*) **Unsigncrypt.** The receiver B with identity ID_B and private key S_B runs this algorithm to obtain plaintext m, if σ is a valid signcryption from L to identity ID_B otherwise return $\perp$.

For consistency, we require that if

s = signcrypt (m, $L = \{ID_1, ..., ID_n\}$, $S_1, ..., S_n$, ID_B, then m = unsigncrypt (σ, $L = \{ID_1, ..., ID_n\}$, ID_B, S_B)

THE PROPOSED SCHEME

Setup. Given k is the security parameter, the PKG chooses the system parameter that includes two groups G_1, G_2 of same prime order q, a bilinear map $e : G_1 \times G_1 \to G_2$, a generator $P \in G_1$, randomly chosen $s \in_R Z_q$, $R \in_R G_1$ $(R \neq P, O)$ and computes $P_{pub} = sP \in G_1$ and $q = e(P_{pub}, R)$. The PKG also chooses cryptographic hash functions $H_0 : \{0, 1\}^* \to G_1$, $H_1 : G_2 \to \{0, 1\}^l$ $H_2 : \{0, 1\}^l \times G_1 \times G_1 \to Z^*_q$ where l is the length of plaintext and ciphertext .

The system public parameters are params = $<q, G_1, G_2, e, l, P, P_{pub}, \theta, R, H_0, H_1, H_2>$.

Key Extract. Given a user identity $ID \in \{0, 1\}^*$, PKG compute public key $Q_{ID} = H_0(ID)$and private key $S_{ID} = sQ_{ID}$.

Signcrypt. Given a message $m \in \{0, 1\}^l$, a receiver's identity ID_B and n senders' identities $L = \{ID_1, ..., ID_n\}$, each user ID_i executes the following steps

(*i*) Randomly chooses $x_i \in \mathbb{Z}^*_q$ and computes $X_i = x_iP$, $Y_i = \theta^{x_i}$ and $U_i = x_i(R + Q_B)$.

(*ii*) Sends (X_i, Y_i, U_i) to other signers through a secure channel.

(*iii*) After receiving from the other signers (X_j, Y_j, U_j), user ID_i computes.

(*a*) $X = \sum_{i=1}^{n} X_i$, $Y = \sum_{i=1}^{n} Y_i$, $Q = \sum_{i=1}^{n} Q_i$ and $U = \sum_{i=1}^{n} U_i$.

(*b*) $c = H_1(Y) \oplus m$.

(*c*) $h = H_2(c, X, U)$

(*d*) $Z_i = hS_i + x_iQ$.

(*iv*) Each user sends Z_i to other users. Every user computes Z and outputs ciphertext σ, where $Z = \sum_{i=1}^{n} Z_i$ and $\sigma = <c, X, Z, U, L>$.

Unsigncrypt: To unsigncrypt the ciphertext $\sigma = <c, X, Z, U, L>$, the receiver with identity ID_B computes

(*i*) $h = H_2(c, X, U)$, and accepts iff

(*ii*) $e(P, Z) = e(X + hP_{pub}, Q)$. It then computes

(*iii*) $Y' = e(P_{pub}, U)\, e(X, S_B)^{-1}$, and recovers

(*iv*) $m = c \oplus H_1(Y')$.

SECURITY

(i) Confidentiality: Without knowing the secrete key of receiver, no one can compute $Y = \prod_{i=l}^{n} Y_i = \theta^{(x_1+...+x_n)} = e(P_{pub}, R)^{(x_1+...+x_n)}$. It is only the specific receiver who can compute the actual value of Y using secrete key as

$$Y¢ = e(P_{pub}, U)\, e(X, S_B)^{-1}$$

$$= e(P_{pub}, \sum_{i=1}^{n} U_i)\, e(X, S_B)^{-1}$$

$$= e(P_{pub}, \sum_{i=1}^{n} x_i(R + Q_B))\, e(X, S_B)^{-1}$$

$$= e(P_{pub}, \sum_{i=1}^{n} x_i(R + Q_B))\, e(X, S_B)^{-1}$$

$$= e(P_{pub}, \sum_{i=1}^{n} x_i R)\ e(sP_{pub}, \sum_{i=1}^{n} x_i Q_B)\ e(X, S_B)^{-1}$$

$$= e(P_{pub}, (x_1 + ... + x_n) R)\ e(sP, (x_1 + ... + x_n) Q_B)\ e(X, S_B)^{-1}$$

$$= e(P_{pub}, R)^{(x_1 + ... + x_n)}\ e((x_1 + ... + x_n)P, sQ_B)\ e(X, S_B)^{-1}$$

$$= \theta^{(x_1 + ... + x_n)}\ e(X, S_B) e\ (X, S_B)^{-1}$$

$$= \theta^{(x_1 + ... + x_n)} = Y.$$

(ii) Public Verifiability: Any one who has access to the signcryptext can verify the signature on the ciphertext which it contains. First the verifier computes $h = H_2(c, X, U)$ and $Q = \sum_{i=1}^{n} Q_i$,then checks

$$e(P, Z) = e(P, \sum_{i=1}^{n} (hS_i + x_i Q))$$

$$= e(P, \sum_{i=1}^{n} hS_i)\, e(P, \sum_{i=1}^{n} x_i Q)$$

$$= e(P, \sum_{i=1}^{n} hsQ_i)\, e(P, \sum_{i=1}^{n} x_i Q)$$

$$= e(P, hs \sum_{i=1}^{n} Q_i)\, e(P, (x_1 + ... + x_n)Q)$$

$$= e(P, hsQ) e((x_1 + ... + x_n)P, Q)$$

$$= e(hsP, Q) e(X, Q)$$

$$= e(hP_{pub}, Q) e(X, Q)$$

$$= e(X + hP_{pub}, Q)$$

(iii) Unforgeability: Signcryptext is generated using the secret key S_i of each of the signers. Thus no one, not even the one among signers can generate a valid signcryptext without knowing the secret key of **all** the signers.

EFFICIENCY COMPARISON

We compare efficiency of our scheme with existing schemes [12, 16]. We consider the costly operations which include scalar multiplications in G_1 (G_1 Mul), exponentiations in G_2 (G_2 Exp) and pairing operations (Pairing) as shown below (in table 1)

REMARKS

(*i*) In the proposed schemes, we use the concept of Duan and Cao [6] which they proposed to construct an Identity based Multi-receiver signcryption scheme.

(*ii*) One of the important advantages of the proposed scheme is that no pairing computation is needed for signcryption. This makes the scheme quite efficient.

(*iii*) To achieve efficiency in Zhang et al. scheme [16], only one signer will compute the signcryptext but in our scheme every user can generates own copy of signcryptext.

(*iv*) The proposed scheme is publicly verifiable. Any one who can access to the signcryptext can verify the signature on ciphertext c. Thus the proposed scheme is more applicable when signing a joint confidential contract between two or more organizations. Any one can verify the authenticity of the contract without getting any knowledge of it, however, only the authority can read the contract.

Table : 1

	Signcrypt			**Unsigncrypt**		
	G_1 Mul	G_2 Exp	Pairing	G_2 Mul	G_2 Exp	Pairing
S. Deva et al. [12]	3n	n	n	0	1	4
Zhang et al. [16]	4n	0	n	0	1	4
Proposed Scheme	4n	n	0	1	0	4

IDENTITY BASED MULTI-SIGNCRYPTION SCHEME FOR MULTIPLE RECEIVERS

An Identity based Multi- Signcryption scheme for Multi-Receivers consists of the following algorithms:

(*i*) **Setup:** Given a security parameter k, the Private Key Generator (PKG) chooses a secret value randomly and generates master secret key *msk* and the public parameters *params* of the system.

(*ii*) **Key Extract:** Given a user identity $ID \in \{0, 1\}^*$, the PKG computes the corresponding private key S and transmits it to the user in a secure way.

(*iii*) **Signcrypt:** Any n users $L = \{ID_1, ..., ID_n\}$ run this algorithm to signcrypt a message m to any n' receiver's with identities $L^* = \{ID'_1, ..., ID'_{n'}\}$, and to obtain signcryption σ.

(*iv*) **Unsigncrypt:** Each receiver with identity ID'_j and private key S'_j runs this algorithm to obtain plain text m if σ is a valid signcryption from L to identity ID'_j otherwise return $\perp$.

For consistency, we require that if

$$s = \text{signcrypt}(m, L, S_1, ..., S_n, L^*) = \{ID'_1, ..., ID'_{n'}\}, \text{ then}$$

$$m = \text{unsigncypt}(\sigma, L = \{ID_1, ..., ID_n\}\ L^*, S'_1, ..., S'_{n'}\}.$$

The proposed scheme :

Setup. Given k is the security parameter, the PKG chooses the system parameter that includes two groups G_1, G_2 of same prime order q, a bilinear map $e : G_1 \times G_1 \rightarrow G_2$, a generator $P \in G_1$, randomly chosen $s \in_R Z_q$, $R \in_R G_1$, $(R \neq P, O)$ and computes $P_{pub} = sP \in G_1$, and $\theta = e(P_{pub}, R)$. The PKG also choose cryptographic hash functions $H_0 : \{0, 1\}^* \rightarrow G_1$, $H_1 : G_2, \rightarrow \{0, 1\}^l$, $H_2 : \{0, 1\}^* \rightarrow Z^*q$, where l is the length of plaintext and ciphertext .

The system public parameters are

$$\text{params} = \langle q, G_1, G_2, e, l, P, P_{pub}, \theta, R, H_0, H_1, H_2 \rangle$$

Key Extract. Given a user identity $ID \in \{0, 1\}^*$ then PKG compute public key $Q_{ID} = H_0(ID)$ and private key $S_{ID} = sQ_{ID}$.

Signcrypt. Given a message $m \in \{0, 1\}^l$, n' receiver's identity $L^* = \{ID'_1, ..., ID'_{n'}\}$ and n senders' identities $L = \{ID_1, ..., ID_n\}$, each user ID_i execute the following steps :

(*i*) Randomly chooses $x_i \in \mathbb{Z}_q^*$ and computes $X_i = x_i P$, $Y_i = \theta^{x_i}$ and $U_{i,j} = x_i (R + Q'_j)$ for $j = 1, ..., n'$.

(*ii*) Sends $(X_i, Y_i, U_{i,1}, U_{i,2}, ..., U_i, n')$ to other signers through a secure channel.

(*iii*) After receiving from the other signers $(X_i, Y_i, U_{i,1}, U_{i,2}, ..., U_{i,n'})$, user ID_i computes

(*a*) $X = \sum_{i=1}^{n} X_i$, $Y = \prod_{i=1}^{n} Y_i$, $Q = \sum_{i=1}^{n} Q_i$ and

$$U_1 = \sum_{i=1}^{n} U_{i,1}, U_2 = \sum_{i=1}^{n} U_{i,2}, ..., U_{n'} = \sum_{i=1}^{n} U_{i,n'}.$$

(*b*) $c = H_1(Y) \oplus m$.

(*c*) $h = H_2(c, X, U_1, U_2, ..., U_{n'})$

(*d*) $Z_i = hS_i + x_i Q$.

(*iv*) Each user sends Z_i to other users. Every user computes Z and outputs ciphertext σ, where $Z = \sum_{i=1}^{n} Z_i$ and $\sigma = \langle c, X, Z, U_1, U_2, ..., U_{n'}, L, L^* \rangle$.

Unsigncrypt. To unsigncrypt the ciphertext $\sigma = \langle c, X, Z, U_1, U_2, ..., U_{n'}, L, L^* \rangle$., the receiver with identity ID'_j computes

(*i*) $h = H_2(c, X, U_1, U_2, ..., U_{n'})$, and accepts iff.

(*ii*) Accept if $e(P, Z) = e(X + hP_{pub}, Q)$. It then extract U_j from σ and computes.

(*iii*) $Y' = e(P_{pub}, U_j) e(X, S'_j)^{-1}$, and recovers.

(*iv*) $m = c \oplus H_1(Y')$.

SECURITY

***(i)* Confidentiality.** Without knowing the secrete key of receiver, no one can compute $Y = \prod_{i=1}^{n} Y_i = Q^{(x_1 + ... + x_n)} = e(P_{pub}, R)^{(x_1 + ... + x_n)}$. It is only the specific receiver who can compute the actual value of Y using secrete key as

$$\begin{aligned}
Y' &= e(P_{pub}, U_j) e(X, S'_j)^{-1} \\
&= e(P_{pub}, \sum_{i=1}^{n} U_{i,j}) e(X, S'_j)^{-1} \\
&= e(P_{pub}, \sum_{i=1}^{n} x_i (R + Q'_j)) e(X, S'_j)^{-1} \\
&= e(P_{pub}, \sum_{i=1}^{n} x_i R) e(P_{pub} + \sum_{i=1}^{n} x_i Q'_j) e(X, S'_j)^{-1} \\
&= e(P_{pub}, (x_1 + ... + x_n) R) e(sP, (x_1 + ... + x_n) Q'_j) e(X, S¢j)^{-1} \\
&= e(P_{pub}, R)^{(x_1 + ... + x_n)} e((x_1 + ... + x_n) P, sQ'_j) e(X, S'_j)^{-1} \\
&= \theta^{(x_1 + ... + x_n)} e(X, S'_j) e(X, S'_j)^{-1} \\
&= \theta^{(x_1 + ... + x_n)} = Y.
\end{aligned}$$

***(ii)* Public Verifiability.** Any one who has access to the signcryptext can verify the signature on the ciphertext which it contains. First the verifier computes $h = H_2(c, X, U_1, U_2, ..., U_{n'})$, $Q = \sum_{i=1}^{n} Q_i$, then checks

$$e(P, Z) = e(P, \sum_{i=1}^{n} (hS_i + x_i Q))$$

$$= e(P, \sum_{i=1}^{n} hS_i)\, e(P, \sum_{i=1}^{n} x_i Q)$$

$$= e(P, \sum_{i=1}^{n} hsQ_i)\, e(P, \sum_{i=1}^{n} x_i Q)$$

$$= e(P, hs\sum_{i=1}^{n} Q_i)\, e(P,(x_1 +...+ x_n)\, Q)$$

$$= e(P, hsQ)\, e((x_1 +...+ x_n)P, Q)$$

$$= e(hsP, Q)\, e(X, Q)$$

$$= e(hP_{pub}, Q)\, e(X, Q)$$

$$= e(X + hP_{pub}, Q).$$

(*iii*) Unforgeability. Signcryptext is generated using the secret key S_i of each the signers. Thus no one, not even the one among signers can generate a valid signcryptext without knowing the secret key of **all** the signers.

CONCLUSION

We have proposed an efficient Identity Based Multi-Signcryption Scheme. We discuss its confidentiality, unforgeability and public verifiability in heuristic way and compare it with two existing Id-based multi-signcryption schemes. We also extend the proposed scheme to multi-signcryption scheme for multiple receivers.

REFERENCES

[1] J. Beak, R. Safavi-Naini and W. Susilo: Efficient multi-receiver identity based encryption and its application to broadcast encryption, PKC 2005, LNCS # 3386, pp. 380-397, Springer-Verlag, (2005).

[2] J. Beak, R. Steinfeld, and Y. Zheng: Formal proofs for the security of Signcryption. In public key Cryptography-PKC 2002, LNCS # 2274, pages 80-98. Springer-Verlag, (2002).

[3] M. Bellare, A. Boldyreva and S. Micali: Public key encryption in a multi-user setting: Security proofs and improvements, EUROCRYPT'2000, LNCS # 1807, pp. 259-274, Springer-Verlag, (2000).

[4] D. Bohen and M. Franklin: Identity-based encryption scheme for Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 213-229(2001).

[5] C. Boyed: Digital Multi Signature, in Proc. IMA Conf. Crypto. Coding, Charendon Oxford, pp 241-246, 1989.

[6] S. Duan and Z. Cao: Efficient and provably secure multi receiver identity based signcryption. ACISP 2006, LNCS # 4058, pp. 195-206, Springer-Heidelberg, (2006).

[7] C. Gentry and Z. Ramzan: Identity-based aggregate signature. In Public Key Cryptography-PKC 2006, LNCS # 3958, pp. 275-273. Springer-Verlag, (2006).

8] S. Lal and P. Kushwah: Anonymous Id based signcryption scheme for multiple receivers. Cryptology ePrint Archive, Report 2009/345, http://eprint. iacr.org/2009/345.pdf, (2009).

[9] J. Malone-Lee: Identity-based signcryption, Cryptology ePrint Archive Report 2002/098, http://eprint. iacr.org/2002/098.pdf, (2002).

[10] S. Mitomi and A. Miyaji: A multi-signature scheme with message flexibility, order flexibility and order verifiability. In Information Security and privacy, ACISP-2000, LNCS # 1841, pp. 298-312. Springer-Verlag, (2000).

[11] S.S.D. Selvi, S.S. Vivek, R. Gopalkrishnan, N.N. Karuturi and C.P. Rangan: On the provable security of multiple receiver signcryption schemes. Cryptology ePrint Archive, Report 2008/238, http://eprint.iacr.org/2008/238.pdf, (2008).

[12] S. S. D. Selvi, S. S. Vivek and C. P. Rangan: Breaking and Fixing of an Identity Based Multi-Signcryption Scheme. Cryptology ePrint Archive, Report 2009/235, http://eprint.iacr.org/2009/ 235.pdf, (2009).

[13] S.S.D. Selvi, S.S. Vivek, R. Srinivasan and C.P. Rangan: An efficient Identity based signcryption scheme for of multiple receivers. Cryptology ePrint Archive, Report 2009/144, http://eprint.iacr.org/2009/144.pdf, (2009).

[14] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology, CRYPTO-1984, LNCS # 196, pp. 47-53. Springer-Verlag, (1984).

[15] J. Zhang and J. Mao: A novel identity-based multi-signcryption scheme. Computer Communications, 32(1): pages 14-18, (2009).

[16] J. Zhang, Y. Yang and X. Niu: A Novel Identity-Based Multi-Signcryption Scheme, International Journal of Distributed Sensor Network, 5(1), pp 28-28 ISSH: 1550-1329, (2009).

[17] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption). In Advances in Cryptology, CRYPTO-1997, LNCS # 1294, pp. 165-179. Springer-Verlag, (1997).