New ID-based Multi-proxy Multi-Signcryption Scheme from Pairings

Sunder Lal and Tej Singh
Department of Mathematics, IBS, Khandari
Agra-282002 (UP)-INDIA
E-mail:- sunder_lal2@rediffmail.com tej_singh2ibs@yahoo.co.in

Abstract: This paper presents an identity based multi-proxy multi-signcryption scheme from pairings. In this scheme a proxy signcrypter group could authorized as a proxy agent by the cooperation of all members in the original signcrypter group. Then the proxy signcryption can be generated by the cooperation of all the signcrypters in the authorized proxy signcrypter group on the behalf of the original signcrypter group. As compared to the scheme of Liu and Xiao, the proposed scheme provides public verifiability of the signature along with simplified key management.

Keywords: Identity-based cryptography, multi signature, proxy signature, signcryption.

1 Introduction

In 1996, Mambo et al [12] first introduced the concept of a proxy signature scheme, which allows the original signer to delegate his signature power to a designed signer, called the proxy signer. Then the proxy signer is able to sign on the behalf of the original signer. Several other multi proxy signature schemes [1], [2], [3], [4], [5], [6], [15] were proposed. In 2001, Hwang et al [2] first proposed the concept of multi-proxy multi-signature scheme. In a multi-proxy multi-signature scheme, only the cooperation of all the signers in the authorized proxy group can generate the proxy signature on the behalf of the original signer group.

A new type of cryptographic primitive called “signcryption” which combines a function of digital signature scheme with a symmetric key encryption algorithm was introduced by Zheng in [16]. Signcryption not only provides authenticity and confidentiality in a single step, but also gives more efficient computations than traditional signature-then-encryption. Steinfiel and Zheng [14] and Malone-Lee and Mao [11] proposed efficient signcryption schemes that are based on integer factorization and using RSA.
An identity – based cryptosystem is a novel type of cryptographic scheme proposed by Shamir [13], which enables any pair of users to communicate securely, and to verify each other’s signatures without exchanging public or private keys, without keeping any key directories and without using the services of any third party. Problem with the traditional public key cryptosystems (PKCs) are the high cost of the infrastructure needed to manage and authenticate public keys, and the difficulty in managing multiple communities. In an ID-based PKC, everyone’s public keys are predetermined by information that uniquely identifies them, such as their email address. There is no need for any public key certificate. A trusted key generation center (KGC) generates the private keys of the entities in the group using their public key. First ID-based signcryption scheme was proposed by Malon-Lee [10] in 2002, Libert and Quisquater [8] proposed a provably secure identity-based signcryption schemes from pairing. Several other ID-based signcryption schemes were proposed. Li et al [7] have proposed a proxy signcryption. However, none of existing signcryption schemes is multi-proxy multi-signcryption scheme. In 2005, Liu Jun Bao and Xiao Guo-Zhen [9] proposed multi-proxy multi-signcryption scheme from pairing.

In this paper we propose an ID-based multi-proxy multi-signcryption scheme from pairing. In this scheme, only the cooperation of all members in the original signcypet group could authorize a proxy group as his proxy agent. Then only the cooperation of all the signcypers in the authorized proxy group can generate the proxy signcryption on the behalf of the original signcypet group. As compared to the scheme in [9] the proposed scheme provides the public verifiability of the signature. Further the scheme is ID-based therefore; the key management problem is simplified.

The rest of the paper is organized as follows. Some definitions and preliminary work are given in section 2, Liu and Xiao scheme is described in section 3, and proposed scheme is given in section 4. The security of the scheme is discussed in section 5. Finally, the conclusions are given in section 6.

2 Preliminary Works

In this section, we briefly describe the basic definition and properties of the bilinear pairing.

2.1 Bilinear Pairings

Let \( G_1 \) be a cyclic additive group generated by \( P \), whose order is a prime \( q \), and \( G_2 \) be a cyclic multiplicative group of the same order \( q \). Let \( a, b \) be elements of \( \mathbb{Z}_q^* \). A bilinear pairings is a map \( e: G_1 \times G_1 \to G_2 \) with the following properties:

1) Bilinearity: \( e(aP, bQ) = e(P, Q)^{ab} \).
2) Non-degeneracy: There exists \( P \) and \( Q \) such that \( e(P, Q) \neq 1 \).
3) Computability: There is an efficient algorithm to compute \( e(P, Q) \) for all \( P, Q \in G_1 \).

The security of our scheme described here relies on the hardness of the following problems:
**DBDHP:** Given two groups $G_1$ and $G_2$ of the same prime order $q$, a bilinear map $e: G_1 \times G_1 \to G_2$ and a generator $P$ of $G_1$, the Decisional Bilinear Diffie-Hellman problem (DBDHP) in $(G_1, G_2, e)$ is to decide whether $h = e(P, P)^{abc}$ given $(P, aP, bP, cP)$ and an element $h \in G_2$.

**CBDHP:** Given two groups $G_1$ and $G_2$ of the same prime order $q$, a bilinear map $e: G_1 \times G_1 \to G_2$ and a generator $P$ of $G_1$, the Computational Bilinear Diffie-Hellman problem (CBDHP) in $(G_1, G_2, e)$ is to compute $h = e(P, P)^{abc}$ given $(P, aP, bP, cP)$.

No algorithm is known to be able to solve any of them so far, through DBDHP is no harder than CBDHP.

### 3 Liu-Xiao Scheme

This scheme consists of four phases:

**System Initialization:** Let $A_1, \ldots, A_n$ be $n$ original signcryption. Each $A_i$ chooses secret key $x_i \in Z_q^*$ and computes public key $y_i = x_P P$.

Let $P_1, P_2, \ldots, P_l$ constitute the group of proxy signcryption. Each proxy signcryption chooses secret key $x_{pj} \in Z_q^*$ and computes public key $y_{pj} = x_P P$.

Let $C$ be the unsigncryption with secret key $x_c \in Z_q^*$ and public $y_c = x_P P$.

Let $E$ and $D$ be the encryption and decryption functions respectively and let $H_1 : \{0,1\}^n \to Z_q^*$, $H_2 : \{0,1\}^n \to G_1$ and $H_3 : G_2 \to \{0,1\}^n$ be the hash functions.

System parameters are $(G_1, G_2, e, P, q, H_1, H_2, H_3, E, D)$.

**Proxy Key Generation:** The original signcryption makes the signed warrant $m_w$ and broadcast to the proxy signcryption. Through the following protocol, each proxy signcryption $P_j$ gets a proxy key $S_{pj}$.

1. Each of the original signcryption computes $S_{aw} = x_w H_2(m_w)$ and broadcasts it all the proxy signcryption.

2. The proxy signcryption group verifies the correctness of each $S_{aw}$ by the equation

$$e(P, S_{aw}) = e(y_w, H_2(m_w))$$

3. If each $S_{aw}$ is verified, then each proxy signcryption $P_j$ computes $S_A = \sum_{i=1}^{n} S_{aw}$ and his proxy signcryption key $S_{pj} = S_A + x_{pj} H_2(m_w)$.

**Multi-Proxy Multi-Signcryption Generation:** One proxy signcryption say $P_1$, may be designated as a clerk, whose task is to combine partial proxy signcryption to generate the final multi-proxy multi-signcryption.
1. Each $P_j$ selects an integer $t_j \in \mathbb{Z}_q^*$, and computes $r_{pj} = e(P, y_j)^{t_j}$ and

2. $P_j$ broadcasts $r_{pj}$ to other proxy signcryption, $P_1, P_2, \ldots, P_{j-1}, P_{j+1}, \ldots, P_l$.

3. Each $P_j$ computes $k = H_3(\prod_{j=1}^l r_{pj})$, $c = E_{s}(m)$, $r_p = H_3(c \parallel k)$

and $u_{pj} = t_j P - r_p S_{pj}$, and sends $u_{pj}$ to the clerk $P_1$ as his partial proxy signcryption on $m$.

4. $P_1$ computes $u_p = \sum_{j=1}^l u_{pj}$, $S = S_{A}$ and sends $(m_w, S, c, r_p, u_p)$ to the b unsigncrypter $C$ as multi-proxy multi-signcryption of $m$.

Unsigncryption: After $(m_w, S, c, r_p, u_p)$, $C$ computes

$$k = H_3(e(u_p, y_p) e(S, y_p)^{r_p} e(H_2(m_w), \sum_{j=1}^l y_{pj})^{r_p})$$

and accepts the multi-proxy multi-signcryption if and only if $r_p = H_3(c \parallel k)$. She then recovers $m = D_{s}(c)$.

4 Our proposed scheme

To make the proposed scheme identity based, we introduce the Private Key Generator (PKG) along with original signcryption group $\{A_1, A_2, \ldots, A_n\}$, proxy signcryption group $\{P_1, P_2, \ldots, P_l\}$ and the unsigncrypter $C$.

Set up: Given a security parameter $k$, the PKG chooses group $G_1$ and $G_2$ of prime order $q$, a generator $P$ of $G_1$, a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ and hash functions $H_1: \{0,1\}^* \rightarrow G_1$, $H_2: G_2 \rightarrow \{0,1\}^n$ and $H_3: \{0,1\}^* \times G_2 \rightarrow \mathbb{Z}_q^*$.

Then PKG chooses a secret key $s \in \mathbb{Z}_q^*$ and computes $P_{pub} = sP$. It also chooses a secure symmetric cryptosystem ($E$, $D$).

The system’s public parameters are $P = (G_1, G_2, n, e, P, P_{pub}, H_1, H_2, H_3, E, D)$.

Key generation: Given an identity $ID$, the PKG computes user’s public key $Q_{ID} = H_1(ID)$ and secret key $S_{ID} = sQ_{ID}$.

Each signcryption $A_i$ has a public key $Q_{ID_{A_i}} = H_1(ID_{A_i})$ and secret key $S_{ID_{A_i}} = sQ_{ID_{A_i}}$. 

4
Similarly each proxy signcrypter $P_j$ has a public key $Q_{ID_{pj}} = H_1(ID_{pj})$ and secret key $S_{ID_{pj}} = sQ_{ID_{pj}}$. Unsigncrypter; C has a public key $Q_{ID_c} = H_1(ID_c)$ and a secret key $S_{ID_c} = sQ_{ID_c}$.

Proxy Keygeneration: To delegate the signcrypting capability to a group of proxy signcrypters, the original signcrypters make the signed warrant $m_w$. Which may include an explicit description of the delegation relation including the identity of the original signcrypters and the proxy signcrypters, the message to be signed, and so on. Then broadcasts $m_w$ to the l proxy signcrypters.

Each proxy signcrypter $P_j$ recover the proxy key $S_{pj}$ in the following manner:

1. Each $A_i$ computes $S_{A_i} = S_{ID_{A_i}}H_1(m_w)$ and broadcasts $S_{A_i}$ to the each proxy signcrypter.
2. The proxy signcrypter group verifies the correctness of each $S_{A_i}$ by the equation

   $$e(P, S_{A_i}) = e(P_{pub}, Q_{ID_{A_i}}H_1(m_w))$$

   i = 1, 2……n

3. If all the above equation holds, the proxy signcrypter group computes $S_A = \sum_{j=1}^{n} S_{A_i}$.

Each proxy signcrypter $P_j$ computes his proxy signcryption key $S_{pj}$ as

$$S_{pj} = S_A + S_{ID_{pj}}H_1(m_w)$$

Multi-Proxy Multi-Signcryption Generation: Here we assume that one member of the proxy signcrypter say $P_1$, is the clerk who combines all partial proxy signcryption.

1. Each $P_j$ selects $t_j \in_R Z_q^*$, and computes $k_{1j} = e(P, P_{pub})^{t_j} \in G_2$ and $k_{2j} = e(P_{pub}, Q_{ID_{pj}})^{t_j} \in G_2$
2. $P_j$ broadcasts $k_{1j}$ and $k_{2j}$ to the remaining proxy signcrypters.
3. Each $P_j$ now computes $k_1 = \prod_{j=1}^{l} k_{1j} \in G_2$ and $k_2 = H_2(\prod_{j=1}^{l} k_{2j}) \in G_2$, $c = E_{k_2}(m)$, $r_p = H_3(c, k_1)$, $u_{pj} = t_j P_{pub} - r_p S_{pj} \in G_1$.

and sends $u_{pj}$ to the clerk $P_1$ as his partial proxy signcryption on m.
4. The clerk computes \( u_p = \sum_{j=1}^{l} u_{pj} \), \( S = IS_{\lambda} \) and sends \((m_w, S, c, r_p, u_p)\) to \(C\) for a multi-proxy multi-signcryption of \(m\).

**Unsigncryption:** After receiving \((m_w, S, c, r_p, u_p)\), \(C\) computes

\[
\begin{align*}
k_1 &= e(u_p, P)e(S, P)^{r_p} e(H_1(m_w), \sum_{j=1}^{l} Q_{ID_j})^{r_{Pr_a}} \text{ and} \\
k_2 &= H_2(e(u_p, Q_ID_j)e(S, Q_ID_j)^{r_p} e(H_1(m_w), \sum_{j=1}^{l} Q_{ID_j})^{r_{Pr_a}})
\end{align*}
\]

accept the proxy signature if and only if \( r_p = H_3(c, k_1) \).

Satisfied, she may recover the message as \( m = D_{k_2}(c) \).

5 **Security Analysis**

**Verifiability:**

\[
k_1 = \prod_{j=1}^{l} k_{1j} = \prod_{j=1}^{l} e(P, P_{pub})^{y_j} = e(\sum_{j=1}^{l} (u_{pj} + r_p S_{pj}), P)
\]

\[
= e(u_p, P)e(\sum_{j=1}^{l} (S_A + S_{ID_j} H_1(m_w)), P)^{r_p}
\]

\[
= e(u_p, P)e(S, P)^{r_p} e(H_1(m_w), \sum_{j=1}^{l} Q_{ID_j})^{r_{Pr_a}}
\]

\[
k_2 = H_2(\prod_{j=1}^{l} k_{2j}) = H_2(\prod_{j=1}^{l} e(P_{pub}, Q_{ID_j})^{y_j})
\]

\[
= H_2(e(\sum_{j=1}^{l} (u_{pj} + r_p S_{pj}), Q_{ID_j}))
\]

\[
= H_2(e(u_p, Q_ID_j)e(\sum_{j=1}^{l} (S_A + S_{ID_j} H_1(m_w)), Q_{ID_j})^{r_p})
\]

\[
= H_2(e(u_p, Q_ID_j)e(S, Q_ID_j)^{r_p} e(H_1(m_w), \sum_{j=1}^{l} S_{ID_j} Q_{ID_j})^{r_p})
\]

\[
= H_2(e(u_p, Q_{ID_j})e(S, Q_{ID_j})e(S, Q_{ID_j})^{r_p} e(H_1(m_w), \sum_{j=1}^{l} Q_{ID_j})^{r_{Pr_a}})
\]
**Strong Unforgeability:** As for multi-proxy multi-signcryption, there are mainly four kinds of attackers: any third party, who do not participate the issue of the multi-proxy multi-signcryption; some proxy signcrypter, who plays an active part in signcryption process; the original signcrypter and the signcryption owner. Because the multi-proxy multi signcryption $u_p = \sum_{j=1}^{l} u_{pj}$ contains secret key information $S_{id_{pj}}$ of each proxy signcrypter $P_j$ in the proxy multi-signcryption key generation phase, without secret key information $S_{id_{pj}}$ of $P_j$, any third party, some proxy signcrypter, the signcryption owner and the original signcrypters cannot generate a valid multi-proxy multi-signcryption scheme by themselves.

**Strong Identifiably:** The unsigncrypter can distinguish proxy’s normal signcryption from his multi-proxy multi-signcryption, because the multi-proxy multi-signcryption key is different from his own private key.

**Strong Nonrepudiation:** In our scheme, each proxy signcrypter $P_j$ cannot repudiate his participation on multi-proxy multi-signcryption while illegal attacker cannot claim that he is proxy signcrypter, because $u_p = \sum_{j=1}^{l} u_{pj}$ contains secret key information $S_{id_{pj}}$ of each proxy signcrypter $P_j$, at the same time, warrant $m_w$ also contains identity information of $P_j$ in addition $k_2 = H_2(e(u_p, Q_{id_c})e(Q_{id}, \cdot)^{r} e(H_1(m_w), \sum_{j=1}^{l}Q_{id_{pj}})^{r} S_{w} \cdot )$ contains $Q_{id_{pj}}$ and $m_w$.

**Confidentiality:** Because the secret key $k_2$ contains secret key information $S_{id_c}$ of C, only C can compute $k_2$ and recover m.

**Prevention of Misuses:** No proxy signcrypter $P_j$ can repudiate his participation on multi-proxy multi-signcryption. In addition, $m_w$ includes the message to be signed, so our scheme can prevent the misuse.

**Public verifiability:** Any third party can verify the multisignature, so our scheme provides the public verifiability.

6 Conclusions

In this paper, based on Liu Jun Bao and Xiao Guo-Zhen scheme [9] we construct a new ID-based multi-proxy multi-signcryption scheme from pairing. As compared to Liu Jun Bao and Xiao Guo-Zhen scheme the proposed scheme provide the public verifiability of the proxy signature. Further the scheme is ID-based therefore; the key management problem is simplified.
References

[1] S.J. Hwang, C.H. Shi, “A simple Multi-Proxy Signature Scheme,” Proceeding of the Tenth National Conference on Information Security, Taiwan, 2000, pp. 134-138.

[2] S.J. Hwang, C.C. Chen, “A New Multi-Proxy Multi-Signature Scheme,” 2001 National Computer Symposium: Information Security, Taipei, Taiwan, 2001, pp. F019-F026.

[3] J.G. Li, Z.F. Cao, Y.C. Zhang, “Improvement of M-U-O and K-P-W proxy signature schemes,” Journal of Harbin Institute of Technology, Harbin, pp. 145-148, Feb.2002.

[4] J.G. Li, Z.F. Cao, Y.C. Zhang, “Nonrepudiable proxy multi-signature schemes,” Journal of Computer Science and Technology, Vol. 18, pp. 399-402, Mar.2003.

[5] J.G. Li, Z.F. Cao, “Improvement of a Threshold proxy signature scheme,” Improvement of Computer Research and Development, Vol. 39, pp. 515-518, Nov.2002.

[6] X.X. Li and K.H. Chen, “Multi-proxy Signature and Proxy Multi-signature Scheme from bilinear pairing,” LNCS #3320, Springer-Verlag, Singapore, pp. 591-595, Dec.2004.

[7] X.X. Li and K.H. Chen, “Identity Based Proxy-Signcryption Scheme from Pairings,” Proceedings of the 2004 IEEE International Conference on Services Computing (SCC’04), pp. 494-497, Sept.2004.

[8] B. Libert and J. Quisquater, “A new Identity Based Signcryption Scheme from Pairings,” in 2003 IEEE Information Theory Workshop, pp. 155-158, Paris, France, 2003.

[9] Jun-Bao Liu and Guo-Zhen Xiao, “Multi-Proxy Multi-Signcryption Scheme from Pairings,” in 2005 available at arxiv.org/abs/cs.CR/0509030.

[10] J. Malone-Lee, “Identity based Signcryption,” Cryptology ePrint Archive, Report 2002/098, 2002. Available from http://eprint.iacr.org/2002/098.

[11] J. Malone-Lee and W. Mao, “Two birds one stone: Signcryption using RSA,” in Topics in Cryptology-CT-RSA 2003, LNCS #2612, pp. 211-225, Springer-Verlag, 2003.

[12] M. Mambo, K. Usuda and E. Okamoto, “Proxy signature: delegation of the power to sign messages,” IEICE Trans. Fundamentals, E79-A:9, 1996, pp. 1338-1353.
[13] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 24, no.11, pp. 612-613, 1979.

[14] R. Steinfeld and Y. Zheng, “A Signcryption Scheme based on Integer factorization,” in The Third Information Security Workshop (ISW 2000), LNCS #1975, pp. 308-322, Springer-Verlag, 2000.

[15] Q.S. Xue, Z.F. Cao, “A Nonrepudiable Multi-proxy Multi-signature Scheme,” in Mobile Future, 2004 and the Symposium on Trends in Communications.Sympo TIC’04, pp. 102-105. Oct. 2004.

[16] Y. Zheng, “Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption),” in CRYPTO’97, LNCS #1924, Springer-Verlag, pp. 165-179, 1997.