An Efficient Identity based Multi-Proxy Multi-Signcryption Scheme from Bilinear Pairings

Tej Singh
Department of Mathematics,
IMS Engineering College
Ghaziabad, India

Rashid Ali
Department of Mathematics,
Krishna Engineering College
Ghaziabad, India

Musharraf Ali
Department of Mathematics
G.F. College
Shahjahanpur, India

ABSTRACT
Signcryption is a cryptography primitive that fulfills both the functions of digital signature and encryption and guarantees non-repudiation, confidentiality and integrity in a more efficient way. In this paper, we propose an efficient and secure identity based multi-proxy multi signcryption scheme from bilinear pairings. In this scheme a group of proxy signcrypters could authorize by a group of original signcrypters. Then multi proxy multi signcryption could generate by the cooperation of all signcrypters in the proxy group.

Keywords
Bilinear Pairings, Identity-based Cryptography, Signcryption, Proxy Signature, Multi Proxy Multi Signcryption

1. INTRODUCTION
In 1984, Shamir [1] firstly proposed the idea of ID based cryptography. The distinguishing property of identity-based cryptography is that a user's public key can be any binary string, such as an email address that can identify the user. Several practical ID-based signature schemes have been devised since 1984 [2], [3], but a satisfying ID-based encryption scheme only appeared in 2001 [4] . In 1996, Mambo et al. [5] first introduced the concept of a proxy signature. In 2001, Hwang et al. [6.] first proposed the concept of multi-proxy multi-signature scheme. In 2005, Li et al. [7] proposed an ID-based a multi-proxy multi-signature scheme.

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to sign-then encrypt the message. Signcryption first proposed by Zheng [8], is a cryptographic primitive that fulfills both the function of digital signature and public key encryption simultaneously, at a cost lower than required by the traditional signature-then-encryption approach. Several ID-based signcryption schemes were also proposed in [9]-[11]. However, none of the existing signcryption schemes is ID-based multi-proxy multi signcryption scheme from pairing. In 2005, Liu Jun Bao and Xiao Guo-Zhen [12] proposed multi-proxy multi-signcryption scheme from pairing. However this scheme is not ID based. In 2007, Lal and Singh [13] proposed ID-based multi-proxy multi-signcryption scheme from pairing. In 2009, Xiaoyen et al. [14] proposed an improved ID-based multi-proxy multi signcryption scheme.

In this paper we propose an efficient ID based multi proxy multi signcryption scheme from pairing. As compared to Xiaoyen et al. [14] scheme, the propose scheme is much more efficient; only need 4 pairing computations, while Xiaoyen et al. [14] scheme needs 8 pairing computations.

The rest of the paper is organized as follows. Basic definitions and properties of bilinear pairings are given in section 2 and proposed scheme is given in section 3. The security of the scheme is discussed in section 4. Finally, the conclusions are given in section 5.

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

Let G1 be a cyclic additive group generated by P, whose order is a prime q, and G2 be a cyclic multiplicative group of the same order q. Let a, b be elements of Z_q^*. A bilinear pairings is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

- Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$.
- Non-degeneracy: There exists P and Q such that $e(P, Q) \neq 1$.
- 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:

Definition 1: 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 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 $h \in G_2$.

Definition 2: 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 DiffieHellman 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. PROPOSED SCHEME

Proposed scheme involves four roles: the Private Key Generator (PKG), a set of original signcrypters $D = \{O_1, O_2, ...O_n\}$ with identity $ID_{O_1}, ID_{O_2}, ...ID_{On}$ a set of proxy signcerypter $L = \{P_1, P_2, ...P_l\}$ with identity $ID_{P_1}, ID_{P_2}, ...ID_{Pl}$ and the

message recipient Bob with identity IDB.

3.1.Set Up

Given a security parameter, the PKG chooses group G1 and G2 of prime order q, a generator P of G1, a bilinear map $e: G_1 \times G_1 \to G_2$ and hash functions $H_1: \{0,1\}^* \to Z_q^*$, $H_2: \{0,1\}^* \to G_1$, $H_3: G_2 \to \{0,1\}^n$ Then PKG chooses a master key $s \in_R Z_q^*$ 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) and keeps the master key s secret.

3.2.Extract

Given a user U's identity $ID_U \in \{0,1\}^*$ the PKG computes user's public key $Q_U = H_2(ID_U)$ and private key $S_U = sQ_U$.

3.3.Generation of proxy key

For delegation of signcrypting capability to a group of proxy signcrypters group L, each original signcrypters O_i follows the following steps to generate the signed warrant m_W and each proxy signcrypter P_j computes his proxy key S_{pj} and proxy public Key Q_{pj}. The warrant m_W specifies the delegation period, identity information of the original signcrypters, what kind of messages is delegated and identity information of the the proxy signcrypter, etc.

Each original signcrypter O_i computes $S_{O_i} = S_{ID_{O_i}} H_1(m_W)$ and broadcasts S_{O_i} to each proxy signcrypter.

- When receiving S_{O_i} each proxy signcrypter group P_j verifies the correctness of S_{O_i} by the equation $e(P, S_{O_i}) = e(P_{Pub}, Q_{ID_{O_i}})^{H_1(m_W)}$ i = 1, 2…….n.
- After verification of equation, the proxy signcrypter group P_j computes $S_O = \sum_{i=1}^{n} S_{O_i}$ and his proxy signcryption key S_{pj} as $S_{pj} = S_O + S_{ID_{pj}} H_1(m_W)$.

3.4.Multi Proxy Multi Signcryption Generation

Suppose the proxy group L wants to send a delegated message m on the behalf of the original group D to Bob. Each proxy signcrypter say P_j generates the partial signature and an appointed clerk C, who is one of the proxy signcrypters, combines the partial proxy signatures to generate the final multi-proxy multi signcryption

- Each P_j selects an integer $x_j \in_R Z_q^*$ and compute $k_j = e(P, Q_{ID_B})^{x_j}$, $j = 1, 2.....l.$ and broadcasts k_j to the other l -1 co-signcrypters.
- Each P_j now computes $k = H_3(\prod_{j=1}^{l} k_j)$, $c = E_k(m)$, $r_p = H_1(c \| k)$, $u_{pj} = x_j P - r_p S_{pj}$ and sends u_{pj} to the clerk C.
- Then clerk computes $u_p = \sum_{j=1}^{l} u_{pj}$ and sends (m_W, c, r_p, u_p) to unsigncrypter Bob.

3.5.Unsigncryption

After receiving (m_W, S, c, r_p, u_p), Bob computes

$$k = H_2(e(u_p, Q_{ID_B}) e(\sum_{i=1}^{n} Q_{ID_{O_i}}, S_{ID_B})^{r_p H_1(m_w)} .e(\sum_{j=1}^{l} Q_{ID_{pj}}, S_{ID_B})^{r_p H_1(m_W)})$$

Third party accept the proxy signature if and only if $r_p = H_1(c \| k)$ and recover the message $m = D_k(c)$.

4. ANALYSIS OF THE SCHEME

In this section first we present the proof of correctness and then we discuss security and efficiency analysis of proposed scheme.

4.1.Proof of Correctness

The consistency of our scheme can be verified as follows:

$$k = H_2(\prod_{j=1}^{l} k_j) = H_2(\prod_{j=1}^{l} e(P, Q_{ID_B})^{x_j})$$

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

$$= H_2(e(u_p, Q_{ID_B}) e(\sum_{i=1}^{n} S_{O_i} + S_{ID_{pj}}, Q_{ID_B})^{r_p H_1(m_w)})$$

$$= H_2(e(u_p, Q_{ID_B}) e(\sum_{i=1}^{n} Q_{ID_{O_i}}, S_{ID_B})^{r_p H_1(m_w)} e(\sum_{j=1}^{l} Q_{ID_{pj}}, S_{ID_B})^{r_p H_1(m_W)})$$

4.2.Security Analysis

In the following we discuss the security requirements of the proposed scheme.

1. **Verifiability:** From the unsigncryption phase, the receiver can be convinced that the proxy sender has the original sender's signature on the warrant m_W. The warrant w also contains the identity information of the original sender, proxy sender and the limit of delegated signcrypting capacity etc. So

the receiver can be convinced of the original sender's agreement on the signcrypted message.

2. **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 play an active 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.

3. **Strong Identifiably:** It contains the warrant m_W in a valid multi proxy multi signcryption text and any one can determine the identity of the corresponding proxy sender from the warrant m_W .

4. **Non-repudiation:** 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

$$k = H_2(e(u_p, Q_{ID_B})e(\sum_{i=1}^{n} Q_{ID_{O_i}}, S_{ID_B})^{r_p H_1(m_w)} .e(\sum_{j=1}^{l} Q_{ID_{pj}}, S_{ID_B})^{r_p H_1(m_W)})$$

contains $Q_{ID_{pj}}$ and m_W .

5. **Confidentiality:** Except the receiver, anyone else can't extract the plaintext m from multi signcryption text (m_W , c, r_p , u_p). For getting the message m, the attacker has to decrypt the cipher text c directly. To do so, the attacker has to obtain the key k but the secret key k contains secret key information S_{ID_B} of Bob, only bob can compute k and recover m.

6. **Prevention of Misuses:** In our multi-proxy multi-signcryption scheme, using the warrant m_W , we have determined the limit of the delegated signcrypting capacity in the warrant and the proxy sender can't signcrypt the message that have been authorized by the original sender.

4.3.Efficiency Analysis

In this section, we compare the efficiency of proposed scheme with Xiaoyen et al. [14] scheme from computation overhead. Here we denote E by an exponentiation in G_2, M by multiplication and P by a computation of pairing.

Table 1. Comparisons of our scheme with Xiaoyen et al. scheme

Algorithm	Xiaoyen et al. scheme	Our Scheme
Signcryption	2E+2M+2P	1E+2M+1P
Unsigncryption	2E+2M+6P	2E+2M+3P

As shown in table 1 our scheme needs only 4 pairing computations, while Xiaoyen et al. scheme needs 8 pairing computations. We know that the computation of the pairing is most time consuming. So our scheme is more efficient.

5. CONCLUSIONS

In this paper, we proposed an efficient ID-based multi-proxy multi-signcryption scheme from pairing. In terms of computational point of view, our scheme needs only 4 pairing computations, while Xiaoyen et al. [14] scheme needs 8 pairing computations. So the proposed scheme is much more efficient than Xiaoyen et al. scheme.

6. ACKNOWLEDGMENT

The author of the manuscript acknowledge Professor Sunder Lal, Ex Vice Chancellor Jaunpur University, India for valuable discussion. Tej Singh is the corresponding author.

7. REFERENCES

[1] A. Shamir, Identity-based cryptosystems and signature schemes, Advancesin Cryptology—CRYPTO'84, LNCS 196, Springer-Verlag, Berlin, 1984, pp 47-53

[2] A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, Advances in Cryptology—CRYPTO'86, LNCS 263, Springer-Verlag, Berlin, 1986, pp. 186–194.

[3] L. Guillou, J.J. Quisquater, A "paradoxical" identity-based signature scheme resulting from zero-knowledge, Advances in Cryptology—CRYPTO'88, LNCS 16 403, Springer-Verlag, Berlin, 1988, pp. 216–231.

[4] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology—CRYPTO 2001, LNCS 2139, Springer-Verlag, Berlin, 2001, pp. 213–229.

[5] M. Mambo, K. Usuda and E. Okamoto: Proxy signature: delegation of the power to sign messages. IEICE Trans. Fundamentals, E79-A:9, pp. 1338-1353(1996)

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

[7] X. Li and K.H. Chen: Multi-proxy Signature and Proxy Multi- signature Scheme from bilinear pairing. Applied mathematics and Computation. 2005, 169(1): 437-445.

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

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

[10] B. Libert and J. Quisquater: A new Identity Based Signcryption Scheme from Pairings. IEEE Information Theory Workshop, pp. 155-158, Paris, France, (2003).

[11] L. Chen, J. Malone-Lee, Improved identity-based signcryption, Public Key Cryptography—PKC 2005, LNCS 3386, Springer-Verlag, Berlin, 2005, pp. 362–379.

[12] J.B. Liu and G.Z. Xiao: Multi-Proxy Multi-Signcryption Scheme from Pairings. Publishing at arxiv.org/abs/cs.CR/0509030 (2005).

[13] Sunder Lal, Tej Singh: New ID-Based Multi-Proxy Multi-Signcryption scheme from Pairings. Publishing at arxiv.org/abs/cs.CR/0509030 (2007).

[14] Zhou Xiaoyan, Wu Yan, Du Weifeng and Gao Yan: An Improved ID- Based Multi-proxy Multi –Signcryption Scheme. IEEE second international symposium on electronic commerce and security, 466-469 (2009).