Multi-PKG ID based signcryption

Sunder Lal and Prashant Kushwah
Department of Mathematics, IBS, Khandari
Agra- 282002 (UP) - INDIA
E-mail: sunder_lal2@rediffmail.com, pra.ibs@gmail.com

Abstract: Here we propose an identity based signcryption scheme in the multi-PKG environment where sender and receiver receive public key from different PKG. We also define security models for our scheme and give security proofs in random oracle model.

Keywords: signcryption, identity based cryptography, bilinear pairings.

1. Introduction: Two fundamental services of pubic key cryptography are privacy and authentication. Pubic key encryption schemes aim at providing confidentiality whereas digital signatures provide authentication and non-repudiation. Many real world cryptographic applications require both these distinct goals to be simultaneously achieved. This motivates Zheng [15] to give a novel cryptographic primitive which he called 'signcryption'. The purpose of this type of cryptosystem is to encrypt and sign data in a single operation which has smaller bandwidth requirements and computational costs than those entailed by doing both operations sequentially. In 1997 Zheng [15] proposed a discrete logarithm based scheme. This original paper did not formalize security notions for signcryption. The first definition of security notions for signcryption appeared in [1, 2]. These deal with privacy and unforgeability. Security proofs of Zheng's original scheme are provided in [2].

In 1984 Shamir [13] introduce the concept of identity based cryptography where a public key can be a binary string identifying its owner non-ambiguously (e.g. an e-mail address, an IP address combine to a user name, a social security number…). Shamir also proposed an identity based signature scheme but for many years identity based encryption remained an open problem. It was in 2001 Boneh and Franklin [3] gave a scheme based on bilinear pairing on elliptic curves and proved its security under (Bilinear Diffie-Hellman) BDH assumption. In 2007, Wang and Cao [14] modified Boneh and Franklin scheme which is secure under mBDHP (modified Bilinear Diffie-Hellman Problem) and which is more practical in multi-PKG environment. Lal and Sharma [9] proved that the security of Wang and Cao scheme is based on Bilinear Diffie-Hellman problem (BDHP). The identity based signature based on pairings was proposed in [5, 8].

The first identity based signcryption (IBSC) scheme was proposed by Malone Lee [11] in 2002 which is based on bilinear pairing on elliptic curve. Several identity based signcryption algorithm have been proposed so far e.g. [4, 6, 7, 10, 11, 12]. With in this handful of results, only [4, 6, 7, 10,] consider schemes supported by formal models and security proofs in the random oracle model. Among all schemes supported by security proofs in formal security models, Chen and Malone Lee's proposal [6] happens to be most efficient construction.

All the identity based signcryption schemes mentioned above have the environment in which sender and receiver belongs to the same private key generator (PKG). In this paper we propose an identity based signcryption scheme in which sender and receiver may belong to different PKG. We are also considering the security notions of signcryption in multi-PKG environment. Detailed discussions of these notions are given in section 3.

The paper follows the approach as in [6] and will proceed as follows. In section 2 we formally define identity based signcryption in multi-PKG environment. Section 3 deals with the security models. In section 4 we give the definition of bilinear pairing and of some computationally hard problems. We present our scheme in section 5 and provide security results in section 6. The paper ends with some concluding remarks.

2. Identity based signcryption:

An identity based signcryption scheme in multi-PKG environment consists of the following seven algorithms: **Gen-Setup**, **PKG-Setup**, **Extract**, **Sign**, **Encrypt**, **Decrypt** and **Verify** described below:

Gen-Setup: On input of a security parameter 1^k the trusted authority uses this algorithm to produce **params**, where params are the general public parameters for the system. The params includes a description of a finite message space $\mathcal{M}$, a description of a finite signature space $\mathcal{S}$ and a finite ciphertext space $\mathcal{C}$. We assume that params are publicly known and there is no need to explicitly provide them as input to other algorithms.

PKG-Setup: Each PKG uses this algorithm to produce his public key (P_{pub}) and his private key (s).

Extract: On input of an identity ID_U of a user U, a PKG uses this algorithm to compute secrete key S_U corresponding to ID_U.

Sign: User A (with identity ID_A and secrete key S_A) uses this algorithm with input (m, S_A, ID_B) to produce a signature σ on m valid under the public key derived from ID_A. It also produces some ephemeral data r.

Encrypt: On input of (ID_B, m, σ, r), A uses this algorithm to produce a ciphertext c. This is the encryption of m, ID_A and ID_A's signature on m, which can be decrypted using S_B.

Decrypt: User B uses this algorithm with input (c, S_B) to produce (m, ID_A, σ) where m is the message and σ is the purported signature by ID_A on m.

Verify: On input of (m, ID_A, σ), this algorithm outputs $\top$ if σ is ID_A's signature on m and output $\perp$ otherwise.

The above algorithms have the following consistency requirement. If

$$(m, \sigma, r) \leftarrow \textbf{Sign}(m, S_A, ID_B)$$

$$c \leftarrow \textbf{Encrypt}(ID_B, m, \sigma, r)$$

$$(\hat{m}, \hat{ID_A}, \hat{\sigma}) \leftarrow \textbf{Decrypt}(c, S_B)$$

then we must have $\hat{ID_A} = ID_A$, $m = \hat{m}$ and

$$\top \leftarrow \textbf{Verify}(\hat{m}, \hat{ID_A}, \hat{\sigma}, ID_B).$$

3. Security notions:

In this section we give the security model for identity based signcryption in multi-PKG environment.

3.1 Message Confidentiality

The accepted notion of security with respect to confidentiality for public key encryption is indistinguishability of encryptions under adaptive chosen ciphertext attack. The notion of security defined in the game below is a natural adaptation of this notion to the multi-PKG environment.

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting params to the adversary. It also provides public keys of PKGs to the adversary and keeps their private keys secrete.

Phase1: The challenger is probed by the adversary who makes the following queries.

- **Sign/Encrypt:** The adversary submits a sender and receiver identity with their corresponding PKG and a message to the challenger. The challenger responds with the signature of the sender on the message, encrypted under the public key of the receiver.
- **Decrypt/Verify:** The adversary submits a ciphertext and a receiver's identity along with its PKG to the challenger. The challenger decrypts the ciphertext under the secrete key of receiver. It then verifies that the resulting decryption is a valid message/signature pair under the public key of the decrypted identity and its corresponding PKG. If so the challenger returns the message, its signature and the identity of the signer, otherwise it returns $\perp$.
- **Extract:** The adversary submits an identity with its PKG to the challenger. The challenger responds with the secrete key of that identity.

At the end of phase1 the adversary outputs two identity $\{ID_A, ID_B\}$ with their PKG and two messages $\{m_0, m_1\}$. The adversary must not have made extraction query on ID_B.

Challenge: The challenger chooses a bit b uniformly at random. It signs m_b under secrete key corresponding to ID_A and encrypts the result under the public key of ID_B to produce c. The challenger returns c to the adversary.

Phase2: The adversary continues to probe the challenger with the same type of queries that it made in the phase1. It is not allowed to extract the private key corresponding to ID_B and it is not allowed to make a decrypt/verify query for c under ID_B.

Response: The adversary returns a bit b'. The adversary wins if $b' = b$.

Definition1: Let $\mathcal{A}$ denote an adversary that plays the game above. If the quantity $\mathbf{Adv}[\mathcal{A}] = \left| \Pr[b' = b] - \frac{1}{2} \right|$ is negligible we say that the scheme is *semantically secure against adaptive chosen ciphertext attack*, or IND-IBSC-CCA2 secure.

Note that above definition deals with insider security since the adversary is assumed to have access to the private key of the sender of a signcrypted message. This means that confidentiality is preserved even if a sender's key is compromised.

3.2 Signature Non-repudiation

Regarding the property of authentication and non-repudiation, the following definition formalize the inability of any adversary to create a cipher text containing a message authenticated by some user without knowing the latter's private key. We define the notion of non-repudiation via the following game

Game

Initial: The challenger runs **Setup** (1^k) and gives the resulting params to the adversary. It also provides public keys of PKGs to the adversary and keeps their private keys secrete.

Probing: The challenger is probed by the adversary who makes queries as in the phase1 of the game in section 3.1.

Forge: The adversary returns a recipient identity ID_B with its PKG and a ciphertext c. Let (m, ID_A, σ) be the result of decrypting c under the secrete key corresponding to ID_B. The adversary wins if $ID_A \neq ID_B$; **Verify** $(m, ID_A, \sigma) = \top$; no extraction query was made on ID_A; no sign/encrypt query (m, ID_A, σ) was responded to with a ciphertext whose decryption under the private key of ID_B is (m, ID_A, σ).

Definition2: Let $\mathcal{A}$ denote an adversary that plays the game above. If the quantity **Adv**[$\mathcal{A}$]=Pr[$\mathcal{A}$ wins] is negligible we say that the scheme is *existentially unforgeable against insider chosen message attack*, or EUF-IBSC-CMA secure.

Definition2 allows the adversary access to the secret key of the recipient of the forgery. It is this that gives us insider security.

4. Definitions:

Bilinear Pairings: Let G_1 be an additive group of order q, a prime and G_2 be a multiplicative group of same 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) $\forall P, Q \in G_1, \forall a, b \in \mathbb{Z}_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$

(ii) For any point $P \in G_1, e(P, Q) = 1$ for all $Q \in G_1$ iff $P = \mathcal{O}$, the identity of G_1.

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

Computational Diffie-Hellman Problem (CDHP): Given P, aP, bP in G_1, for some (unknown) $a, b \in \mathbb{Z}_q^*$, compute abP in G_1.

Modified Computational Diffie-Hellman Problem (mCDHP): Given P, aP, a^{-1}P bP in G_1, for some (unknown) $a, b \in \mathbb{Z}_q^*$, compute abP in G_1.

Bilinear Diffie-Hellman Problem (BDHP): Given P, aP, bP, cP in G_1, for some (unknown) $a, b, c \in \mathbb{Z}_q^*$, compute $e(P, P)^{abc}$ in G_2.

Bilinear Decision Diffie-Hellman Problem (BDDHP): Given P, aP, bP, cP in G_1 and $h \in G_2$, for some (unknown) $a, b, c \in \mathbb{Z}_q^*$, decide whether $h = e(P, P)^{abc}$.

Modified Bilinear Diffie-Hellman Problem (mBDHP): Given P, aP, a^{-1}P, bP, cP in G_1, for some (unknown) $a, b, c \in \mathbb{Z}_q^*$, compute $e(P, P)^{abc}$ in G_2.

Modified Bilinear Decision Diffie-Hellman Problem (mBDDHP): Given P, aP, a^{-1}P, bP, cP in G_1 and $h \in G_2$, for some (unknown) $a, b, c \in \mathbb{Z}_q^*$, decide whether $h = e(P, P)^{abc}$.

It is to be noted that mCDHP, (mBDHP, mBDDHP) is no harder than CDHP (BDHP, BDDHP) in polynomial time. Moreover, no known existing algorithm solves mCDHP, mBDHP or mBDDHP.

5. The Scheme:

In this section we describe our identity based signcryption scheme in multi-PKG environment. We will refer to the scheme as IBSC henceforth.

Gen-Setup:

– Establishes parameters G_1, G_2, q, $e: G_1 \times G_1 \to G_2$, $H_0: \{0,1\}^{k_1} \to G_1$, $H_1: \{0,1\}^{2k_0+n} \to \mathbb{Z}_q^*$, $H_2: G_2 \to \{0,1\}^{k_0+k_1+n}$ where k_0 is the number of bits required to represent an element of G_1; k_1 is the number of bits required to represent an identity; and n is the number of bits of a message to be signed and encrypted.

– Chooses P, a generator of cyclic group G_1.

– The system parameters **params** are $\langle G_1, G_2, q, e, P, n, H_0, H_1, H_2 \rangle$.

PKG-Setup:

– Each private key generator PKG_i chooses his own private key $s_i \in \mathbb{Z}_q^*$

– Calculates his public key $P_{pub_i} = s_i^{-1} P$.

Extract: For given identity $ID_U \in \{0,1\}^{k_1}$

– Computes the public key $Q_U = H_0(ID_U)$

– Computes the secrete key $S_U = s_i\, Q_U$ under the PKG_i.

Sign: For user A under PKG_1 to sign $m \in \{0,1\}^n$ with private key $S_A = s_1 H_0(ID_A)$ corresponding to public key $Q_A = H_0(ID_A)$ for the receiver B

– Choose r uniformly and randomly from $\mathbb{Z}_q^*$

– Computes $X = rQ_A$, $Q_B = H_0(ID_B)$, $h_1 = H_1(X \,||\, Q_B \,||\, m)$ and $Z = (r + h_1) S_A$

– Returns and forwards the signed message as (m, h_1, X, Z) to **Encrypt**.

Encrypt: To encrypt the signed message (m, h_1, X, Z) by A for receiver B under PKG_2

– Computes $U = h_1 P_{pub_2}$

– Computes $\omega = e(P, Q_B)^{h_1}$

– Computes $y = H_2(\omega) \oplus (Z \,||\, ID_A \,||\, m)$ and returns ciphertext (X, U, y).

Decrypt: For user B to decrypt (X, U, y) using $S_B = s_2 H_0(ID_B)$

– Computes $\omega' = e(U, S_B)$ and $y \oplus H_2(\omega') = Z \,||\, ID_A \,||\, m$

– Computes $h_1 = H_1(X \,||\, Q_B \,||\, m)$

– Accept the message iff $U = h_1 P_{pub_2}$ otherwise return $\perp$

– Forward message m, (X, Z) and purported sender A with PKG_1 to **Verify**.

Verify: To verify user A's signature under PKG_1

– Compute $Q_A = H_0(ID_A)$

– If $e(Ppub_1, Z) = e(P, X + h_1 Q_A)$, return $\top$. Else return $\perp$.

Now we will show the scheme is consistent,

$$\begin{aligned}\omega' = e(U, S_B) &= e(h_1 P_{pub_2}, s_2 Q_B) \\ &= e(s_2^{-1} P, s_2 Q_B)^{h_1} \\ &= e(P, Q_B)^{h_1} = \omega\end{aligned}$$

$$\begin{aligned}e(Ppub_1, Z) &= e(s_1^{-1} P, (r + h_1) S_A) \\ &= e(s_1^{-1} P, (r + h_1) s_1 Q_A) \\ &= e(P, rQ_A + h_1 Q_A) \\ &= e(P, X + h_1 Q_A)\end{aligned}$$

Note that proposed IBSC scheme is a combination of Wang and Cao encryption scheme [14] and a variant of Cha-Cheon signature scheme [5] in the manner that it is semantically secure against adaptive chosen ciphertext attacks as well as existentially unforgeable against insider chosen message attacks.

6. Security:

In this section we state the security results for the IBSC scheme under the definition of section 3. The proofs which are suitable modification in the proofs in [6], are available in pre-print.

All our security results are based on the modified Bilinear Diffie-Hellman Problem (mBDHP) defined in section 4. Our results assume that the hash functions H_0, H_1 and H_2 in the IBSC scheme are all random oracles. In each of the results below we assume that the adversary makes q_i queries to H_i for i= 0, 1, 2. The number of sign/encrypt and decrypt/verify queries made by the adversary are denoted by q_s and q_d respectively.

6.1 Message Confidentiality

Theorem 1. If there is an IND-IBSC-CCA2 adversary $\mathcal{A}$ of IBSC that succeeds with probability ϵ, then there is a simulator $\mathcal{B}$ running in polynomial time that solves the mBDHP with probability at least

$$\epsilon \cdot \left(1 - \frac{q_s(q_1 + q_s)}{q}\right) \cdot \frac{1}{q_0 q_2}$$

6.2 Signature Non-repudiation

Theorem 2. If there is an EUF-IBSC-CMA adversary $\mathcal{A}$ of IBSC that succeeds with probability ϵ, then there is a simulator $\mathcal{B}$ running in polynomial time that solves the mBDHP with probability at least

$$\epsilon \cdot \left(1 - \frac{q_s(q_1 + q_s)}{q}\right)^2 \cdot \frac{1}{4q_0^2(q_1 + q_s)^2}$$

Remark: Boyen [4] gave three additional security notions ciphertext unlinkability, ciphertext authentication and ciphertext anonymity for identity based signcryption schemes. The proposed scheme does not possess the ciphertext unlinkability, ciphertext authentication, ciphertext anonymity as per the definition of [4]. However, in the proposed scheme an adversary C can create a valid ciphertext for the receiver B, if C knows the signature of

sender A on a message m. Also the proposed scheme resists the man in middle attack as in the signature we use receiver public key Q_B .

Conclusion:

We present a signcryption scheme which has the sign then encrypt approach and which is more efficient in the multi-PKG environment. One advantage of the scheme is that the signer can compute all the term without knowing the receiver PKG. As soon as and as he knows the receiver's PKG he just computes $U = h_1 P_{pub_2}$ and sends the ciphertext (X, U, y). We note that Wang and Cao [14] basic encryption scheme does not have chosen ciphertext security, however, our use of the signature part of the proposed scheme achieves message confidentiality against adaptive chosen ciphertext attack by checking the integrity of message.

Reference:

1. J. H. An, Y. Dodis and T. Rabin: On the security of joint signature and encryption. EUROCRYPT 2002, LNCS # 2332, Springer-Verlag, 2002, 83-107.
2. J. Beak, R. Stenfield and Y. Zheng: Formal proofs for the security of signcryption. PKC-2002, LNCS # 2274, Springer-Verlag, 2002, 80-98.
3. D. Boneh and M. Franklin: Identity–based encryption scheme from Weil pairing. CRYPTO 2001, LNCS # 2139, Springer-Verlag, 2001, 213-229.
4. X. Boyen: Multipurpose Identity based signcryption: A Swiss army knife for identity based cryptography. CRYPTO 2003, LNCS # 2729, Springer-Verlag, 2003, 389-399.
5. J.C. Cha and J.H. Cheon: An identity-based signature from Gap Diffie-Hellman Groups. PKC-2003, LNCS # 2567, Springer-Verlag, 2003, 18-30.
6. L. Chen and J. Malone-Lee: Improved Identity-based signcryption. PKC 2005, LNCS # 3386, Springer-Verlag, 2005, 362-379.
7. S. S. M. Chow, S. M. Yiu, L. C. K. Hui and K. P. Chow: Efficient forward and provably secure ID based signcryption scheme with public verifiability and public cipher text authenticity. ICISC'2003, LNCS # 2971, Springer-Verlag, 2003, 352-369
8. F. Hess: Efficient identity-based signature scheme based on pairings. In proceedings of selected areas in cryptography 2003, LNCS # 2595, Springer-Verlag, 2003, 310-324.
9. Sunder Lal and Priyam Sharma: Security proof for Shengbao Wang's identity based encryption scheme. Cryptology ePrint Archive, Report 2007/316, http://eprint.iacr.org/2007/316.pdf, 2007.
10. B. Libert and J.J. Quisquater: New Identity based signcryption schemes from pairings. IEEE Information Theory Workshop, Paris (France) 2003.
11. J. Malone-Lee: Identity-Based signcryption. Cryptology ePrint Archive, Report 2002/ 098, 2002, http://eprint.iacr.org/.
12. D. Nalla and K. C. Reddy: Signcryption scheme for identity based cryptosystems. Cryptology ePrint Archive, Report 2003/066, http://eprint.iacr.org/2003/066.pdf, 2003.
13. A. Shamir: Identity-based cryptosystems and signature schemes. CRYPTO 84, LNCS # 196, Springer-Verlag, 1984, 47-53.
14. S. Wang and Z. Cao: Practical identity-based encryption (IBE) in multiple PKG environment and its applications, http://eprint.iacr.org/2007/100.pdf, 2007.
15. Y. Zheng: Digital signcryption or How to Achieve cost (Signature & Encryption) << cost (Signature) + cost (Encryption). CRYPTO'97, LNCS # 1294, Springer-Verlag, 1997, 165-179.