A PROVABLY SECURE MULTI-RECEIVER IDENTITY-BASED SIGNCRYPTION USING BILINEAR MAPS

Shivaramakrishnan Narayan and Parampalli Udaya
Department of Computer Science and Software Engineering
University of Melbourne, Victoria - 3010, Australia

Keywords: Identity based Cryptography, Bilinear Maps, Signcryption, Multi-Receiver, Existential Unforgeability, Adaptive Chosen Ciphertext Attack.

Abstract: In this paper, we present a new, efficient multi-receiver identity (Id) based signcryption scheme. Our signcryption construction involves no pairing operations for sign-encrypt unlike other schemes which require at least one pairing. The scheme provides confidentiality, authenticity, non-repudiation and facilitates public verifiability. We provide the security result of our scheme in the random oracle model for message confidentiality and signature unforgeability properties under the multi-receiver security notion.

1 INTRODUCTION

Practical applications demand confidentiality, authenticity and non-repudiation simultaneously at low cost, signcryption is a public key primitive which perfectly meet such requirements. The idea of signcryption was first proposed by Zheng in 1997. Signcryption has always been defined for a single sender/receiver scenarios. Evolving applications using multi-casting present the need of cryptographic primitive such as signcryption to achieve confidentiality and authentication at a low cost/time. For example, in an organizational set up we might need to send a common message to multiple employees. This leads to a multi receiver scenario where the sender and the multiple receivers require both confidentiality and authentication. This can be addressed using a multi-receiver signcryption. But as in case of a conventional signcryption, it should be computationally infeasible for any unauthorized user to recover the encrypted message and also computationally infeasible to forge the signature.

The idea of a multi-receiver based setting was first proposed by Bellare et al. (Bellare et al., 2000) for public key encryption. Later in 2002, Kurosawa (Kurosawa, 2002) presented a multi-receiver public key encryption scheme using *randomness re-use* approach.

In this paper we are concerned with multi-receiver signcryption in Identity (Id) based cryptography using bilinear maps. The main difference between traditional cryptography and Id-based cryptography is in the way a public key is defined. In Id-based cryptography, a public key is a function of user's identity unlike in traditional cryptography where user's public key is a random string. Shamir proposed the concept of Id-based signature scheme in (Shamir, 1984). It was only after Joux presented the tripartite key agreement protocol (Joux, 2000), Boneh-Franklin (Boneh and Franklin, 2001) and Sakai et al. (Sakai et al., 2001) in 2001, independently proposed a practical Id-based encryption scheme using bilinear pairing on elliptic curves.

1.1 Our Contributions

In this paper, we present a new, efficient and provably secure multi-receiver Id-based signcryption scheme which provides confidentiality and authenticity. The public parameters of our scheme uses pre-computed pairing values and hence, the signcrypt function does not require any pairing computations thereby improving the efficiency.

We present a semantically secure scheme with public verifiability and present the security results for message confidentiality and signature unforgeability

Narayan S. and Udaya P. (2007).
A PROVABLY SECURE MULTI-RECEIVER IDENTITY-BASED SIGNCRYPTION USING BILINEAR MAPS.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 305-308
DOI: 10.5220/0002130103050308

properties. Public verifiability is defined as follows: given a signature, and possibly some additional information provided by the recipient, any third party would effectively be able to verify the authenticity of the signature. We present a slightly modified security model addressing the presence of multiple receivers, where we assume one sender and multiple receivers. The security notion followed in this paper for message confidentiality and signature unforgeability is given in Section 3. The security results are based on the intractability of collision attack assumption (CAA) and bilinear collision attack assumption (BCAA). These problems are equivalent to well known hard problems in cryptography: the CAA is equivalent to inverse computational Diffie-Hellman (Mitsunari et al., 2002) and the BCAA is equivalent to inverse bilinear Diffie-hellman assumptions (Chen and Cheng, 2005).

The paper is organized as follows: Section 2 gives the mathematical preliminaries required for Id-based cryptography, followed by the security model of the scheme in Section 3. We describe our scheme in Section 4. In Section 5, we discuss the security of our signcryption scheme. Section 6 describes the efficiency of our scheme in comparison to other signcryption schemes. Finally, we present our conclusion in Section 7.

2 BACKGROUND

Our scheme is defined using bilinear maps on elliptic curves. Consider two groups G_1 and G_2, additive and multiplicative in nature respectively of the same prime order q. Let Z_q^* denote the set of all non-zero integers modulo prime q. A bilinear map is a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$, satisfying the following properties.

Bilinearity: $\forall P,Q \in G_1$, $\forall a,b \in Z_q^*$, we have $\hat{e}(aP,bQ) = \hat{e}(P,Q)^{ab}$.

Non-degeneracy: Given a point $P \in G_1$, $\hat{e}(P,Q) = 1$, $\forall Q \in G_1$, iff $P = O$.

Computable: There exists an efficient algorithm to compute $\hat{e}(P,Q)$.

We discuss the important Diffie-Hellman assumptions used in our scheme. A detailed explanation of other related Diffie-Hellman assumptions and its equivalence is presented in the extended paper[1].

Definition 2.0.1 *Given a group G_1 of prime order q, a generator $P \in G_1$, an integer k, $x \in_R Z_q^*$ and $\left(P, h_1, ..., h_k \in Z_q^*, \frac{1}{h_1+x}P, ..., \frac{1}{h_k+x}P\right)$, the collision attack assumption is to compute $\frac{1}{h+x}$ for some $h \notin \{h_1, ...h_k\}$. An algorithm $\mathcal{A}_{k-CAA}$ solves k-CAA problem with the probability ε if $Pr[\mathcal{A}_{k-CAA}(P, xP, \frac{1}{h_1+x}P, ..., \frac{1}{h_k+x}P) = \frac{1}{h+x}P] \geq \varepsilon$, where the probability is over the random choice of generator $P \in G_1$, $x \in Z_q^*$, $h_1, ..., h_k \in Z_q^*$ and $h \notin \{h_1, ...h_k\}$.*

Definition 2.0.2 *Given a group G_1 of prime order q, a generator $P \in G_1$, an integer k, $x \in_R Z_q^*$ and $\left(P, h_1, ..., h_k \in Z_q^*, \frac{1}{h_1+x}P, ..., \frac{1}{h_k+x}P\right)$, the bilinear collision attack assumption is to compute $\hat{e}(P,P)^{\frac{1}{h+x}}$ for some $h \notin \{h_1, ...h_k\}$. An algorithm $\mathcal{A}_{k-BCAA}$ solves k-BCAA problem with the probability ε if $Pr[\mathcal{A}_{k-CAA}(P, xP, \frac{1}{h_1+x}P, ..., \frac{1}{h_k+x}P) = \hat{e}(P,P)^{\frac{1}{h+x}}] \geq \varepsilon$, where the probability is over the random choice of generator $P \in G_1$, $x \in Z_q^*$, $h_1, ..., h_k \in Z_q^*$ and $h \notin \{h_1, ...h_k\}$.*

3 SECURITY NOTIONS

In this section, we provide the security definitions of the signcryption scheme for message confidentiality and signature non-repudiation properties in the multi-receiver model.

Definition 3.0.3 *We say that a multi-receiver Id-based signcryption scheme (MIDSC) has the indistinguishability against adaptive chosen ciphertext attack property (IND-MIDSC-CCA2), if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following attack game.*

Start-up: The challenger runs the **Setup** algorithm of the scheme and sends the global system parameter to the adversary $\mathcal{A}$.

Phase 1**:** $\mathcal{A}$ performs polynomially bounded number of queries to the following oracles:

Extract: The adversary submits an identity ID_i to the challenger. The challenger responds with the secret key S_{ID_i} for that identity.

Signcrypt: The adversary submits a sender identity, the receiver's identity $(ID_1, ...ID_N)$ and a message M to the challenger. The challenger responds with the signcryption of the message processed with private key of the sender and public key of the receivers.

Decrypt/Verify: The adversary submits a ciphertext and identities of the receivers to the challenger. The challenger decrypts the ciphertext under the secret key of the receivers. It then verifies the message and signature pair under the public key of the decrypted identity. If the verifcation succeeds, the challenger returns the message, the signature and the identity of the signer, otherwise $\perp$.

[1]The extended paper will appear in eprint and is also available at http://www.csse.unimelb.edu.au/∼udaya

At the end of Phase 1, the adversary outputs sender's identity ID_A, the identities of the receivers $(ID_1^*,....ID_N^*)$ as the challenge identities, and two messages M_0, M_1. The challenge identities that the adversary submits must satisfy the criteria: $ID_i^* \notin \{ID_1,.....ID_{q_0}\}$ for $1 \leq i \leq N$, where N denotes the number of receivers. No extraction query on $(ID_1^*,....ID_N^*)$ is allowed to be made by the adversary.

Challenge: The challenger chooses a random bit b and computes the signature and encryption of the message and sends the ciphertext to the adversary.

Phase 2: The adversary continues to probe the challenger with the same type of queries that it made in Phase 1. It is not allowed to, extract the private key corresponding to any identity in $(ID_1^*,....ID_N^*)$ and to make a decrypt/verify query for the ciphertext under sender ID_A and any receiver's identity in $(ID_1^*,....ID_N^*)$.

Response: The adversary outputs a bit b' and wins the game if $b' = b$. The adversary's advantage is defined to be $Adv(\mathcal{A}) = |\Pr[b' = b] - 1/2|$[2].

Definition 3.0.4 *We say that a multi-receiver Id-based signcryption scheme (MIDSC) has existential unforgeability property against chosen-message attack or (EUF-MIDSC-CMA), if no polynomially bounded adversary $\mathcal{A}$ has a non-negligible advantage in the following attack game.*

The Start-up and Phase 1 follows from the CCA2 game detailed above. After Phase 1, the adversary outputs a sender identity ID_A and recipients identity $(ID_1^*,.....ID_N^*)$ as challenge identities. After issuing the challenge identities, the adversary can make additional queries as given in Phase 1. But the adversary cannot make an extraction query on ID_A.

Forge: The adversary returns the recipients identities $(ID_1^*,.....ID_N^*)$ and a ciphertext. Let (M, ID_A) be the resulting message under the secret key corresponding to ID_i^*, where $(1 \leq i \leq N)$.

Response: The adversary wins if $ID_A \neq ID_i^*$, for all $1 \leq i \leq N$. The ciphertext should not result from a signcrypt query $Signcrypt(M,\ ID_A,\ (ID_1^*,.....ID_N^*))$. The adversary's advantage is defined to be $Adv(\mathcal{A}) = \Pr[\mathcal{A}\ wins]$.

4 OUR SCHEME

Let k_1, k_2, k_3, n denote the number of bits required to represent an identity, an element in G_2, an element in G_1 and the message respectively. We define the hash functions $(H_0,\ H_1,\ H_2)$ such that, $H_0 : \{0,1\}^{k_1} \rightarrow Z_q^*,\ H_1 : \{0,1\}^{k_2+n} \rightarrow Z_q^*,\ H_2 : G_2 \rightarrow \{0,1\}^{k_1+k_3+n}$. Let N denote the number of receivers.

Setup: $params = [P, P_{pub} = sP, P'_{pub} = s^2P, g = \hat{e}(P,P), g_1 = \hat{e}(P, P_{pub}), H_0 : \{0,1\}^{k_1} \rightarrow Z_q^*, H_1 : \{0,1\}^{k_2+n} \rightarrow Z_q^*, H_2 : G_2 \rightarrow \{0,1\}^{k_1+k_3+n}]$, where $P \in E[q]$ and $s \in Z_q^*$ is the master secret of the private key generator .

Extract: Given a public Id of a user with "*identity*" $\in \{0,1\}^{k_1}$, the private key generator does the following:

(1) $ID = H_0(\text{"}identity\text{"})$.

(2) Secret key $S_{ID} = (s + ID)^{-1}P$.

(3) Return (S_{ID}).

Signcrypt $(M, ID_{sender}, (ID_1,....ID_N))-$

(1) Choose $r \in_R Z_q^*$ and Compute, $Y = g_1^r$.

(2) Compute, $V = g^r$, $M' = H_1(M||V)$, $w = H_2(Y)$.

(3) $Z = (r + M')S_{sender}$.

(4) $C = (M||Z||ID_{sender}) \oplus w$.

For $i = 1$ to N do, choose $t_i \in_R Z_q^*$ and compute, $U_i = ((r + t_i)P'_{pub} + (r + t_i)ID_iP_{pub}, t_iP)$.

The ciphertext is $(C, U_1.....U_N, V)$.

Decrypt/Verify: Obtain the secret key S_{ID_i} from the private key generator and compute:

(1) $(M||Z||ID_{sender}) = C \oplus H_2(\frac{\hat{e}(U_i[1], S_{ID_i})}{\hat{e}(U_i[2], P_{pub})})$.

(2) $M' = H_1(M||V)$.

Accept the message if,

$\hat{e}(P_{pub} + ID_{sender}\ P, Z) = g^{M'}\ V$.

5 SECURITY RESULTS

In this section, we briefly state the security results for the attack models explained in Section 3. The detailed proof will appear in the extended paper in eprint or can be obtained from the second author's webpage[3]. All our results are based on the intractability of k-BCAA problem and k-CAA problem. Whilst proving our scheme, we assume that the adversary $\mathcal{A}$ makes q_i queries to the hash oracle H_i for $i = 0, 1, 2$. The number of signcrypt and decrypt/verify queries made by the adversary is denoted as q_s and q_d respectively.

Theorem 5.0.1 *If there exists an EUF-MIDSC-CMA adversary $\mathcal{A}$ that succeeds against chosen message attack game with a probability ε, then there is a challenger $\mathcal{B}$ running in polynomial time that solves the q_0-CAA problem with probability ε' of at least*

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

[2] Pr[] denotes probability of an event occurring.

[3] http://www.csse.unimelb.edu.au/∼udaya

Theorem 5.0.2 *If there exists an IND-MIDSC-CCA2 adversary $\mathcal{A}$ that succeeds against the indistinguishability of chosen ciphertexts attack game with a probability ε, then there is a challenger $\mathcal{B}$ running in polynomial time that solves the q_0-BCAA problem in G_2 with probability ε' of at least*

$$\frac{\varepsilon}{(q_0+N)q_2}(1-\frac{q_d}{q}).$$

6 EFFICIENCY OF OUR SCHEME

In Table 1, we compare the efficiency of our scheme with known multi-receiver based signcryption constructions.

Table 1: Comparison of Signcryption Schemes.

Mult = Multiplication Exp = Exponentiations			
Schemes	G_1 Mult.	Pairing	G_2 Exp.
(Duan and Cao, 2006)	$4+N_{receivers}$	5	0
(Boyen, 2003)	5	$4+N_{receivers}$	1
Ours	$2+N_{receivers}$	3	3

The scheme presented by Boyen (Boyen, 2003) is based on performing signature once for all the receivers and encrypting for each user. This increases the computational cost because a sender has to perform $N_{receivers}$ pairing operations, where $N_{receivers}$ denotes total number of receivers. Further, the ciphertext size also increases since it includes the encryption for each receiver which is $2N_{receivers}|G_1|+|ID|+|M|$, where M denotes the message and ID denotes the user identity. The most recent multi-receiver based signcryption presented by S. Duan and Z. Cao (Duan and Cao, 2006) in 2005 uses one pairing operation for signcryption and the message is signcrypted only once for all receivers but the randomness is calculated for each receiver in blinded form. Overall, the scheme uses five pairing operations (four for Decrypt/Verify operation). The ciphertext size of their scheme is $(N_{receivers}+2)|G_1|+|M|+|ID|$. In any multi-receiver based schemes, the size of the ciphertext necessarily is linear in number of receivers.

The computational efficiency of our scheme (in single receiver scenario) can be compared to (Barreto et al., 2005). The main computational cost involved in Id-based cryptography using bilinear maps is the cost of performing a pairing operation. In our scheme, the signcryption does not involve any pairing operation, thus the computations from a signer's perspective is minimal. The scheme presented in Section 4 can also be defined over Co-gap groups which offer reduced public parameters size and increased computational efficiency.

7 CONCLUSION

In this paper, we presented a public verifiable, semantically secure multi-receiver signcryption scheme using bilinear pairings. The scheme is efficient in terms of computational complexity and also is provably secure under chosen message and chosen ciphertext attack. We believe our scheme is more efficient than all others proposed so far.

REFERENCES

Barreto, P., Libert, B., McCullagh, N., and Quisquater, J. (2005). Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In *ASIACRYPT 2005*, volume 3788, pages 515–532. Lecture notes in computer science, Springer, Berlin,.

Bellare, M., Boldyreva, A., and Micali, S. (2000). Public-key encryption in a multi-user setting: Security proofs and improvements. In *B. Preneel (Ed.), Advances in Cryptology EUROCRYPT, 2000*, volume 1807, pages 259–274. LNCS, Springer- Verlag, Berlin Germany.

Boneh, D. and Franklin, M. (2001). Identity based encryption from weil pairing. In *J. Kilian, editor, CRYPTO 2001*, volume 2139, pages 213–229. LNCS, Springer-Verlag, Berlin.

Boyen, X. (2003). Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography. In *Proceedings of Crypto-2003*, volume 2729, pages 383–399. LNCS, Springer- Verlag, Berlin.

Chen, L. and Cheng, Z. (2005). Security proof of sakai-kasahara's identity-based encryption scheme. In *Cryptography and coding (10th IMA Intl Conf., Cirencester, UK, December 19-21, 2005)*, volume 3796, pages 442–459. Lecture notes in computer science, Springer, Berlin, ALLEMAGNE.

Duan, S. and Cao, Z. (2006). Efficient and provably secure multi-receiver identity-based signcryption. In *ACISP 2006*, volume 4058, pages 195–206. LNCS, Springer-Verlag, Berlin.

Joux, A. (2000). A one round protocol for tripartite diehellman. In *Proc. 4th Alg. Numb. Th. Symp.*, volume 1838, pages 385–294. Lecture notes in computer science, Springer, Berlin.

Kurosawa, K. (2002). Multi-recipient public-key encryption with shortened ciphertext. *Proceedings of the Fifth International Workshop on practice and theory in Public Key Cryptography (PKC'02)*, pages 48–63.

Mitsunari, S., Sakai, R., and Kasahara, M. (2002). A new traitor tracing. pages 481–484. IEICE Transactions Fundamentals, E85-A(2).

Sakai, R., Ohgishi, K., and Kasahara, M. (2001). Cryptosystems based on pairing over elliptic curve. *The 2001 Symposium on Cryptography and Information Security*.

Shamir, A. (1984). Identity-based cryptosystems and signature schemes. *Lecture Notes in Computer Science*, 196:47–53.