Signcryption scheme for Identity-based Cryptosystems

Divya Nalla, K.C.Reddy

AILab, Dept of Computer/Info. Sciences, University of Hyderabad, Gachibowli, Hyderabad, 500046, India
divya@msitprogram.net, kcrcs@uohyd.ernet.in

Abstract

An Identity-based cryptosystem is a Public Key cryptosystem in which the public keys of the entities are their identities, or strings derived from their identities. Signcryption combines digital signatures and encryption with a cost significantly smaller than that required for signature-then-encryption. This paper proposes an ID-based signcryption scheme based on bilinear pairings on elliptic curves. It is shown that the new scheme is an improved version of the existing signcryption scheme [10] by comparing the computations in both the schemes.

Keywords: Signature, Signcryption, Identity based cryptosystems, ID-based signcryption, ID-based signatures.

1. Introduction

An Identity-based cryptosystem is a novel type of cryptographic scheme proposed by Shamir [2], 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. Problems 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. Whilst ID-based PKCs will not replace the conventional Public Key infrastructures, it might prove to be a complementary technology.

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 centre(KGC) generates the private keys of the entities in the group using their public key. In 1984, Shamir [2] proposed the idea of identity-based cryptosystems. While the ID-based signature schemes have satisfactory solutions [1] [15], the first practical ID-based encryption scheme was that of Boneh and Franklin in 2001 [4]. Several other ID-based schemes [8] [5] [12] [13] were proposed based on Boneh-Franklin's scheme.

Suppose Alice wishes to send a message to Bob. It is required that the message should be authenticated and reach securely to Bob. In traditional Public key cryptosystems, Alice first agrees on a secret key with Bob, digitally signs the message using his private key, and sends the encrypted message along with the signature to Bob. Bob then decrypts the message and verifies the signature. Traditionally, this is done using a digital signature scheme and an encryption algorithm.

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. Forward secrecy is not offered in this scheme. Signcryption schemes with forward secrecy were proposed in [7]. But both these schemes did not provide non-repudiation. A formal model of security for signcryption with non-repudiation is proposed in [11].

This paper discusses various issues in signcryption, and proposes a new ID-based signcryption scheme. The efficiency of the new scheme is observed by comparing to the existing

ID-based signcryption scheme by Malone-Lee [10]. The security properties of the new scheme are discussed.

The paper is organized as follows. ID-based cryptosystems are introduced in section 2. Section 3 describes the original signcryption scheme by Zheng [16]. The ID-based signcryption scheme by Malone-Lee is discussed in Section 4. Section 5 discusses the new scheme. The security and efficiency of the new scheme are discussed in sections 6 and 7 respectively. Section 8 concludes the paper. The issues comparing ID-based cryptosystems with the traditional PKI are given in Appendix A.

2. ID-based Cryptosystems

The need to make available authentic copies of entities' public keys is a major drawback to the use of public-key cryptography. The traditional approach for doing this is to use the public key infrastructures, in which a certification authority (CA) issues a certificate which binds a user's identity with his/her public key. With ID-based cryptosystems, this binding is not necessary as the identity of the entity would be his/her public key (If not directly, the public key is derived from the identity).

In ID-based PKC, everyone's public Keys are predetermined by information that uniquely identifies them, such as their email address. This concept was first proposed by Shamir [2]. Shamir's original motivation for ID-based encryption was to simplify certificate management in e-mail systems. Each entity in the system sends his/her identity to a trusted third party called the Key Generation Center (KGC), to obtain the private key. The private key is computed using the private key of the KGC and the identity of the user. Key escrow is inherent in ID-based systems since the KGC knows all the private keys. For various reasons, this makes implementation of the technology much easier, and delivers some added information security benefits. ID-based PKC (ID-PKC) remained a theoretical concept until [3] and [4] were proposed.

Some of the issues to be addressed to compare the ID-based systems with the traditional PKI supported public-key cryptography are given by Paterson in [12] (given in appendix A).

3. Signcryption

Signcryption is a scheme which combines a function of digital signature scheme with a symmetric encryption algorithm. A digital signature scheme is used for the authentication of messages and an encryption scheme is used for the confidentiality of messages. Signcryption offers these two properties at the same time and a more efficient computational cost than the traditional signature-then-encryption.

3.1 Signcryption from shortened Digital signature scheme

The following is a digital signcryption scheme [16]. The public parameters used in the scheme are:

Parameters public to all:

p – a large prime
q – a large prime factor of p-1
g – an integer with order q modulo p chosen randomly from {1,….p-1}
hash – a one-way hash function whose output has, say, at least 128 bits
KH – a keyed one-way hash function
(E, D) – the encryption and decryption algorithms of a private key cipher.

A's Keys:

x_a - *A*'s private key, chosen uniformly at random from [1, ….. q-1]

y_a - *A*'s public key $y_a = g^{x_a} \bmod p$

B's Keys:

x_b - *B*'s private key, chosen uniformly at random from [1, ….. q-1]

y_b - *B*'s public key $y_b = g^{x_b} \bmod p$

A signcrypts a message *M* and sends the signcrypted message (C, r, s) to *B*.

Signcryption:

A carries out this process to send a message *M* to *B* authentically and securely.

1. Pick x uniformly at random from [1,….., *q*-1], and let $k = \text{hash}(y_b^x \bmod p)$.
   Split *k* into k_1 and k_2 of appropriate length.
2. $r = KH_{k_2}(M)$ (keyed hash function)
3. $s = x/(r + x_a) \bmod q$
4. $C = E_{k_1}(M)$
5. Send to *B*, the signcrypted text (C, r, s)

Unsigncryption:

B calculates original message from the received message (C, r, s)

1. Recover *k* from *r*,*s*, *g*, *p*, y_a and x_b:
   $k = \text{hash}\ ((y_a.g^r)^{s.x_b} \bmod p)$
2. Split *k* into k_1 and k_2
3. $M = D_{k_1}(C)$
4. Accept *M* as a valid message originated from *A* only if $KH_{k_2}(M)$ is identical to *r*.

The most significant advantage of signcryption over signature-then-encryption lies in the reduction of computational cost and communication overhead. It is shown in [16] that cost(signcryption << cost(signature) + cost(encryption). Zheng's scheme does not provide forward secrecy and non-repudiation. Note that during unsigncryption, the following is satisfied:

$hash\ ((y_a.g^r)^{s.x_b} \bmod p) = hash\ ((y_b^{x_a+r})^s \bmod p)$

B calculates $k = hash((y_a.g^r)^{s.x_b} \bmod p)$ using his private key x_b. But, when x_a is revealed, anyone can calculate $k = \text{hash}\ ((y_b^{x_a+r})^s \bmod p)$.

With signature-then-encryption, if *A* denies the fact that he/she is the originator of the message, all *B* has to do is to decrypt the message and present to a judge the message together with its associated signature by *A*, based on which the judge will be able to settle a dispute.

In case of signcryption, *B* unsigncrypts the message and presents the following data items to the judge: (p,q,g,y_a,y_b , *M, r, s*). from these data items alone, it cannot be judged that *A* had sent the message. To solve this problem, *B* and the judge have to engage in an interactive zero-knowledge proof/argument protocol.

Thus the scheme does not provide both forward secrecy and non-repudiation. A modified signcryption scheme providing forward secrecy is proposed in [7]. A signcryption model with non-repudiation is presented in [11].

Comparing signcryption to the traditional signature-then-encryption with a static key, signcryption is more desirable in view of the cost for both these algorithms. The signcryption scheme reduces the cost of the traditional signature-then-encryption by providing all the functionalities in a single and a more simple algorithm. A session key is also agreed in this process.

In a signcryption scheme, basically the sending party computes a secret key using the public information of the receiving party, encrypts the message using that key, and computes the signature using its private key. The signature and the encrypted text are sent to the receiver, where the receiver does some computations using his private key and the received signature to retrieve the key for decrypting the encrypted message.

Following the same approach, this paper proposes an ID-based signcryption scheme. A parallel work on ID-based signcryption by Malone-Lee [10] is discussed before discussing the new scheme.

4. IDSC

This section discusses a parallel work on ID-based signcryption by Malone-Lee [10]. Some initial settings are assumed in ID-based systems. These are similar to the *Setup* and *Extract* algorithms in [4]. The system parameters including a description of a finite message space, and a finite ciphertext space are assumed. Suppose G_1 is a subgroup of an Elliptic curve for which the modified Weil Pairing $\hat{e}$ [13] maps into the finite field G_2 . G_1 is an additive group of prime order q, and G_2 is a multiplicative group of the same order q. (i.e., The existence of a bilinear map $\hat{e}: G_1 \times G_1 \to G_2$ is also assumed). A cryptographic hash function H: $\{0, 1\}^* \to G_1$ is also defined. All these parameters are published.

The Key Generation Centre(KGC) chooses a secret Key $s \in Z_q^*$

The KGC produces a random $P \in G_1$ and computes $P_{KGC} = [s]P$. Then the KGC publishes (P, P_{KGC}) When a user with identity *ID* wishes to obtain a public/private Key pair, the public Key is given by $Q_{ID} = H(ID)$, and the KGC computes the private Key $S_{ID} = [s]\, Q_{ID}$

The initial parameters $G_1, G_2,$ hash function H , P, $P_{KGC} = [s]P$ (where s is the secret key of the key generation centre) are all published. Two more hash functions are defined: $H': \{0,1\}^* \to Z_q^*$ $H'': Z_q^* \to \{0,1\}^*$.

For signcrypting a message M intended for B, A performs the following steps:

1. A picks a random $x \in Z_q^*$
2. Computes the following:
   - $U = xP$
   - $r = H'(U \,||\, M)$
   - $W = x.P_{KGC}$
   - $V = r.S_A + W$
   - $y = \hat{e}(Q_B, W) = \hat{e}(Q_B, xP_{KGC}) = \hat{e}(Q_B, P_{KGC})^x$
     (Hence $\hat{e}(Q_B, P_{KGC})$ can be precomputed)
   - $k = H''(y)$
   - $C = k \oplus M$

3. *A* sends the signcrypted message $\sigma = (C, U, V)$

B knows the values (Q_A, S_B, σ), and unsigncrypts σ as follows:

1. *B* computes
   - $y = \hat{e}(S_B, U)$
   - $k = H''(y)$
   - $M = k \oplus C$
   - $r = H'(U \| M)$
2. *B* verifies if $\hat{e}(V, P) = \hat{e}(Q_A, P_{KGC})^r . \hat{e}(U, P_{KGC})$

If these are not equal, then it can be concluded that the message has been tampered en route, and hence can be rejected. Here, the value $\hat{e}(Q_A, P_{KGC})$, and the pairing $\hat{e}(P_{KGC}, Q_B)$ can be precomputed, and hence the total number of computations (considering the expensive ones) includes 5 weil pairings (of which 2 can be precomputed), 3 point multiplications, 1 exponentiation, and 2 hash functions.

In this scheme, the key *k* is computed from computations involving the message *M* and the public key of the receiver Q_B. The value *V* is computed from the private key of the sender S_A. Thus *U* and *V* constitute the signature comprising of values computed from the secret values (private keys) of the sender. At the receiver end, the receiver's private key S_B is used to compute the key for decrypting the message *M*.

An improved version of this scheme is proposed in the next section.

5. The new ID-based signcryption scheme

A new ID-based signcryption scheme is proposed in this section, based on the same principles as the original signcryption scheme of Zheng [16]. The first requirement in any signcryption scheme is to agree on a common key between the sender and receiver. Using this idea, signcryption and unsigncryption of a message $M \in \{0,1\}^*$ is done as follows.

The initial assumptions of the two groups G_1 and G_2 and the weil pairing $\hat{e}$ are defined in the same way as in the previous section. In addition to these, hash functions $H' : \{0,1\}^* \to Z_q^*$, $H'' : Z_q^* \to \{0,1\}^*$, and $H_1 : G_2 \to \{0,1\}^*$ are required.

When *A* wishes to send an authenticated encrypted message for *B*, *A* obtains its public and private key pair (Q_A , S_A) from the key generation centre by sending its identity. Similarly, when *B* wishes to unsigncrypt the signcrypted message sent from *A*, it obtains its public and private key pair (Q_B , S_B) from the KGC.

Signcryption

A knows the values (Q_A, Q_B, S_A, *M*) and hence signcrypts the message *M* using *B*'s public key Q_B and *A*'s private key S_A.

To signcrypt a message $M \in \{0,1\}^*$, the user *A*

chooses a random $a \in Z_q^*$, and computes the following:

- $R = a.S_A$, $R' = (R \| H_1(\hat{e}(Q_B, S_A)) \| M)$ and
- $S = a.H'(R')Q_A = a.H'(R \| H_1(\hat{e}(Q_B, S_A)) \| M)Q_A$.
- $k_A = H''(\hat{e}(Q_B, S_A)^{aH'(R')})$

- $C = k_A \oplus M$

A sends the signcrypted message (R, S, C) to *B*

Unsigncryption

B knows the values (R, S, C, Q_A, Q_B, S_B) and hence unsigncrypts the message using his private key S_B.

- $k_B = H''(\hat{e}(S_B, S))$
- $M = k_B \oplus C$

Consistency

$$k_B = H''(\hat{e}(S_B, S)) = H''(\hat{e}(S_B, a.[H'(R')]Q_A))$$
$$= H''(\hat{e}(Q_B, S_A)^{a.H'(R \| H_1(\hat{e}(Q_B, S_A)) \| M)}) = k_A$$

Verification

To verify if the message *M* has reached properly, *B* computes $H'(R \| H_1(\hat{e}(S_B, Q_A)) \| M)$, and accepts the signature only if $\hat{e}(S_B, S) = \hat{e}(Q_B, R)^{H'(R \| H_1(\hat{e}(S_B, Q_A)) \| M)}$, rejects otherwise. This verifies any message tampering on route since

$$\hat{e}(Q_B, R)^{H'(R \| H_1(\hat{e}(S_B, Q_A)) \| M)} = \hat{e}(Q_B, a.S_A)^{H'(R \| H_1(\hat{e}(S_B, Q_A)) \| M)}$$

$$= \hat{e}(Q_B, S_A)^{a.H'(R \| H_1(\hat{e}(S_B, Q_A)) \| M)} = \hat{e}(S_B, a.H'(R \| H_1(\hat{e}(Q_B, S_A)) \| M) Q_A)$$
$$= \hat{e}(S_B, S)$$

If the message were tampered en route, then this verification would detect the change. The signcryption is a valid one if both are equal, and it is rejected if they are not equal since it implies that the message has not reached *B* properly.

In this scheme, the key k_A is computed by *A* using the public key of *B*, Q_B, private key of *A*, S_A, and the message *M*. The key k_A is used to encrypt the message *M*.

Checking for the number of computations, it can be observed that during signcryption and unsigncryption, the pairings to be computed ($\hat{e}(Q_B, S_A)$), and ($\hat{e}(S_B, Q_A)$) can be precomputed. Thus, the total computations during the execution of the scheme (considering the expensive ones) constitute 4 Weil pairings (of which two can be precomputed), 2 point multiplications, and 2 exponentiations. Since computation of a pairing is much more expensive than an exponentiation, it can be concluded that the new ID-based signcryption scheme is an improved version of the existing scheme [10]. These computations are shown in a tabular form in section 7. The security properties of the new signcryption scheme are discussed in the next section.

6. Security

The new ID-based signcryption scheme satisfies all the properties required for an authenticated encryption. It provides confidentiality, authentication, forward secrecy, and non-repudiation.

- *Confidentiality* is achieved by encryption
- *Authenticity* is guaranteed by having the signature since the sender uses his/her private key to signcrypt.

- Key escrow is inherent in ID-based systems since the KGC knows the long term private keys of all the users in the group (since secret key $S_{ID} = [s]Q_{ID}$, and s is the secret key of KGC). Thus *non-repudiation* is possible in the new scheme.
- To check whether the scheme is *forward secure*, suppose that the long term private key of A, S_A is compromised. Now, if an adversary knows the values (R, S, C) of an earlier session along with S_A , and tries to get back the message, he has to compute $k_A = H''(\hat{e}(Q_B, S_A)^{a.H'(R\|H_1(Q_B,S_A)\|M)})$. But 'M' and 'a' are not known to compute this key. Also $H'(R \| H_1(Q_B, S_A) \| M)$ cannot be computed from the given (R, S, C) and S_A. Thus it is proved that the new scheme is forward secure.

7. Computations and Efficiency

The computations in each of the schemes are compared in the following table. The number of computations for the signature-then-encryption method using Boneh-Franklin ID-based encryption scheme [4] and Hess's signature scheme [5], and the comparison of the computations of the existing ID-based signcryption scheme by Malone-Lee and the new improved ID-based signcryption scheme are illustrated in the table. Hess's signature scheme is chosen since it is shown in [5] that computations in Hess's signature are less compared to the signature schemes in [8], [12] and [14]

Scheme	Algorithm	Weil Pairing	Point Multiplication	Exponentiation
Computations in BF-IBE, and ID-based signature scheme (signature-then-encryption)	Encrypt	1 (can be precomputed)	1	1
	Decrypt	1	0	0
	Sign	1 (can be precomputed)	1	1
	Verify	2 (1 can be precomputed)	0	1
	Total computations	5 (3 can be precomputed)	2	3
IDSC ID-based signcryption by Malone Lee	Signcryption	1 (can be precomputed)	3	0
	Unsigncryption (and verification)	4 (1 can be precomputed)	0	1
	Total computations	5 (2 can be precomputed)	3	1
The new ID-based signcryption scheme	Signcryption	1 (can be precomputed)	2	1
	Unsigncryption (and verification)	3 (1 can be precomputed)	0	1
	Total computations	4 (2 can be precomputed)	2	2

Table 1 : Comparison of computations in signature-then-encryption, ID-based signcryption by Malone-Lee, and the new signcryption scheme

If the operations listed above are regarded as the expensive ones in the generation and validation of cipher texts, it can be seen from the table that the total computations required for the new ID-based signcryption scheme are less than the computations required for ID-based signature-then-encryption scheme. Also, it can be observed that the number of Weil pairings to be computed in the new scheme is less than the number in Malone-Lee's signcryption scheme. Thus, it can be concluded that the new scheme is an improved version of the existing signcryption scheme.

8. Conclusions and future work

A new ID-based cryptographic scheme called the ID-based signcryption scheme has been proposed for authenticated and secure message delivery. This has been proposed as an efficient alternative to the traditional signature-then-encryption method. The scheme is compared to the existing ID-based signcryption scheme by Malone-Lee [10] and is found to be computationally efficient. The new scheme provides confidentiality, authenticity, non-repudiation, and forward secrecy. Heuristic arguments have been provided for these security properties. The formal security proofs for this scheme are being worked out presently. Future work involves proposing new schemes more efficient than the current one. Identity-based group signatures is another aspect to be worked on.

References

1. A. Fiat and A. Shamir, *How to proveyourself: Practical solutions to identification and signature problems*. Proceedings of Crypto'86, LNCS, Vol.263, pp.186-194, Springer-Verlag, 1987.
2. A. Shamir, *Identity based cryptosystems and signature schemes*. Advances in Cryptology – Proceedings of Crypto'84.
3. C. Cocks. *An Identity based encryption scheme based on quadratic residues*. Cryptography and Coding, 2001.
4. D. Boneh and M. Franklin. *Identity-based encryption from the Weil Pairing*. In Advances in Cryptology – CRYPTO 2001, Springer-Verlag LNCS 2139, 213-229, 2001.
5. F. Hess. *Efficient Identity based signature schemes based on pairings*. Proceedings of 9th workshop on selected areas in Cryptography – SAC 2002, Lecture notes in Computer Science, Springer-Verlag.
6. F. Hess. *Exponent group signature schemes and efficient Identity-based signature schemes based on pairings*. Cryptology eprint archive, Report 2002/012, available at http://eprint.iacr.org/
7. Hee Yun Jung, Dong Hoon Lee, Jongin Lim, and Ki Sik Chang, *Signcryption Schemes with Forward Secrecy* , *WISA 2001*, Vol.2, pp. 403-475, 2001.
8. J. C. Cha and J. H. Cheon. *An Identity-based signature from Gap Diffie-Hellman groups*. Cryptology ePrint Archive, Report 2002/018, http://eprint.iaccr.org/.
9. J. H. An, Y. Dodis, and T. Rabin. *On the security of joint signature and encryption*. In Advances in Cryptology – EUROCRYPT 2002, volume 2332 of LNCS, pp 83-107, Springer-verlag, 2002.
10. J. Malone-Lee. *Identity-based signcryption*. Cryptology ePrint Archive, Report 2002/098, 2002, http://eprint.iacr.org/
11. J. Malonee-Lee, *Signcryption with Non-Repudiation*, Technical Report CSTR-02-004, Department of Computer Science, University of Bristol, June 2002.

12. K.G.Paterson. *ID-based signatures from pairings on elliptic curves*. Cryptology eprint archive, Report 2002/004, available at http://eprint.iacr.org/
13. N.P. Smart. *An Identity based authenticated Key Agreement protocol based on the Weil Pairing*. Cryptology ePrint Archive, Report 2001/111, 2001. http://eprint.iacr.org/.
14. R. Sakai, K. Ohgishi, and M. Kasahara. *Cryptosystems based on pairings*. In SCIS 2000, 2000.
15. U. Feige, A. Fiat, and A. Shamir, *Zero-knowledge proofs of identity*. Journal of Cryptology, vol.1, pp. 77-94, 1988.
16. Y. Zheng, *Digital Signcryption or how to achieve cost(signature&encryption) << cost(signature)+cost(encryption)*. In Advances in Cryptology, CRYPTO'97, Volume 1294 of LNCS, pages 165-179, Springer-Verlag, 1997.

Appendix A. ID-PKC versus PKI

Some of the following issues can be addressed to compare the ID-based systems with the traditional PKI supported public-key cryptography [12].

Authenticity of system parameters: Any user involved in the identity-based scheme has access to authentic values for the system parameters. The situation where these parameters may be compromised, is similar to the need for authenticity of a root certificate in a PKI.

Secure delivery of private keys: A secure channel is required to deliver the private keys to the correct users in an identity-based scheme, whereas in traditional PKI, the private key is known only to the user. This leads to the key escrow property in ID-based systems. Key escrow can be avoided by having multiple trust authorities. Since a single authority for key generation may present an obvious point of compromise or system failure, and it can masquerade as any given entity, it is split into two or more cooperating parties. The authorities perform a one-time set-up in order to share the system secrets in a secure manner. The user proves itself to each authority. Each authority then returns its part of the private key. The user combines these parts to obtain his private key. This provides more security as the private key remains split until use. We can also have n-authorities in the system wherein no n-1 of them can generate a key or compromise the system.

Revocation: In a PKI-based system, Certificate Revocation lists, or online certificate status checking can be used for revocation of public keys. A key may be revoked if it is compromised or if a certificate expires. This would be a problem in case of identity-based systems since the compromise of the key would not allow to get a new key, as the key is dependent on the identity of the user. One solution to this problem is to concatenate identities with expiry times in identity-based systems.

Key management and scalability: The KGC is a single point of failure in an ID-based system. If the private key of the KGC is compromised, the security of the entire scheme is lost. This is also true in case of PKI-based systems, where management of CA root keys is required.

The major advantage of traditional PKI over ID-PKC is that PKI is a well established technology, with many vendors, many deployed systems, and many standards in place. ID-based PKI has simple procedure of managing public key list, it has advantages such as automatic key escrow/recovery [4]. Also when the whole ID-based scheme is used by one user, it can be applied for delegation of duties on encryption.