An Efficient Signcryption Scheme Based on ECC with Public Verification and Forward Secrecy

Prof. Sumanjit Das

Dept. of Computer Science & Engineering
School of Engineering, Bhubaneswar,
Centurion University of Technology and Management

Er.Sangram Keshari Swain

Dept. of Computer Science & Engineering School of Engineering, Bhubaneswar,
Centurion University of Technology and Management

Er. Prasant Kumar Sahoo

Dept. of Computer Science & Engineering,
Subas Institute of Technology, Bhubaneswar

Abstract

Information is an asset that has a value. As an asset, information needs to be secured from attacks. Security becomes a challenge all field of communication. While sending a message to a person over an unreliable channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation [1]. These are the four major security aspects [2] or goals. Cryptography was concerned only with message confidentiality (i.e., encryption). In this paper an efficient signcryption scheme based on elliptic curve cryptosystem is proposed which can effectively combine the functionalities of digital signature and encryption and also take a comparable amount of computational cost and communication overhead. It provides confidentiality, authentication, integrity, unforgeability and non repudiation, along with forward secrecy of message confidentiality and public verification.

Keywords

Signcryption, Public key cryptography, Elliptic curve cryptography, Digital signature, Forward secrecy, Encrypted Message Authentication.

Introduction

Information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks. Now-a-days security becomes an essential feature in almost all area of communication. While sending a message to a person over an insecure channel such as internet we must provide confidentiality, integrity, authenticity and non-repudiation [1]. These are the four major security aspects [2] or goals. Before the modern era, cryptography was concerned solely with message confidentiality (i.e., encryption) conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). Encryption was used to (attempt to) ensure secrecy in communications, such as those of spies, military leaders, and diplomats. In recent decades, the field has expanded beyond confidentiality concerns to include techniques for message integrity checking, sender/receiver identity authentication, digital signatures, and interactive proofs and secure computation, among others. In ancient times, the use of cryptography was restricted to a small community essentially forms by the military and secret services. The keys were distributed secretly by a courier and the same key is used to encipher and decipher the message. We have a number of encryption algorithms those can be broadly classified into two categories: *Symmetric/Private key encipherment* and *Asymmetric/Public key encipherment* [3, 4].

In order to send a confidential letter in a way that it can't be forged, it has been a common practice for the sender of the letter to be sign it, put it in an envelope and then seal it before handing it over to be delivered. Discovering public key cryptography has made communication between people who have never met before over an open and insecure network such as Internet [10], in a secure

and authenticated way possible. Before sending a message the sender has to do the following:

1. Sign it using a digital signature scheme (DSS).
2. Encrypt the message and the signature using a private key encryption algorithm under randomly chosen encryption key.
3. Encrypt the random message encryption key using receiver's public key.
4. Send the message following steps 1 to 3.

This approach is known as "*Signature-Then-Encryption* ". It can be shown in the following Figure 1.4. This figure has been taken from [15].

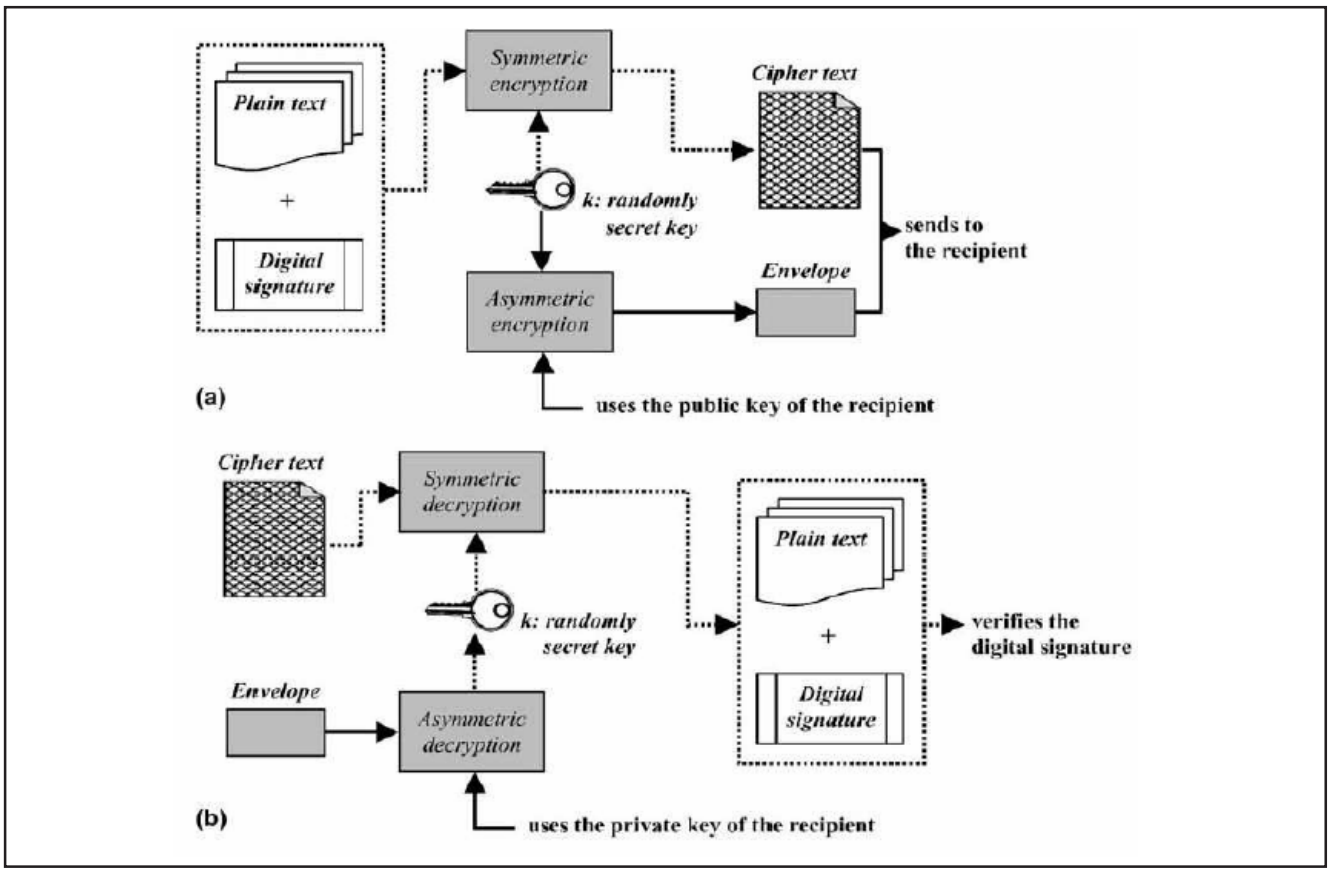

Figure 1.4: (a) Signature-Then-Encryption (b) Decryption-Then-Verification

1.2 Signcryption

Of the many goals which the study of cryptography sets out to achieve, the most important and widely studied are confidentiality and authenticity. Traditionally, these two goals have been studied separately. In the case of public-key cryptography, confidentiality is provided by encryption schemes, while authenticity is provided by signature schemes. In many applications, both confidentiality and authenticity are needed together. Such applications include secure email (S/MIME), secure shell (SSH), and secure web browsing (HTTPS). Until recently, the de facto solution was to use both an encryption scheme and a signature scheme, typically by sequentially composing the encryption and signature operations. This state of affairs changed in 1997, when Zheng [15] proposed using a single cryptographic primitive to achieve both confidentiality and authenticity. He called this primitive signcryption. At first glance, it is not clear why there should be any advantage to lumping both goals into a single primitive. However, Zheng and others have demonstrated, through concrete examples, that signcryption schemes can provide clear benefits over the traditional sequential composition of encryption and signature schemes.

3. Related Work:

The history of cryptography defines the level of developments on it. But it's not for the use of common purpose. Now a days it developed in many terms like signcryption which is the most authentic one in the world of security. Many researchers given their proposal for signcryption based on modular exponential and some are based on elliptic curves. Y.Zheg [1] proposed signryption scheme which saves 58% computational cost and saving about 40% communication cost than the traditional signature-then-encryption scheme. This scheme was based on discrete logarithmic problem (DLP) and it involves modular exponential. Then Zheng and Imai proposed another signcryption scheme based on elliptic curves discrete logarithm problem (ECDLP) that achieved similar functionality [2]. Both the schemes lacked forward secrecy, public verifiability and encrypted message authentication. Gamage-Leiwo-Zheng scheme was based on DLP signcryption and lacked forward secrecy. Bao and Deng proposed a signcryption scheme based on DLP. It lacked forward secrecy and encrypted message authentication. CHEN Wen and Kefei modified Zheng and Bao-Deng scheme to add public verifiability property [6]. Their scheme was based on DLP but lacked forward secrecy and encrypted message authentication.

3.2 Zheng-Imai Signcryption scheme Based on Elliptic curve:

Zheng –Imai proposed two schemes based on elliptic curve named ECSCS1 & ECSCS2 [2]. Only ECSCS1 is described here the case is similar for the other. Alic was the sender having message m send to Bob. Before sending the message Alic signcrypts m as follows so that the effect to signature then encryption.

Public Parameter:

C: an elliptic curve of GF (ph), either with pe"2 150 and h=1 or p=2 and & he"150.

q: a large prime number whose size is approximately |ph|.

G: a point with order q, chosen randomly from the points on C.

hash: a one-way hash function output of 128 bits at least.

KH: a keyed one-way hash function.

ED: the encryption and decryption algorithm of a private key cipher.

Alice's key:

Va: Alice's private key, chosen uniformly at random from [1,….q-1].

Pa: Alice's public key (Pa=VaG, a point on C).

Bob's Key:

Vb: Bob's private key, chosen uniformly at random from [1,….q-1].

Pb: Bob's public key (Pb=VbG, a point on C).

Signcryption of m by Alice:

Step-1: v å r [1,……q-1].

Step-2: (k1, k2) = hash (vPb).

Step-3: c=Ek1 (m).

Step-4: r= KHk2 (m).

Step-5: s= v/(r+Va) mod q.

Send c, r, s to Bob

Unsigncryption of c, r, s by Bob:

Step-1: u= sVb mod q.

Step-2: (k1, k2) = hash (uPa+urG).

Step-3: m= Dk1(c).

Accept m only if KHk2 (m) = r.

The disadvantage of the above scheme is that it doesn't support forward secrecy and encrypted message authentication. From the above Zheng and Imai scheme we can see that if *Alice* divulged his private key *va* inattentively then an adversary can get the information about the past messages.

4. The proposed Scheme

4.1 The proposed signcryption scheme with public verification and forward secrecy

The proposed signcryption scheme was based on elliptic curve cryptosystem. In this thesis the scheme provides all the basic features of security functions such as message integrity, message confidentiality, non-repudiation, sender's authenticity, encrypted message authenticity, forward secrecy and public verification, with a cost less than or comparable with the existing schemes.

4.1.1 Algorithm for proposed scheme:

The proposed scheme consists of three phases like Initialization, Signcryption, and Unsigncryption. Each user should get the certification of his public key from the certificate authority (CA). The Alice and Bob are uniquely identified by their unique identifiers IDA and IDB. The new scheme has the same public parameters and the same key for Alice and Bob as Zheng-Imai. It works as follows.

Initialization phase:

In this phase, some public parameters are generated. The steps are as follows:

q: a large prime number, where q is greater than 2^{160} .

V_a: Alice's private key, chosen uniformly at random from 1 to q-1.

P_a: Alice's public key, where $P_a=V_aG$, a point on C.

V_b: Bob's private key, chosen uniformly at random from 1 to q-1.

Pb: Bob's public key, where $P_b=V_bG$ a point on C.

Signcryption of m by Alice:

Assume that Alice want to send a message m to Bob. Alice generate the digital signature (R,s) of message m and uses the symmetric encryption algorithm and a secret key k for encrypt of m. c will the cipher text. Alice generate the signcrypted text (c,R,s) as follows:

Step 1: Verify Bob's public key P_b by using his certificate.

Step 2: Select v å r [1,… q-1].

Step 3: Compute k_1=hash (vP_b).

Step 4: compute k_2= hash (vG)

Step 5: Uses encryption algorithm to generate cipher text

$$\mathbf{c= Ek_1 (m)}$$

Where key k1 generated in step 3.

Step 6: Uses the one-way hash function to generate

$$\mathbf{r = hash(c||k_2||ID_A||ID_B)}$$

Where IDA and IDB are identification given by certificate authority (CA).

Step 7: computes s = v/(r + v_a) mod q.

Step 8: compute R = rG.

Step 9: Send signcrypted text (c, R, s) to Bob.

Unsigncryption of c, R, s by Bob:

Bob receives the signcrypted text (c, R, s). He decrypts cipher text 'c' by performing decryption algorithm with secret key k. He also verifies the signature. Bob gets the plain text as follows.

Step 1: Verifies Alice's public key P_a by using her certificate.

Step 2: Computes K_2 = hash(s(R + P_a)).

Step 3: computes K_1 = hash(V_bs(R+P_a)).

Step 4: Uses one way keyed hash function to generate

$$\mathbf{r = hash\ (c||k_2||ID_A\ ||ID_B)}$$

where ID_A & ID_B are the identifications given by the certificate authority(CA).

Step 5: Uses decryption algorithm to generate plain text

$$\mathbf{m = Dk_1\ (c)}$$

where the secret key k1 is computed in step 3.

Step 6: Bob accepts the c only if rG = R. otherwise he rejects.

Verification of c, R, s by a firewall or judge:

K_2 = hash (s(R + P_a))

r = hash (c, k_2)

Accept c only if **rG = R**

4.2 Analysis

4.2.1 Proof

To prove the verification condition:

$sR + sP_a = vrG / (r + v_a)$

$= (vrG + vP_a) / (r + v_a)$

$= vG (r + v_a) / (r + v_a)$

$= vG$

There fore hash ($sR + sP_a$) = hash (vG) = hash (k_2).

Computing k_2 allows the verification of the signcrypted text.

To prove the decryption step:

$Svb(R + p_a) = v_b(sR + sP_a)$

$= v_b\ vG$

$= vP_b$

Thus hash ($sv_b(R + P_a)$) = hash (vP_b) = hash (k_1)

Computing k1 allows the decryption of the message using m = Dk_1(c).

4.2.2 Security properties of proposed scheme:

Table 4.1 indicates the security features supported by existing signcryption schemes along with the proposed schemes. The proof is based on the fact that it is almost intractable to solve the elliptic curve discrete logarithmic problem (ECDLP) [8, 13].

Table 4.1: Comparisons based on securities properties [13]

	Confidentiality	Integrity	Unforgeability	Forward Security	Public verification
Zheng	Yes	Yes	Yes	No	No
Zheng and Imai	Yes	Yes	Yes	No	No
Bao & Deng	Yes	Yes	Yes	No	Yes
Gamage et al	Yes	Yes	Yes	No	Yes
Jung et al.2001	Yes	Yes	Yes	Yes	No
Han et al.2004	No	No	No	No	Yes
Hwang et al.2005	No	No	No	No	Yes
Proposed scheme	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Confidentiality:

Confidentiality is achieved by encryption. To decrypt the cipher text(c), an adversary needs to have Bob's **private key (v_b).**which is the secret key of Bob and he will never disclose it. Therefore it is unknown to third party.

Unforgeability:

It is computationally infeasible to forge a valid signcrypted text (*c*, *R*, *s*) and claim that it is coming from Alice without having Alice's private key v_a. The private key of Alice is unknown to third party. The computation process of R and s is very difficult and infeasible to guess the solution of signcryption text.

Non-repudiation:

If the sender Alice denies that she sent the signcrypted text (*c*, *R*, *s*), any third party can run the verification procedure above to check that the message came from Alice.

Public verifiability:

Verification requires knowing only Alice's public key. All public keys are assumed to be available to all system users through a certification authority or published directly. The receiver of the message does not need to engage in a zero-knowledge proof communication with a judge or to provide a proof. If we have the public key of Alice Pa then only we can compute K2 as follows:

K_2 = hash (s(R + P_a))

After finding the value of K2 we can compute r as

r = hash (c, K_2)

Now we can satisfy the condition for acceptance of c i.e rG = R. Hence it's coming from Alice as it satisfy the condition with help of Alice's public key (P_a).

Forward secrecy:

An adversary that obtains v_a will not be able to decrypt past messages. Previously recorded values of (*c*, *R*, *s*) that were obtained before the compromise cannot be decrypted because the adversary that has v_a will need to calculate *r* to decrypt. Calculating *r* requires solving the ECDLP on *R*, which is a computationally difficult.

Where r = hash(c,K_2) and rG = R which make it infeasible to solve also the value of s= v/(r + V_a)mod q depends on private key of Alice and the value of r.

Encrypted message authentication:

The proposed scheme enables a third party to check the authenticity of the signcrypted text (*c*, *R*, *s*) without

having to reveal the plaintext *m* to the third party. This property enables firewalls on computer networks to filter traffic and forward encrypted messages coming from certain senders without decrypting the message. This provides speed to the filtering process as the firewalls do not need to do full unsigncryption to authenticate senders. It also provides additional confidentiality in settling disputes by allowing any trusted/untrusted judge to verify messages without revealing the sent message *m* to the judge by running verification process as follows.

K_2 = hash (s(R + P_a))

r = hash (c, k_2)

Accept c only if **rG = R**

As the signcrypted text computed by the help of Alice's public key P_a and the ID_A can be verify by certificate Authority (CA). There fore we can say the message is coming from Alice without decrypting the original message and which is authentic sender.

4.2.3 Computational Complexity:

Elliptic curve point operations are time consuming process. The propose signcryption scheme is having three point multiplication for signcryption, two point multiplication for unsigncryption and one point addition, for verification it requires one point multiplication and one point addition. The table 4.2 gives the details of comparison with the existing schemes and proposed scheme. [13]

Table 4.2: comparison of schemes on basis of computational complexity

Schemes	Participant	ECPM	ECPA	Mod. Mul	Mod. Add	Hash
Zheng & Imai	Alice	1	-	1	1	2
	Bob	2	1	2	-	2
Han et al	Alice	2	-	2	1	2
	Bob	3	1	2	-	2
Hwang et al	Alice	2	-	1	1	1
	Bob	3	1	-	-	1
Proposed scheme	**Alice**	**2**	**1**	**-**	**-**	**2**
	Bob	**3**	**-**	**1**	**1**	**2**
Schemes	**Participant**	**Mod. Exp**	**Mod.div**	**Mod. Mul**	**Mod. Add**	**Hash**
Zheng	Alice	1	1	-	1	2
	Bob	2	-	2	-	2
Jung el	Alice	2	1	-	1	2
	Bob	3	-	1	-	2
Bao & Deng	Alice	2	1	-	1	3
	Bob	3	-	1	-	3
Gamage et al	Alice	2	1	-	1	2
	Bob	3	-	1	-	2

Table 4.3: comparison based on average computational time of major operation in same secure level the elliptic curve multiplication only needs 83ms & the modular exponential operation takes 220 ms for average computational time in infineon's SLE66CU* 640P security controller.[15]

Schemes	Sender average. computational time in ms	Recipient average computational time in ms
Zheng	1 * 220 = 220	2*220 = 440
Zheng & Imai	1* 83=83	2*83=166
Bao & Deng	2*220=440	3*220=660
Gamage et al	2*220=440	3*220=660
Jung et al	2*220=440	3*220=660
Proposed scheme	**2*83=249**	**3*83=166**

5. Lesson learned

Although Zheng originally set out to achieve greater efficiency by combining encryption and signature schemes, the focus has subsequently shifted to other issues, such as security and non-repudiation. The issue of security is of key importance, since it has implications for all systems which use encryption and signatures together. This thesis introduces elliptic curve based signcryption schemes for secure and authenticated message delivery, which fulfills all the functions of digital signature and encryption with a cost less than that required by the current standard signature-then-encryption method. The Zheng and Imai scheme is the most efficient signcryption scheme based on ECC. But the drawback of the above scheme is that it does not provide forward secrecy. So it is necessary to provide forward secrecy. There are few schemes which can provide forward secrecy but the computational cost and

communication overhead is more. The cost of the proposed schemes are comparatively lower than other schemes in terms of computational and communication overhead. ECC has been used for the implementation of our algorithm because of its unique property of ECDLP which is significantly more difficult than either the IFP or DLP. Proposed schemes save more computational cost for the sender to suit the application of limited computing power like smart card based applications, mobile devices, etc.

5.2 Direction for future work

Another area worthy of exploration is the use of the signcryption primitive in cryptographic protocols. The signcryption primitive is a powerful abstraction, since it encompasses not only confidentiality and authenticity, but also user identities (via its multi-user security definition). This has allowed for the construction of a very simple authenticated key-exchange protocol. Undoubtedly there are other protocols which could be similarly simplified using signcryption.

In 1988 Koblitz [12] suggested to use the generalization of Elliptic Curves (EC) for cryptography, the so-called Hyperelliptic Curves (HEC). While ECC applications are highly developed in practice, the use of HEC is still of pure academic interest. However, one advantage of HECC [12] resides on the fact that the operand size for HECC is at least a factor of two smaller than the one of ECC. More precisely, while typical bit-lengths for ECC are at least 160 bits, for HECC this lower bound is around 80 bits (in the case of genus 2 curves). This fact makes HECC a very good choice for platforms with limited resources. Now we should look forward to develop schemes based on HECC which is an open challenge for us.

Reference:

1. Yuliang Zheng. Digital signcryption or how to achieve cost (signature encryption)

   Cost (signature), Cost (encryption). In *CRYPTO '97:* Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 165-179, London, UK, 1997. Springer-Verlag.
2. William Stallings. *Cryptography and Network security: Principles and Practices*. Prentice Hall Inc., second edition, 1999.
3. Paul C. van Oorschot Alfred J. Menezes and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press,1996.
4. Behrouz A. Forouzan. Cryptography and Network Security. Tata McGraw-Hill, 2007.
5. F.Bao, R.H. Deng, "A signcryption scheme with signature directly verifiable by public key", Proceedings of PKC'98, LNCS 1431, Springer-Verlag, 1998, pp. 55–59.
6. LEI Feiyu, CHEN Wen, CHEN Kefei, "A generic solution to realize public verifiability of signcryption", Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.
7. Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve. *Computer and Electrical Engineering, International Conference on*, 428-432, 2008.
8. Yuliang Zheng and Hideki Imai. How to construct efficient signcryption schemes on elliptic curves. *Inf. Process. Lett.*, 68(5):227-233, 1998.
9. Jung.H.Y,K.S Chang, D.H Lee and J.I. Lim, Signcryption scheme with forward secrecy. Proceeding of Information Security Application-WISA, Korea, 403-475, 2001.
10. Gamage, C., J.Leiwo, Encrypted message authentication by firewalls. Proceedings of International Workshop on Practice of Theory in Public Key Cryptography, Berlin, 69-81, 1999.
11. X. Yang Y. Han and Y. Hu. Signcryption based on elliptic curve and its multi-party schemes. Proceedings of the 3rd ACM International Conference on Information Security (InfoSecu 04), pages 216-217, 2004.
12. Henri Cohen and Gerhard Frey, editors. Handbook of elliptic and hyperelliptic curve cryptography. CRC Press, 2005.
13. Mohsen Toorani and Ali Asghar Beheshti Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. *Journal of Applied Sciences*, 9(6):1025 -1035, 2009.
14. G. Seroussi. Elliptic curve cryptography. page 41, 1999.
15. Hwang Lai Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. Journal of applied mathematics and computation, pages 870-881, 2005.
16. Mohsen Toorani and Ali Asghar Beheshti Shirazi. Cryptanalysis of an elliptic curve-based signcryption scheme. International journal of network security vol.10, pp 51-56,2010.
17. Wang Yang and Zhang. Provable secure generalized signcryption. Journal of computers, vol.5, pp 807-814, 2010.