A Modified Signcryption Scheme using Elliptic Curve Cryptography

Anuj Kumar Singh

Department of Computer Sciene & Engineering Amity University Haryana Gurgaon, India

Abstract— In this paper, an efficient signcryption scheme based on elliptic curve cryptosystem is going to be proposed which can effectively combine the functionalities of digital signature and encryption and also takes a comparable amount of computational cost and communication overhead. The proposed scheme provides confidentiality, integrity, unforgeability and nonrepudiation, along with encrypted message authentication, forward secrecy of message confidentiality and encrypted message authentication. By forward secrecy of message confidentiality function we mean, although the private key of the sender is divulged inattentively, it does not affect the confidentiality of the previously stored messages. In addition, proposed scheme will save great amount of computational cost but at the same time an interactive zero knowledge proof is required. In the proposed scheme the number of ECPM (Elliptic Curve point Multiplication) operations are minimized which is the most costly operation in ECC (Elliptic Curve Cryptography). The proposed scheme can be applied to the lower computational power devices, like smart card based applications, e-voting and many more, due to their lower computational cost. The Proposed Scheme is discussed in this paper and is compared with the existing schemes with respect to computational cost and the security functions it provides.

Keywords- Public key cryptography, Elliptic curve cryptography, Digital Signature., Signcryption.

I. INTRODUCTION

The encryption and digital signature are two fundamental cryptographic mechanisms that can provide the security of communications. Until the before decade, they have been viewed as important but distinct building blocks of various cryptographic systems. In the public key schemes, a traditional method is to digitally sign a message then followed by an encryption (signature-then-encryption) that can have two problems: Low efficiency and high cost of such summation, and the case that any arbitrary scheme cannot guarantee the security. The signcryption is a relatively new cryptographic technique that is supposed to fulfill the functionalities of digital signature and encryption in a single logical step. It effectively decreases the computational costs and communication overheads in comparison with the traditional signature-then-encryption schemes. The word signcryption was first introduced by Yuliang Zheng [1] in the year 1997.

II. LITERATURE REVIEW

Y.Zheng [1] proposed signcryption scheme which saves about 50% computational cost and about 85% communication cost than the traditional signature-then-encryption scheme. This scheme was based on discrete logarithmic problem. It involves modular exponentiation. Bao and Deng [2] enhanced Zheng's signcryption scheme such that the judge can verify signature without the recipient's private key. But a key exchange protocol is required in the process of verification. Then Zheng and Imai [4] suggested an ECC based signcryption scheme thus providing all the basic security features, with cost less than as required by “signature-then-encryption” which saves about 58% computational cost and saving about 40% communication cost than signature-then-encryption. They choose ECC because elliptic curve based solutions are usually based on the difficulty of ECDLP which is discussed in the next Chapter. As it is based on elliptic curve cryptosystem the key size used is smaller as compare to the other schemes, which is one of the advantages of this scheme but still it needs forward secrecy. Gamage et al. [3] modified Zheng's [1] signcryption scheme so that anyone can verify the signature of cipher text (encrypted message authentication). Their scheme only verifies the cipher text to protect confidentiality of message in firewall application. After that, Jung et al. showed that Zheng's [1] scheme does not provide forward secrecy of message confidentiality when the sender's private key disclosed. They also proposed a new signcryption based on discrete logarithm problem (DLP) with forward secrecy. In Jung's scheme [5], even attacker obtains the sender's private key, he cannot get the corresponding original message yet that sender had sent. However, in those research results, when dispute occurs, the judge cannot directly verify the signature because of not knowing the recipient's private key. Hwang et. al [5]showed that Jung’s scheme does not provide Public Verifiability and proposed an efficient signcryption scheme based on elliptic curve with forward secrecy and publicly verifiable. The proposed signcryption scheme with forward secrecy satisfies the message confidentiality of previous encrypted message even if the sender divulged his private key inattentively with a cost comparable to the existing schemes. After all these schemes Mohsen Toorani and Ali Asghar [6] proposed a signcryption scheme based on elliptic curve which provide all the security attributes. But this scheme takes more computational cost as compared to existing schemes. The signcryption scheme involve with 2 elliptic curve point multiplication in the signcryption phase and 4 elliptic curve point multiplication in the unsigncryption phase.

So finally it has been observed that out of all signcryption schemes stated above some signcryption schemes support all major security goals while some takes a considerable amount of computational and communication overhead. But some of these schemes do not support encrypted message authentication, forward secrecy and public verification. So our objective is to propose a new efficient scheme such that it will take a comparable computational and communication cost and should provide encrypted message authentication, forward secrecy and public verification.

III. THE PROPOSED SCHEME

Throughout this paper, Alice is the sender, Bob is the recipient. The proposed scheme spends lower time in computation, especially for receiver. It contains four phases: initialization phase, signcryption phase, unsigncryption phase and judge verification phase.

The initialization phase includes selecting the domain parameters, generating the private/public keys, and getting a certificate for the public key of each user. In signcryption phase, Alice signcrypts her message and sends it to Bob. In unsigncryption phase, Bob performs the unsigncryption to recover the signcrypted text and verify the signature. The judge verification phase is used only when any dispute occurs in which the judge decides whether Alice has sent the signcrypted message to Bob or not.

A. Initialization Phase

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

q:A large prime number, where $q > 2^{160}$ [15].

a, b: Two integer elements which are smaller than q and satisfy the following condition

$4a^3 + 27b^2 \mod q \neq 0$.

F: The selected elliptic curve over finite field q

$y^2 = x^3 + ax + b \mod q$.

G: A base point of elliptic curve F with order n.

O: A point of F at infinite.

n : The order of point G, where n is a prime, $n \times G = O$ and $n \geq 2^{160}$. (The symbol " X " denotes the elliptic curve point multiplication,).

H : A one-way hash function,

$E_k() / D_k()$: Symmetric encryption/decryption algorithm with private key k such as DES or AES.

The sender Alice randomly selects an integer v_a as her private key and $v_a \leq n-1$. She computes her public key $P_a = v_aG$. The recipient Bob also selects private key v_b and public key $P_b = v_bG$ by the same way as Alice. They need to get a certificate of their public key from the certificate authority (CA).

B. Signcryption Phase

Assume that Alice wants to send a message m to Bob. Alice generates digital signature (T, s) of message m and uses the symmetric encryption algorithm and secret key k to encrypt m. Let c be the cipher text. Alice generates the signcrypted text (c, T, s) in the following steps.

Step 1: Verifies Bob's public key Pb by using his certificate.

Step 2: Randomly selects an integer v, where $v \leq n - 1$.

Step 3: Computes (k1, k2) = hash(vPb).

Step 4: Uses the symmetric encryption algorithm to generate cipher text:

$c = E_{k1}(m)$

where the secret k1 is generated in Step 3.

Step 5: Uses the one-way keyed hash function to generate:

$r = KH_{k2}(c \parallel ID_A \parallel ID_B)$

where ID_A and ID_B are the identifications given by the certification authority(CA).

Step 6: Computes $s = (v - r)/v_a \mod q$

Step 7: Compute T = rG.

Step 8: Sends the signcrypted text (c, T, s) to Bob.

C. Unsigncryption Phase

Bob receives the signcrypted text (c, T, s). He decrypts cipher text 'c' by performing symmetric 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 Pa by using her certificate.

Step 2: Computes (k1,k2) = hash(vbT + vbsPa).

Step 3: Uses one way keyed hash function to generate:

r = KH_{k2} (c || ID_A || ID_B)

where ID_A and ID_B are the identifications given by the certification authority(CA).

Step 4: Uses a symmetric decryption algorithm to generate plain text:

m = D_{k1} (c)

where the secret key k1 is computed in Step 2.

Step 5: Bob accepts the message 'm' only when:

rG = T .

Otherwise he rejects.

D. Judge Verification

Using Dffie-Hellman key exchange protocol Bob will send his private key to the verifier or judge and provides signcrypted text (c, T, s) to the judge. The judge performs the following steps:

Step1: Computes

(k1,k2) = hash(vbT + vbsPa)

Step 2: Computes

r = KH_{k2} (c || ID_A || ID_B)

where IDA and IDB are the identifications given by the certificate authority(CA).

Step 3: If rG = T, then the signcrypted text (c, T, s) is sent by the sender Alice otherwise not.

Several precautions should be taken into account in implementation of the proposed scheme. It is strongly recommended to use a strong block cipher (such as AES) for encrypting messages. The generated random numbers and also the state of pseudo-random generators should be erased from the memory as soon as the signature is generated. The private keys should be stored in a secure storage media such as a Hardware Security Module (HSM).

IV. SECURITY FUNCTIONS OF THE PROPOSED SCHEME

The proposed scheme provides a wide variety of security attributes as it is depicted in Table I.

The proposed scheme gets its security from several components:

1) The security attributes of the session key establishment,

2) The security attributes of the certificates,

3) The security attributes of deployed block cipher, one-way hash function, and HMAC,

4) Intractability of ECDLP due to the selected domain parameters

The proof is based on the fact that it is almost intractable to solve the elliptic curve discrete logarithmic problem (ECDLP). We should choose the parameters in such a way that it will become infeasible for an eavesdropper to solve ECDLP.

Table -I : The Provided Security Attributes of Different Signcryption Schemes.

Signcryption Schemes	Confidentiality	Integrity	Unforgeability	Non-repudiation	Forward Secrecy	Public Verification
Proposed Scheme	Yes	Yes	Yes	Another Protocol	Yes	Yes
M. Toorani & A.A Beheshti Shirazi [6]	Yes	Yes	Yes	Directly	Yes	Yes
Zheng [1]	Yes	Yes	Yes	Another Protocol	No	No
Zheng and Imai [4]	Yes	Yes	Yes	Another Protocol	No	No
Bao and Deng [2]	Yes	Yes	Yes	Directly	No	Yes
Gamage et. al. [3]	Yes	Yes	Yes	Directly	No	Yes
Jung et al. [5]	Yes	Yes	Yes		Yes	

V. COST ANALYSIS

The costs involved in the Signcryption schemes are represented in the terms of the computational cost and the communication overhead. The operational costs involving machine cycles take the form of the computational cost.

Table -II : Average Computational Time (in MS) of Major Operations of Different Signcryption Schemes.

Signcryption Schemes	Sender Computational Time (ms)	Recipient Computational Time (ms)
Proposed Scheme	**2 X 83=166**	**2 X 83=166**
M. Toorani & A.A Beheshti Shirazi [6]	2 X 83=166	4X 83=332
Zheng [1]	1 X 220=220	2 X 220=440
Zheng and Imai [4]	1 X 83=83	2 X 83=166
Bao and Deng [2]	2 X 220=440	3 X 220=660
Gamage et al. [3]	2 X 220=440	3 X 220=660
Jung et al. [5]	2 X 220=440	3 X 220=660
Han et al. [11]	2 X 83=166	3 X 83=249

Table -III : Comparative Analysis of Computational Cost of Different Signcryption Schemes.

Signcryption Scheme	Participants	EXP	DIV	ECPM	ECPA	MUL	ADD	KH (.)
Zheng [1]	Alice	1	1	-	-	-	1	2
	Bob	2	-	-	-	2	-	2
Jung et al. [5]	Alice	2	1	-	-	-	1	2
	Bob	3	-	-	-	1	-	2
Bao and Deng [2]	Alice	2	1	-	-	-	1	3
	Bob	3	-	-	-	1	-	3
Gamage et al. [3]	Alice	2	1	-	-	-	1	2
	Bob	3	-	-	-	1	-	2
Zheng and Imai [4]	Alice	-	1	1	-	1	1	2
	Bob	-	-	2	1	2	-	2
Han et al. [11]	Alice	-	1	2	-	2	1	2
	Bob	-	1	3	1	2	-	2
Hwang [5]	Alice	-	-	2	-	1	1	1
	Bob	-	-	3	1	-	-	1
M. Toorani & A.A Beheshti Shirazi [6]	Alice	-	-	2	-	2	2	2
	Bob	-	-	4	2	-	-	2
Proposed scheme	**Alice**	**-**	**1**	**2**	**-**	**1**	**1**	**2**
	Bob	**-**	**-**	**2**	**1**	**-**	**-**	**2**

Where - ECPM = the number of elliptic curve point multiplication operation. ECPA = the number of elliptic curve point addition operation. EXP = the number of modular exponentiation operation. DIV = the number of modular division (inverse) operation. MUL = the number of modular multiplication operation. ADD = the number of modular addition operation. KH(.) = the number of one-way or keyed one-way hash function operation.

The Table III shows the comparative analysis of computational overhead of different signcryption schemes.

The proposed scheme requires only 2 ECPM (Elliptic Curve Point Multiplication) operations for signcryption and 2 ECPM for unsigncryption. In the same security level, the elliptic curve point multiplication needs 83 ms and the modular exponentiation operation needs 220 ms for average computational time in the Infineon's SLE66CUX640P security controller [5]. Although our scheme is slower than Zheng and Imai scheme [4] as shown in the Table II but they provide added functionality such as encrypted message authentication, forward secrecy, public verifiability. From this we may conclude that the proposed scheme gives better result than all other schemes such as Hwang et al., Zheng & Imai and M. Toorani.

VI. CONCLUSION

In this paper we have discussed a Signcryption scheme which provides the security properties of message confidentiality, authentication, integrity, unforgeability and non-repudiation, along with encrypted message authentication, forward secrecy of message confidentiality and public verifiability. The proposed scheme requires only 2 ECPM operations for each phase (signcryption and unsigncryption) .

Since the proposed scheme is based on elliptic curve cryptography and uses symmetric ciphering for encrypting messages, it has great advantages to be deployed in resource-constrained devices such as mobile phones. As a one-pass scheme, it is also so attractive for security establishment in store-and-forward applications such as E-mail and Short Message Service. Our scheme saves more computational cost for both sender and receiver to suit the application of restricted computational devices like mobile device, smart cards etc. (using zero knowledge proof for authentication) at the same time providing encrypted message authentication and forward secrecy.

REFERENCES

[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] R.H. Deng F. Bao, “A signcryption scheme with signature directly verifiable by public key”, Proceedings of PKC'98 LNCS 1431, pages 55 - 59, 1998.

[3] Gamage, Jussipekka Leiwo, and Yuliang Zheng, “Encrypted message authenti-cation by firewalls”, In Proc. of PKC99, LNCS 1560, pages 69 - 81. Springer-Verlag, 1999.

[4] Yuliang Zheng and Hideki Imai, “How to construct efficient signcryption schemes on elliptic curves”, Inf. Process. Lett., 68(5):227 - 233, 1998.

[5] Ren-Junn Hwang, Chih-Hua Lai, and Feng-Fu Su, “An effcient signcryption scheme with forward secrecy secrecy based on elliptic curve”, Applied Mathematics and Computa-tion, 167(2):870 - 881, 2005.

[6] Mohsen Toorani and Ali Asghar Beheshti Shirazi, “An elliptic curve-based signcryp-tion scheme with forward secrecy”, Journal of Applied Sciences, 9(6):1025-1035, 2009.

[7] M. Bellare and P. Rogaway, “Random Oracles are Practical: A Paradigm for Designing Efficient Protocols”, In Proceedings of the First ACM Conference on Computer and Communications Security (CCS '93), pages 62-73. 1993.

[8] Mohsen Toorani and Ali Asghar Beheshti Shirazi, “Cryptanalysis of an efficient signcryption scheme with forward secrecy based on elliptic curve”, Proceedings of International Conference on Computer and Electrical Engineering, 0:428 - 432, 2008.

[9] Johan Borst, Bart Preneel, and Vincent Rijmen, “Cryptography on smart cards”, Computer Networks, 36(4):423 - 435, 2001.

[10] Scott A. Vanstone, “Elliptic curve cryptosystem the answer to strong, fast public-key cryptography for securing constrained environments”, Information Security Technical Report, 2(2):78 - 87, 1997.

[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] Yuliang Zheng Joonsang Baek, Ron Steinfeld, “Formal proofs for the security of signcryption”, Journal of Cryptology, 20(2):203 - 235, 2007.