ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analysis of an Improved Signcryption Scheme Based on Elliptic Curves with Forward Secrecy

G.Balakrishna
Department of Computer Science & Engineering
Mewar university,chittorgarh(raj) India
balakrisnagudla@gmail.com

Manoj Paliwal*
Department of Computer Science & Engineering
V.B. polytechnic college,Udaipur(raj) India
manoj_paliwal_in@hotmail.com

Abstract: An elliptic curve based signcryption scheme is presented in this paper. This scheme not only provides message confidentiality, non-repudiation, integrity and un-forgebility but also provides forward secrecy and encrypted message authentication. A judge can verify the sender's signature on signcrypted message without decrypting message and take any help from sender. If the private key of the sender is divulged inattentively, it does not affect the confidentiality of the previous stored messages. Elliptic curves are used for their key size, security and bandwidth advantage .The proposed scheme can be applied to mobile communication environment due to low computational and communication cost.

Keywords: Signcryption, elliptic curves, mobile communication

I. INTRODUCTION

The security of message and authentication of sender for communication purposes is important for internet. To keep messages confidential and unforged the sender uses a digital signature algorithm with his private key to sign the message and then encrypts the message with a randomly chosen key using a symmetric cipher. The public key of the recipient is used to encrypt the random key to form an envelope. The sender than sends the envelope and the cipher text to the recipient. When the recipient receives the cipher text, he uses his private key to decrypt the envelope to get the secret key and then decrypts the cipher text to obtain the plain text and signature. Finally, the recipient verifies the message on the basis of signature, this is called signature-then-encryption scheme.

The problem with this method is high cost and low efficiency. An alternate scheme was proposed by Zheng, is signcryption that performs message encryption and digital signature in a single logical step with computational cost lower than signature-then-encryption approach this scheme was based on discrete logarithmic problems (DLP). Zheng and Imai proposed another signcryption scheme based on elliptic curves that save about 58% computational cost and 40% communication cost as compared to signature-then-encryption scheme.

This scheme was based on elliptic curve discrete logarithmic problem (ECDLP). Both the schemes achieve similar functionality but both the schemes lack forward secrecy, public verification and authentication of encrypted messages. Jung et.al proposed a new signcryption scheme based on discrete logarithmic problem with forward secrecy. In Jung's scheme, even attacker obtains the private key of the sender, he could not get the corresponding message yet that sender had sent. However, when dispute occurs, the judge cannot directly verify the signature because of not knowing the recipient private key. Bao and Deng enhanced Zheng's signcryption scheme that the judge can verify the signature without the recipient private key. This scheme was based on DLP but this scheme lacks forward secrecy and encrypted message authentication. Several signcryption schemes are proposed over years and each provide a different level of security service and computational cost. In this paper, we proposed a signcryption scheme based on elliptic curves that not only provides confidentiality, integrity, unforgeblity and non-repudiation but also forward secrecy of message confidentiality, public verification and encrypted message authentication. By forward secrecy of message confidentiality means, although the private key of sender is disclosed, it does not affect the confidentiality of previous messages. In the public verification function, a judge can directly signature of original message without sender's private key, when dispute occurs. In addition our scheme saves a great amount of computational cost especially for sender. The lower computation cost make our scheme can be applied to low powered devices like mobile devices efficiently.

II. THE PROPOSED SCHEME

In this paper we are improving the signcryption scheme developed by by Zheng and Imai which gives approx saving in communication overhead by 40%.

We assume that Alice is the sender, Bob is the recipient, and Eve is the malicious s active attacker in this paper. The scheme consists of four phases: initialization, signcryption, unsigncryption, and judge verification.

A. *Initialization Phase:*

This phase includes selecting the domain parameters, generating the public/private keys and getting a certificate for the public key of each user from certification authority. We select some public parameters as follows:

m- A large prime number, where $m>2^{160}$

a, b- two integer elements which are smaller than m and satisfy the following equation: $4a^3+27b^2 \bmod m \neq 0$.

C- The selected elliptic curve defined over finite field m

G- A base point of elliptic curve C with order n.

n- The order of point G, where n is a prime, $n\times G=O$ and $n\geq 2^{160}$

O- A point of C at infinite.

H- A keyed one way hash function

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

Alice keys: The sender Alice randomly selects an integer X_a as his private key and Xa<n-1.

X_a – Alice private key chosen uniformly at random from [1,-----,n-1]

Y_a – Alice public key ($Y_a = X_aG$, a point on C)

Bob’s keys: The receiver Bob randomly selects an integer X_b as his private key and X_b<n-1

X_b – Bob’s private key chosen uniformly at randomly from [1,------,n-1]

Y_b^{---} Bob’s public key ($Y_{b=}$ X_bG, a point on C)

They need to get a certificate of their public key from certification authority (CA).

B. *Signcryption Phase:*

Alice generates digital signature (T,s) of the message m and uses the symmetric encryption algorithm and secret key k to encrypt m. let c be cipher text.

Steps:

a. Verifies Bob’s public key Y_b by using his certificate.
b. Randomly selects an integer value v, where v ≤ n-1.
c. Computes k_1 = hash (vG).
d. Calculate ($k_{2,}$ $k_{3)\,=}$ hash $_($vY_b)
e. Uses the symmetric key encryption algorithm to get cipher text: c =E_{k2} (m)
f. Use the one way keyed hash function to generate: r = KH_{k3} (c‖k_1‖Id_a‖Id_b) where Id_a,Id_b are identification given by certification authority
g. Compute s = v / (r+Xa) mod q
h. Compute T = rG
i. Send the signcrypted text (c, T, s) to Bob.

C. *Unsigncryption Phase:*

Bob receives signcrypted text (c, T, s). He decrypts cipher text by performing symmetric decryption algorithm with secret key. He also verifies the signature:

Steps:

a. Verifies Alice public key Y_a by using her certificate.
b. Calculate k_1 = hash (sT+sY_a)
c. Compute (k_2, k_3) = hash (X_bsT + X_bsY_a)
d. Use the one way keyed hash function to generate : r = KH_{k3} (c‖k_1‖Id_a‖Id_b)
e. Use a symmetric decryption algorithm to generate plain text: m = D_{k2}(c)
f. Bob accepts the message only when rG = T . otherwise, he rejects the message.

D. *Verification:*

The verification of signcrypted message by judge:

k_1 = hash (sT+sY_a)

r = KH_{k3} (c‖k_1‖Id_a‖Id_b)

accept m only if rG = T

III. ANALYSIS OF SCHEME

Proof:

To prove the verification condition

$$X_bsT + sX_bY_a = X_b\left(\frac{v}{r+X_a}\right)rG + \left(\frac{v}{r+X_a}\right)X_bY_a$$

$$= \frac{X_bvrG}{r+X_a} + \frac{vX_bY_a}{r+X_a}$$

$$= \frac{Y_bvr}{r+Xa} + \frac{vX_bGX_a}{r+X_a}$$

$$= \frac{Y_bvr}{r+Xa} + \frac{vY_bX_a}{r+X_a}$$

$$= vY_b\left(\frac{r+X_a}{r+X_a}\right)$$

$$= vY_b$$

To prove the decryption stage:

$$ST + SY_a = \frac{vT}{r+X_a} + \frac{vY_a}{r+X_a}$$

$$= \frac{vrG}{r+X_a} + \frac{vX_aG}{r+X_a}$$

$$= vG\left(\frac{r+X_a}{r+X_a}\right)$$

$$= vG$$

A. *Security:*

The security properties of the proposed scheme are as follows:

a. Unforgeability: It is computationally infeasible to forge a valid signcrypted text (c,T,s) and claim that it is coming from sender Alice without having sender’s private key.
b. Non-repudiation: If the sender Alice denies that he sent the signcrypted text (c,T,s), any third party can apply the verification procedure to determine that the message came from sender.
c. Confidentiality: It is achieved by encryption. To decrypt the cipher text, an adversary need to have recipient’s Bob’s private key.
d. Public Verifiability: Verification requires only sender’s public key. All public keys are 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.
e. Forward secrecy: An adversary that obtains sender’s private key will not be able to decrypt past messages. Previously recorded values of (c,T,s) that were obtain before the compromise cannot be decrypted because the adversary that has sender’s private key will need to calculate r to decrypt. Calculating r requires solving the ECDLP on r, which is computationally infeasible.
f. Encrypted message authentication: The scheme enables a third party to check the authenticity of the signcrypted text (c,T,s) without having to reveal the plain text to the third party.

IV. COST ANALYSIS

The cost which is invested in the process of signcryption and in the process of unsigncryption by receiver is analyzed.

A. *Saving in Computational Complexity:*

It is assumed that the elliptic curve point operations are the most expensive computational in terms of the time consume. The proposed scheme requires three point multiplications, unsigncryption requires two point multiplication and one point addition, and verification requires one point multiplication and one point addition. The traditional signature-then-encryption EIgamal elliptic curve encryption requires three point multiplications with one point addition for signature-encryption and three point multiplications with two point additions for verification-decryption. This makes the proposed scheme faster than signature-then-encryption in both signcryption and unsigncryption. The Zheng-Imai requires one point multiplication for signcryption and two point multiplications with one point addition for unsigncryption. Thus, the proposed scheme is slower than Zheng-Imai in sigcryption, but this scheme is justified by fact that it provides public verifibity and forward secrecy properties.

B. Saving in Communicational Overhead:

Communication overhead calculations are based on the following assumptions:

1) |hash(.)| = |KH(.)| = |q| ÷ 2

2) $|q| \approx |p^m|$

3) Point compression is used.

The communication overhead of SECDSS1 followed by ElGamal elliptic curve encryption is,

(|hash(.)| + |q|) + 2(|q| + 1) = |hash(.)| + 3 |q| = 3.5 |q| assuming that |q| >>1

The communication overhead of the proposed schemes is

|q| + (|q| + 1) = 2 |q| + 1 ≈ 2 |q| assuming that |q| >>1

Thus bandwidth saving can be calculated as (3.5 |q| − 2 |q|)/3.5 |q| = 42.86%

This saving is higher than the one calculated in Zheng-Imai paper, which is 40%. In addition it supports forward secrecy and public verifiability.

V. CONCLUSIONS

The paper presents a efficient signcryption scheme. It utilizes elliptic curves due to smaller key size and more security. It also provides public verifiability, forward secrecy and encrypted message authentication. This scheme achieves these security properties with saving in computational cost as compared to other approaches. The scheme can be applied to restricted computational devices like mobile devices.

VI. REFERENCES

[1]. Wiiliam stallings, cryptography and network security: principles and practices. Prentice hall inc., fourth edition, 2004.

[2]. Behrouz A. Forouzan , cryptography and network security. Tata mcgraw-hill, 2007.

[3]. Ren-junn Hwang, Chih-hua Lai, Feng-fu Su. An efficient syncryption scheme with forward secrecy based on elliptic curve, applied mathematics and computation, 167(2):870_881, 2005.

[4]. X. Yang 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.

[5]. 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, 0:428-432, 2008.

[6]. R. H. Deng, F. Bao. A signcryption scheme with signature directly verificable by public key. Proceedings of PKC’98 LNCS1431, pages 55-59, 1998.

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

[8]. Mohsen Toorani and Ali Ashgar Beheshti Shirazi. An elliptic curve-based signcryption scheme with forward secrecy. Journal of Applied Sciences, 9(6): 1025-1035, 2009.

[9]. Y. Zheng, “digital signcryption or how to achieve cost (signature and encryption)<<cost(signature) +cost(encryption)” , Advances in Cryptography- crypto’97, LNCS 1294, Springer-Verlag, 1997 pp. 165-179.

[10]. Xiang-xue, CHEN Ke-fei, LI shi-qun, “cryptanalysis and improvement of signcryption schemes on elliptic curves”, Wuhan University Journal of Natural Sciences, Vol. 11, No. 6, 2006, 1589-1592.

[11]. Lawrence C. Washington, “elliptic curves: Number theory and Cryptography”,CRC Press, 2003.