International Journal of Information & Network Security (IJINS)
Vol.2, No.3, June 2013, pp. 253~259
ISSN: 2089-3299

An Efficient Signcryption Scheme based on The Elliptic Curve Discrete Logarithm Problem

F. Amounas*, H.Sadki* and E.H. El Kinani**
* R.O.I Group, Computer Sciences Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Box 509. Morocco
** A.A Group, Mathematical Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Box 509 .Morocco

Article Info

Article history:

Received Feb 02nd, 2013
Accepted Feb 30th, 2013

Keyword:

Cryptography, Digital Signature, Elliptic Curve, Signcryption, Forward Security, Public Verifiability.

ABSTRACT

Elliptic Curve Cryptosystems (ECC) have recently received significant attention by researchers due to their performance. Here, an efficient signcryption scheme based on elliptic curve will be proposed, which can effectively combine the functionalities of digital signature and encryption. Since the security of the proposed method is based on the difficulty of solving discrete logarithm over an elliptic curve. The purposes of this paper are to demonstrate how to specify signcryption scheme on elliptic curves over finite field, and to examine the efficiency of such scheme. The results analysis are explained.

Corresponding Author:

E.H. El KINANI
A.A Group, Mathematical Department
Moulay Ismaïl University,
Faculty of Sciences and Technics, Box 509 Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

1. INTRODUCTION

The encryption and digital signature are two basic cryptographic mechanisms that can provide the security of communications. To guarantee unforegeability, integrity and confidentiality of communications, the traditional method is to digitally sign a message with the private key of the sender then encrypt the message and the signature with a randomly chosen key using a symmetric cipher. The random key is then encrypted using the public key of the receiver. The encrypted (message and signature) is then sent with the encrypted symmetric key. The opposite process is run at the receiver. This scheme is known as signature-then-encryption. An alternative scheme called signcryption was proposed by Zheng to simultaneously sign and encrypt messages in a single logical step with a computational cost significantly lower than that required by the traditional signature-then-encryption approach [1].

Nowsdays, the signcryption schemes are widely adopted for building the infrastructures of many advanced communication services. To garantiee the quality of these cryptographics services, severals signcryption schemes are proposed in the literature [2-8]. Here, the proposed method is compared to the existing schemes based ECC to find out our algorithm performance.

In our previous works [9-13], we provide the public-key cryptosystems based on ECC mechanism. Then, we investigate the elliptic curve digital signature using Boolean permutation [14]. In the present paper, a new signcryption scheme based on the Elliptic Curve Discrete Logarithm Problem (ECDLP) is proposed that simultaneously provides the attributes of message confidentiality, unforegeability and nonrepudiation, public verifiability, forward secrecy, and encrypted message authentication.

The structure of this paper is organized as follows. Section 2 investigates the related work. Section 3 briey reviews some basic notions connected with elliptic curve. Section 4 introduces the new signcryption scheme. We make the comparisons among the previous schemes and ours in Section 5. Finally, Section 6 makes some conclusions.

2. RELATED WORK

In the literature, many of the proposed signcryption schemes include modular exponentiation while some of them are based on elliptic curves. Y.Zheng [1] proposed signcryption scheme which saves about 58% computational cost and saving about 40% communication cost than signature-then-encryption scheme based on elliptic curve. This scheme was based on discrete logarithmic problem.

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. Gamage and al. [3] modified Zheng's signcryption scheme so that anyone can verify the signature of cipher text. Their scheme only verifies the cipher text to protect confidentiality of the message. Jung and al. [4] showed that Zheng's 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. However, in those research results, when dispute occurs, the judge cannot directly verify the signature because of not knowing the recipient's private key.

Zheng and Imai [5] suggested an ECC based signcryption scheme thus providing all the basic security features, with cost less than as required by "signature-then-encryption". They choose ECC because elliptic curve based solutions are usually based on the difficulty of ECDLP. 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. After all these schemes, Mohsen Toorani and al.[6] proposed a signcryption scheme based on elliptic curve which provide all the security attributes. But, this scheme takes more computational as compared to existing schemes. So, a secure and novel signcryption scheme based on elliptic curve is urgently required in this field.

In this paper, we show that a recent signcryption schemes, i.e. Hwang scheme [7], Han scheme [8] and M.Toorani scheme, have such vulnerability and many other security flaws and shortcomings that are described throughout the paper. Here, we propose a new signcryption scheme based on elliptic curve, which provide the required properties.

3. BRIEF REVIEW OF ELLIPTIC CURVE

The hardness of ECDLP enables ECC operates on groups of points over EC for security. An elliptic curve takes the general form as:

$$y^2 = x^3 + ax + b, \qquad (1)$$

Where x, y are coordinates of finite field F_p, and a, b are integer modulo p, satisfying:

$$4a^3 + 27b^2 \neq 0 \pmod{p}. \qquad (2)$$

Here ‘p’ is modular prime integer which makes the EC of F_p. An elliptic curve E over F_p consist of the points (x,y) defined by equations (1) and (2), along with an additional point called Ω (point at infinity) in EC. These points are said to be afine points.

Some fundamentals operations of elliptic curve that is essential to understand the mathematical description of elliptic curve used in the cryptographic scheme is discussed below:

- Point Addition: It is possible to obtain a third point R on the curve given two points P and Q. The symbol `+' represents the elliptic curve addition R = P+Q.
- Point Multiplication: k×P denotes the multiplication of an elliptic curve point P by an integer k. This is analogous to the addition of P to itself k times and this results is another point on the curve.

Definition (The Elliptic Curve Discrete Logarithm Problem). Let P and Q be two points of an elliptic curve with order n where n is a prime. Then, we compute a point Q = k.P (i) where k<n. Given these two points P and Q, find the correct value of k, satisfying (i). Up to now, it is computational infeasible to generate k from P and Q [15].

4. THE PROPOSED SCHEME

The proposed signcryption scheme consists of four phases: initialization phase, signcryption phase, unsigncryption phase and judge verfication phase. In the initialization phase, system generates and publishes domain parameters of elliptic curve, and each user generates his own private key and the related public key.

In the signcryption phase, the sender Alice signs and encrypts a message. Then she sends the signcrypted text to the recipient Bob. In the unsigncryption phase, the recipient Bob derives secret key to decrypt plaintext. He also verifies the signature. In the judge verification phase, a judge decides whether the

sender Alice sent the signcrypted message or not, when dispute occurs. We describe these four phases in the following [16].

4.1 Initialization

In this phase, some public parameters are generated. The steps are as follows:
Let E the selected elliptic curve over finite field: F_p.
G: a base point of elliptic curve E with order n.
$E_k(.)/D_k(.)$: symmetric encryption/decryption algorithm with private key k.
Alice's keys:
v_a: Alice's private key, chosen uniformly at random from [1..n-1].
P_a: Alice's public key ($P_a = v_aG$, a point on E).
Bob's keys:
v_b: Bob's private key, chosen uniformly at random from [1.. n-1].
P_b: Bob's public key ($P_b = v_bG$, a point on E).

4.2 Step's involved in Signcryption

A scheme of signcryption and unsigncryption stages of the proposed scheme is depicted in Figure 1. Assume that Alice wants to send a message m to Bob. Alice generates digital signature (R,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,R,S) in the following steps:

Step 1. Randomly selects a point on elliptic curve noted K = (k1,k2) except Ω.
Step 2. Compute the cipher text as: $c = E_{k1}(m)$ where the secret k1 is the x-coordinate of K (Step 1).
Step 3. Computes r=Hash(c,k2) with the secret k2 is the y-coordinate of K (Step 1).
Step 4. Computes:

$$S = vP_b + K \quad \text{where } v=v_ar.$$

Step 5. Computes $R = rP_a$.
Step 6. Sends the signcrypted text (c,R,S) to Bob.

4.3 Step's involved in Unsigncryption

Bob receives the signcrypted text (c,R,S). He decrypts cipher text c by performing symmetric decryption algorithm and verifies the signature. Bob gets the plaintext as follows:

Step 1. Computes $(k1,k2) = S - v_bR$.
Step 2. Computes r = Hash(c,k2).
Step 3. Decrypts the received ciphertext as: $m = D_{k1}(c)$, where the secret key k1 is computed in Step 1.
Step 4. Bob accepts the message m only when $rP_a = R$. Otherwise he rejects.

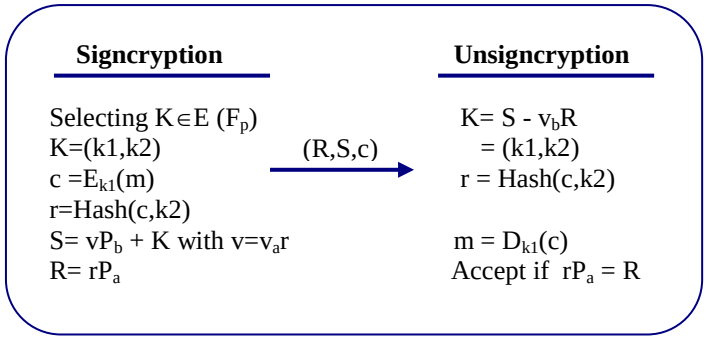

Figure 1. The proposed scheme.

4.4 Verification of the signcrypted message: by a firewall or judge.

$k2 = (S - v_bR)_y$
r = hash (c, k2)
Accept c only if $rP_a = R$.

4.5 Proof

To prove the verification condition and the decryption stage:

$S - v_bR = (rv_aP_b + K) - v_b(rP_a)$

$= rv_aP_b + K - (rv_av_bG)$

$= K$

Hence proved.

Thus, K = (k1,k2), Computing k2 allows the verification of the signcrypted text, Computing k1 allows the decryption of the message using: $m = D_{k1}(c)$.

5. THE SECURITY FUNCTIONS OF THE PROPOSED SCHEME

The below table (Table 1) indicates the security features supported by existing signcryption schemes along with the proposed scheme. The proof is based on the fact that it is almost intractable to solve the elliptic curve discrete logarithmic problem (ECDLP) [17]. We should choose the parameters in such a way that it will become infeasible for an eavesdropper to solve ECDLP.

Table 1. Comparison based on security properties

Signcryption Schemes	Confi-Dentiality	Integrity	Un-forgeability	Non-Repudiation	Public Verifiability	Forward security
Our scheme	Yes	Yes	Yes	Directly	Yes	Yes
Han and al.	No	No	Yes	Directly	No	No
Hwang and al.	No	No	Yes	Directly	No	No
M.Toorani and al	Yes	Yes	Yes	Directly	Yes	Yes

Although M.Toorani and al. scheme provides all the security attributes. But, this scheme takes more computational cost as compared to our scheme.

a. Cost Analysis

In our proposed scheme, we try to reduce the computational cost. Table 2 shows the comparative analysis of computational overhead of different signcryption schemes based ECC.

Table.2. Comparative analysis of computational overhead

Signcryption schemes	Participant	EXP	DIV	ECPM	ECPA	MUL	ADD	HASH
Han and al.	Alice	-	1	2	-	2	-	2
(2004)	Bob	-	1	3	1	2	1	2
Hwang and al.	Alice	-	-	2	-	1	1	1
(2005)	Bob	-	-	3	1	-	-	1
M.Toorani and al	Alice	-	-	2	-	2	2	2
(2009)	Bob	-	-	4	2	-	-	2
Our scheme	Alice	-	-	2	1	1	-	1
	Bob	-	-	1	1	-	-	1

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), HASH (the number of one-way or keyed one-way hash function operation).

The above table (Table 2) shows the comparisons of computational cost of sender and recipient among our signcryption scheme and others [15]. The proposed scheme requires only 2 ECPM for signcryption and 1 ECPM for unsigncryption. The elliptic curve point multiplication needs 83 ms, noted T_{ECM} [18]. The table (Table 3) shows that our scheme give better result than other schemes such as Hwang and al., Han and al. and M.Toorani and al.

Table.3. Comparative analysis of different schemes on the average computational time of major operations.

Schemes	Sender Average computational time in ms	Recipient Average computational time in ms
Han and al.	$2\times T_{ECM}$ =166	$3\times T_{ECM}$ =249
Hwang and al.	$2\times T_{ECM}$ =166	$3\times T_{ECM}$ =249
M.Toorani and al.	$2\times T_{ECM}$ =166	$4\times T_{ECM}$ =332
Our scheme	$2\times T_{ECM}$ =166	$1\times T_{ECM}$ =83

In figure 2 shows the comparative analysis of the proposed scheme with the existing schemes based ECC. From this we may conclude that the proposed scheme give better result than all other schemes such as M.Toorani and al. In fact, the proposed scheme provides a wide variety of security attributes as it is depicted in Table 1 and saves great amount of computational cost.

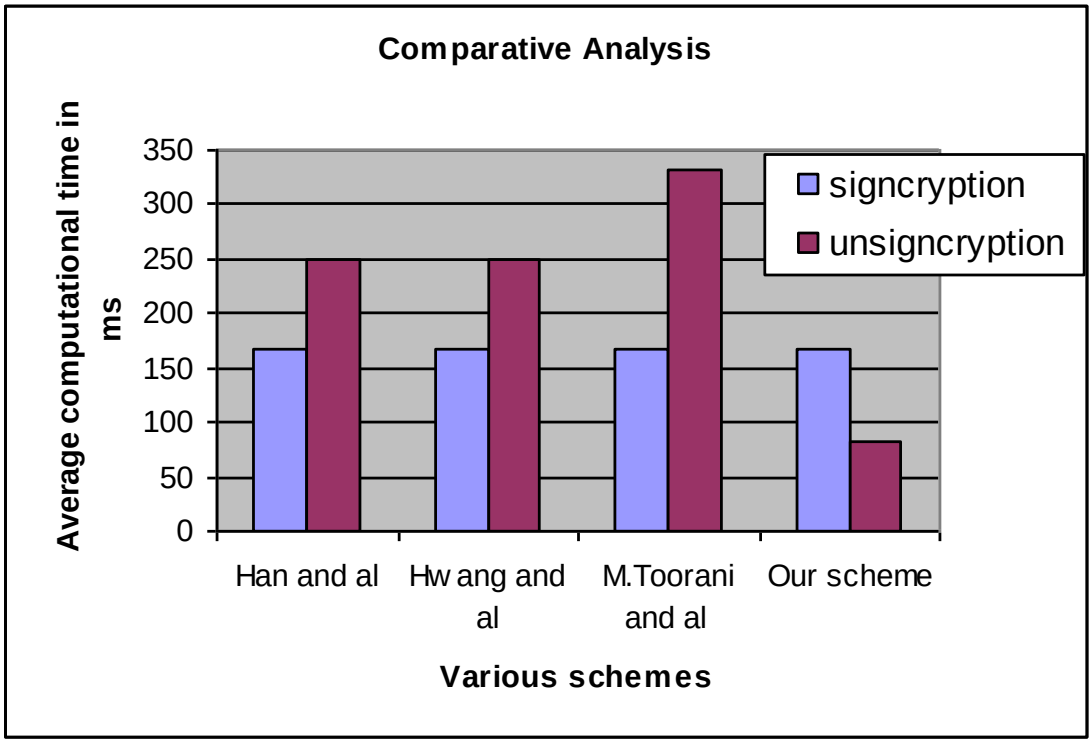

Figure 2. Performance

6. CONCLUSION

This paper presents an improved signcryption scheme that achieves the highly desired features in secure network applications. It utilizes elliptic curves for their high security and small key size. Our signcryption scheme based on ECDLP simultaneously provides the attributes of message confidentiality, unforegeability and non-repudiation, public verifiability, forward secrecy, and encrypted message authentication. Furether, the proposed scheme achieves these security properties with a saving in computation cost compared to the traditional signature-then-encryption scheme, which makes the new scheme more appropriate for environments with limited computing power. Finally, the proposed scheme can be applied to mobile communication environment more efficiently because of the low computation and communication cost.

REFERENCES

[1] Y. Zheng, Digital signcryption or how to achieve cost (signature & encryption) <<cost(signature)+cost(encryption)>>, *Advances in Cryptology* -Crypto'97, LNCS 1294, Springer-Verlag, pp. 165-179, 1997.

[2] F. Bao, R.H. Deng, A signcryption scheme with signature directly verifiable by public key, *Proceedings of PKC98, LNCS 1431, Springer-Verlag*, pp. 55-59, 1998.

[3] A. Gamage, J. Leiwo, Y. Zheng, Encrypted message authentication by firewalls, Proceedings of 1999. *International Workshop on Practice and Theory in Public Key Cryptography (PKC99),* LNCS 1560, Springer-Verlag, pp. 69-81, 1999.

[4] H.Y. Jung, K.S. Chang, D.H. Lee, J.I. Lim, Signcryption schemes with forward secrecy, *Proceeding of WISA* 2, pp. 403–475, 2001.

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

[6] 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.

[7] Ren-Junn Hwang, Chih-Hua Lai, and Feng-Fu Su. An efficient signcryption scheme with forward secrecy based on elliptic curve. *Applied Mathematics and Computation*, 167(2) pp.870-881, 2005.

[8] X.Yan, 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, pp.216-217, 2004.

[9] F.Amounas, E.H. El Kinani and A. Chillali, An application of discrete algorithms in asymmetric cryptography, *International Mathematical Forum*, Vol. 6, no. 49, pp.2409-2418, 2011.

[10] F.Amounas and E.H. El Kinani, Cryptography with Elliptic Curve Using Tifinagh Characters, *Journal of Mathematics and System Science* Vol.2, No.2, pp.139-144, 2012.

[11] F. Amounas and E.H. El Kinani, Fast Mapping Method based on Matrix Approach For Elliptic Curve Cryptography *International Journal of Information & Network Security (IJINS)* Vol.1, No.2, pp. 54-59, 2012.

[12] F.Amounas and E.H. El Kinani, Elliptic Construction Efficiency of the Elliptic Curve Cryptosystem using Code Computing for Amazigh Alphabet, International *Journal of Information & Network Security (IJINS),* Vol.2, No.1, pp. 43-53, 2013.

[13] F.Amounas and E.H. El Kinani, A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin 1/2 Matrices, International *Journal of Information & Network Security (IJINS),* Vol.2, No.2, pp. 190-196, 2013.

[14] F.Amounas and E.H. El Kinani, Elliptic Curve Digital Signature Algorithm Using Boolean Permutation based ECC, International *Journal of Information & Network Security (IJINS),* Vol.1, No.3, pp. 216-222, 2012.

[15] D. Johnson, A. Menezes, S. Vanstone, The elliptic curve digital signature algorithm (ECDSA), *International Journal of Information Security* 1 (1), pp. 36–63, 2001.

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

[17] Lawrence C. Washington. ,Elliptic Curves: Number Theory and Cryptography. CRC Press, 2003.

[18] Lejla Batina, SIddIka Berna rs, Bart Preneel, and Joos Vandewalle. Hardware architectures for public key cryptography. Integration, the VLSI Journal, 34(1-2):1- 64, 2003.

BIOGRAPHY OF AUTHORS

EL HASSAN EL KINANI received the Ph.D in mathematical physics in 1999 from Mohamed V University Rabat Morocco. He is full professor at department of mathematics in Moulay Ismaïl University, Faculty of Sciences and Technics, Errachidia, Morocco. He is interested in classical and quantum cryptography.

E-mail: elkinani_67@yahoo.com

FATIMA AMOUNAS received the DESS (diploma of high special study) degree in informatic in 2002 from Sidi Mohamed Ben Abdellah University, Faculty of Sciences Dhar El Mehrez, Fès Morocco. She is currently a Ph.D student in University Moulay Ismaïl, Faculty of Sciences and Technics, Errachidia, Morocco. Her research interests include elliptic curve and cryptography.

E-mail: F_amounas@yahoo.fr