Computer Engineering and Applications Vol. 2, No. 1, March 2013

Proposed Developements of Blind Signature Scheme Based on ECC

F. Amounas[1] and E.H. El Kinani[2]
[1]R.O.I Group, Computer Sciences Department Moulay Ismaïl University,
Faculty of Sciences and Technics Errachidia, Morocco
E-mail: F_amounas@yahoo.fr

[2]A.A Group, Mathematical Department Moulay Ismaïl University,
Faculty of Sciences and Technics Errachidia, Morocco
E-mail: elkinani_67@yahoo.com

ABSTRAKSI

Dalam beberapa tahun terakhir, Elliptic Curve Cryptography (ECC) yang menarik perhatian peneliti karena struktur yang kuat matematika dan keamanan tertinggi dibandingkan dengan algoritma lain yang sudah ada seperti RSA. Tujuan utama dalam pekerjaan ini adalah untuk memberikan skema tanda tangan blind novel berdasarkan ECC. Keamanan hasil metode yang diusulkan dari ketidaklayakan untuk memecahkan logaritma diskrit melalui kurva elips. Dalam tulisan ini kami memperkenalkan diusulkan untuk pengembangan skema tanda tangan blind dengan kompleksitas dibandingkan dengan skema yang ada.

Kata Kunci: Kriptografi, Blind Signature, Curve Elliptic, Kebutaan, Untraceability

ABSTRACT

In recent years, Elliptic Curve Cryptography (ECC) has attracted the attention of researchers due to its robust mathematical structure and highest security compared to other existing algorithm like RSA. Our main objective in this work was to provide a novel blind signature scheme based on ECC. The security of the proposed method results from the infeasibility to solve the discrete logarithm over an elliptic curve. In this paper we introduce a proposed to development the blind signature scheme with more complexity as compared to the existing schemes.

Keywords*:* Cryptography, Blind Signature, Elliptic Curve, Blindness, Untraceability.

1. INTRODUCTION

With growing importance of sender privacy in various schemes such as electronic voting protocol, blind signature schemes are gaining momentum. A blind

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

signature scheme is a protocol allowing the recipient to obtain a valid signature for a message, from the signer without him or her seeing the message. Blind signature is a form of digital signature in which the signer doesn't have authority over message, as also a third party could able to verify without knowing the secrets of both the parties that are involved in signature.

The concept of blind signature was first introduced by Chaum [1] in 1982. Any blind signature must satisfying two properties: Blindness and untraceability [1,2]. Blindness means the content of a message should be blind to the signer. Untraceability is satisfied if, whenever a blind signature is revealed to the public, the signer will be unable to know who the owner of the signature is.

In the literature, several applications of blind signature schemes have been developed through the e-commerce and e-voting fields. In 1995, Camenisch and al. [3] proposed a novel blind signature scheme based on the Discrete Logarithm Problem (DLP). But it fails the untraceability [5].

Blind signature scheme suggested by Camenisch and al. has been proved by Lee and al. that it does not satisfy correctness property [2]. In 2005, Wu and Wang [6] proved the untraceability of the Camenisch and al.'s scheme. They corrected the proof of Lee and al. untraceability and concluded that Camenisch and al.'s scheme is still more efficient than Lee and al.

Later, Jena and al. [7] proposed two novel blind signature schemes nevertheless there was no reasonable proof for correctness of their schemes. Recently Fan and al. [8] devised an attack on [2,6] schemes such that a signature requester, by performing only one round of system, can obtain more than one valid signature. Therefore, a novel blind signature scheme is required in this area.

Elliptic Curve Cryptosystem is accepted to be a secure and efficient public-key cryptosystem. In [9], Vanstone had concluded that ECC provided roughly 10 times greater efficiency than either integer factorization systems or discrete logarithm systems, in terms of computational overheads, key sizes and bandwidth.

Here we would like to focus on the security of ECC, relying upon the difficulty of solving the elliptic curve discrete logarithm problem. As were the cases with the integer factorization problem and the discrete logarithm problem modulo p, no efficient algorithms are known to solve the elliptic curve discrete logarithm problem. Vanstone [9] states," the elliptic curve discrete logarithm problem is believed to be harder than both the integer factorization problem and the discrete logarithm problem modulo p."

In the previous works, we provide the public-key cryptosystems based ECC [10-13]. Then, we propose a novel signcryption scheme based on the elliptic curve discrete logarithm problem (ECDLP) [14]. In this paper, a novel blind signature scheme based on elliptic curve will be proposed. The rest of the paper is organized as follows: Basic concept of elliptic curve (EC) is discussed in Section 2. Our blind signature scheme is presented in section 3. Section 4 is devoted to the security analysis of the proposed method. Finally, conclusions are made in section 5.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

2. FUNDAMENTALS OF ELLIPTIC CURVE CRYPTOGRAPHY

Some fundamentals of elliptic curve cryptography that is essential to understand the mathematical descriptions of elliptic curve over finite field F_p used in the cryptographic scheme are discussed below:

• **Scalar addition:** A new scalar can be obtained as a result of the addition of two or more scalars. Common integer addition modulo p is the addition in case of F_p. The scalar addition of a and b producing c is given by c = a + b.

• **Scalar Multiplication:** A new scalar can be obtained by the multiplication of two or more scalars. Common integer multiplication modulo p is the multiplication in case of F_p. The scalar multiplication of a and b producing c is given by $c = a \times b$.

Scalar Inversion: a^{-1}, the denotation of multiplicative inverse of any constituent element of F_p has the property $a.a^{-1} = 1$. The Fermat's method or the extended Euclidean algorithm aid in its computation.

• **Point:** A point may be defined as an ordered pair of scalars conforming to the elliptic curve equation. These elements are denoted by capital letter such as P_1, P_2, etc. An alternative notation for a point P_1 is $P_1 = (x,y)$ where both x and y belong to the field.

• **Point Addition:** It is possible to obtain a third point R on the curve given two points P and Q with the aid of a set of rules. Such a possibility is termed elliptic curve point addition. The symbol '+' represents the elliptic curve addition R = P + Q. Point addition is not to be confused with scalar addition.

• **Point Multiplication:** $k \times P$ 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 in another point on the curve.

• **Elliptic Curve Group:** When the above discussed point addition operation is considered as a group operation, an additive group that consists of the set of the solutions of the elliptic curve equation and a special point called point-at-infinity, is formed.

The equation of $E(F_p)$ can be defined as:

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

where p $a \in F_p$ and $b \in F_p$ are constants such that:

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

An abelian group [15] is created with the set of points defined by the point addition extended by the point Ω. For points on an elliptic curve, we define a certain addition, denoted '+'. The addition rules are given below.

1) $\Omega + P = P$ and $P + \Omega = P$, where Ω serves as the additive identity.

2) $P + (-P) = (-P) + P = \Omega$, where $-P$ is the negative point of P.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

3) (P + Q) + R = P + (Q + R).
4) P + Q = Q + P.

For any two points P (x_1,y_1) and Q (x_2,y_2) over $E_p(a,b)$, the elliptic curve addition operation, which is denoted as P+Q=R (x_3,y_3), where the coordinates x_3 and y_3 satisfying:

$$\begin{cases} x_3=(t^2-x_1-x_2) \bmod p, \\ y_3=(t(x_1-x_3)-y_2) \bmod p, \end{cases}$$

Where the parameter t is given by:

$$t = \begin{cases} \frac{3x_1^2+a}{2y_1} \bmod p, \text{ if } P=Q \\ \frac{y_2-y_1}{x_2-x_1} \bmod p, \text{ if } P\neq Q \end{cases}$$

3. THE PROPOSED BLIND SIGNATURE SCHEME

In this section, we shall propose a novel efficient and low computation blind signature based on ECDLP. The underlying principles of the new blind signature scheme are explained using two kinds of participants: a signer and a requester (user). A user requests signatures from the signer, and the signer computes and issues blind signatures to the user. The different phases of the proposed scheme are explained below.

In the initialization phase, the domain's parameter is defined, and the signer publishes the necessary information. To obtain the signature of a message, the user submits a blinded version of the message to the signer in the request phase. In the signature generation phase, the signer signs the blinded message, and sends the result back to the user. Afterwards, the user extracts the signature in the extraction phase. During the verification phase, the validity of the declared signature is verified. We describe these five phases in the following:

Initialization Phase

Initially, some public parameters are generated. The signer specifies an appropriate elliptic curve (E) over the finite field F_p. Then, the base point is selected, which having the largest order n such that nG=Ω. He declares the values $E(F_p)$, G and n as public.

In this phase, the private key and public key of the signer are generated using elliptic curve, i-e the signer chooses randomly an integer v_s as the private key and computes the public key: $P_s = v_sG$.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

Moreover, the signer selects randomly an integer $v \in F_p$. Then, he computes the point $R_1=vG$ and keeps the value of v secret. The signer then sends back the point R_1 to the user.

Requesting Phase

After receiving R_1, the requester randomly selects an point K (k_1,k_2) into EC. Then its x-coordinate is used as blinding factor, which is F_p element. Therefore, the requester computes a point R having coordinates (x_0,y_0) as follows:

$$R=k_1^{-1}R_1 \qquad (3)$$

Note that k^{-1} indicates the inversion in the finite field [16]. If R is equal to Ω, the requester has to reselect the blinding point K, and then recalculate R (3).
After calculating $r = x_0 \bmod n$, the requester blinds the message m' as: $m'=k_1rm+ k_2$ and transmits m' to the signer.

Signing Phase: The signer computes the blind signature s' as: $s' = v_sm'+v$.
So, the signer generates the signature parameter s', then sends it to the requester.

Extraction Phase: the requester should do the followings to recover the real signature S after receiving the blinded signature s' from the signer: $S = k_1^{-1}s'G-k_1^{-1}k_2P_s$.
Then, the requester declares the tuple (R,S) as the signature of the message m.

Verifying Phase: The verifier verifies the signature as follows:

$$S \stackrel{?}{=} rmP_s+ R$$

The validity of the signature (R,S) for a message m is verified as following:

$$\begin{aligned} S -R &= k_1^{-1}s'G - k_1^{-1}k_2P_s - k_1^{-1}R_1 \\ &= k_1^{-1}(v_sm'+v)G - k_1^{-1}k_2P_s - k_1^{-1}R_1 \\ &= k_1^{-1}v_sm'G + k_1^{-1}(vG) - k_1^{-1}k_2P_s - k_1^{-1}R_1 \\ &= k_1^{-1}v_s(k_1rm + k_2)G - k_1^{-1}k_2P_s \\ &= rm(v_sG) + k_1^{-1}k_2(v_sG)-k_1^{-1}k_2P_s \\ &= rmP_s \end{aligned}$$

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

The different phases are given as following:

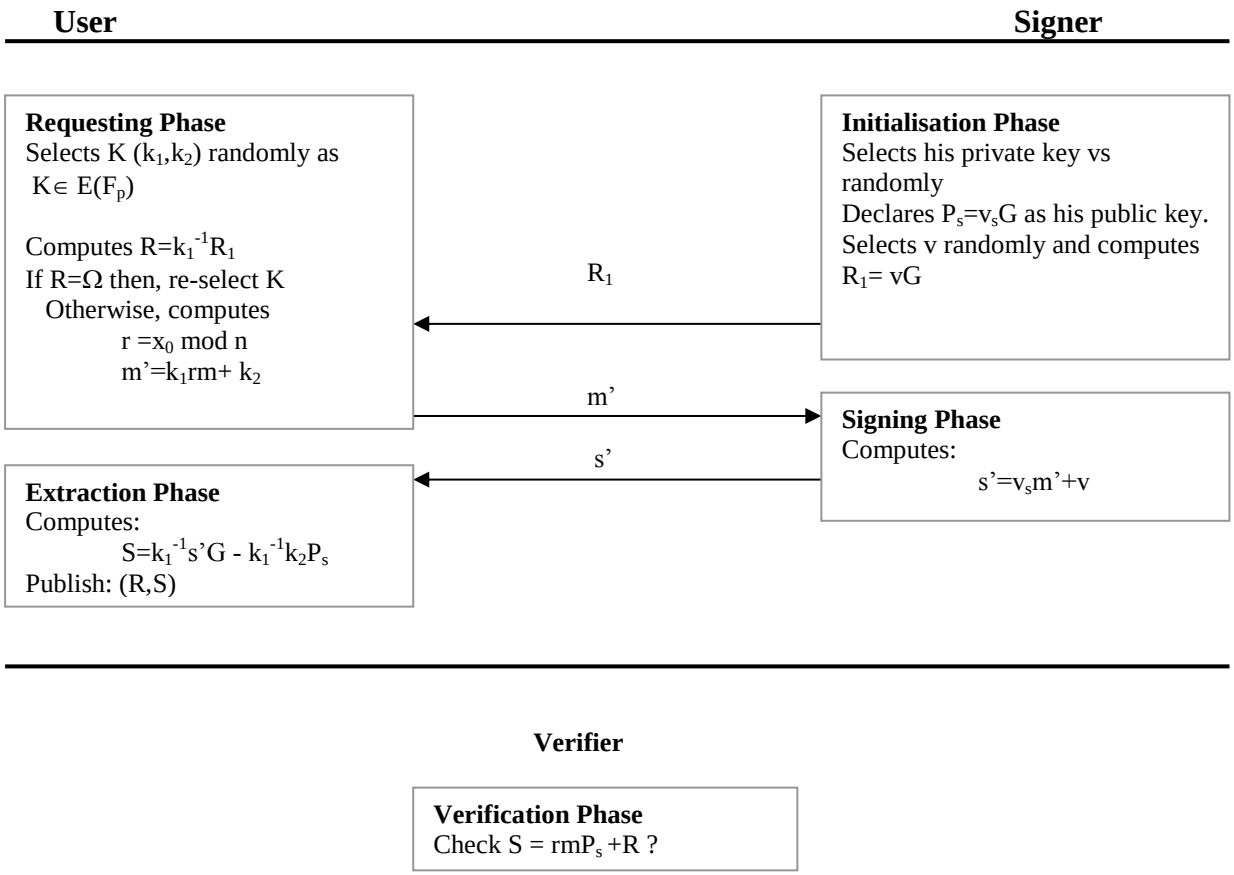

Figure 1. Flow of the proposed blind signature scheme.

4. SECURITY ANALYSIS

4.1 Property of blind signature

In this section, we would like to examine that our scheme satisfies the properties that a blind signature should hold. The security of the proposed method is based on the difficulty of the ECDLP (Elliptic Curve Discrete Logarithm Problem).

- Blindness

The blinded message of our scheme is generated as $m'=k_1r(m) + k_2$ in the request phase, since the signer is unable to derive the message m without the value k_1, k_2 and r. It is considered that equation (3) could not reveal any information about the blind factor since finding the blinding factors in this equation leads to solving ECDLP and this is infeasible. The signer can never find k_1, k_2 and r without the value of K, hence blindness property is correctly achieved. By the way, our scheme is satisfied the blindness property since the signer signs the blinded message and knows nothing about the true message.

- Untraceability

The signer cannot link the signature to the message as signer only has the information (v, R_1, m', s') for each blind signature requested. Therefore, without the

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

knowledge of the secret information of the requester (k_1, k_2, r), can not trace the blind signature.

4.2. Performance

In [4], the authors provide a novel untraceable blind signature scheme based on the ECDLP. Also, they declared that their blind signature scheme has a high performance compared to Camenisch and al [3].

In this work, our purpose is to redure a computional cost in terms of Multiplication. In fact, we shall compare our scheme to other methods [3, 4] to find out our algorithm performance.

In particular, we investigate the performance of the time complexity of various operation in terms of Multiplication (EXP: exponentiation, ECPM: multiplication in an elliptic curve point, MUL: Multiplication, ECPA: Addition of two points in an elliptic curve, ADD: Addition, INV: Inversion). Note that the time for computing modular addition is ignored, since it is much smaller than time for computing modular multiplication and modular inverse.

The comparisons of computation costs between the proposed blind signature protocol and other schemes are summarized in Table 1.

According to [17], the elliptic curve point multiplication needs $29T_{MUL}$, the elliptic curve point addition needs 0.12 T_{MUL} and the modular exponentiation operation needs $240T_{MUL}$ in termes of time complexity of a modular multiplication. The time complexities of the various schemes are illustrated in Table 1. The required computational cost for all schemes has been estimated by accumulating execution times of all the required operations.

Table 1. Comparative analysis of computational overhead in terms of T_{MUL}

Various schemes	Modular Exponentiation EXP	Elliptic Curve Point Multiplication ECPM	Elliptic Curve Point Addition ECPA	Modular inverse INV	Modular Multiplication MUL	Modular Addition ADD	Required Computation cost
Scheme [3]	7	-	-	2	10	2	$1696T_{MUL}$
Scheme [4]	-	7	3	1	6	3	203.57 T_{MUL}
Our scheme	-	6	2	1	6	2	$180.31T_{MUL}$

The above table shows the comparative analysis of the proposed scheme with the existing schemes [3, 4]. From this we may conclude that the proposed schemes give better result than all other schemes. In fact, our elliptic curve blind signature scheme

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

is as secure as the schemes [3] and [4]. But, our scheme is more efficient because it requires minimal operation performed by the user and signer in signing and thus makes it very efficient.

5. CONCLUSION

This paper suggests a novel blind signature scheme based on the Elliptic Curve Discrete Logarithm Problem. The scheme has been proved to be secure, robust and untraceable. The proposed scheme shows efficiency owing to lower storage requirements and computational overhead, which is due to the use of ECC. As the scheme is based on ECDLP, it achieves the same security with fewer bits key as compared to RSA. In addition, it has low-computation requirements. Besides, our scheme also satisfies the requirements of a blind signature scheme. Therefore, it can be efficiently applied to electronic cash payment systems or anonymous voting systems.

REFERENCES

[1] David Chaum. Blind Signatures for Untraceable Payments. In Advances in Cryptology| CRYPTO '82, pages 199{203, Santa. Barbara, California, 1982. Plemum.
[2] Cheng-Chi Lee, Min-Shiang Hwang, and Wei-Pang Yang. A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability. Applied Mathematics and Computation, 164(3): 837{841, 2005.
[3] Jan L. Camenisch, Jean-Marc Piveteau, and Markus A. Stadler. Blind Signatures Based on the Discrete Logarithm Problem. In Advances in Cryptology|EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, pages 428-432, 1994.
[4] Morteza Nikooghadam, Ali Zakerolhosseini, An Efficient Blind Signature Scheme Based on the Elliptic Curve Discrete Logarithm Problem. The ISC Int'l Journal of Information Security, Volume 1, Number 2, pp. 125-131, 2009.
[5] Lein Harn. Cryptanalysis of the Blind Signatures Based on the Discrete Logarithm Problem. Electronic Letters, 31(14):1136, 1995.
[6] Wu Ting and Jin-Rong Wang. Comment: A New Blind Signature Based on the Discrete Logarithm Problem for Untraceability. Applied Mathematics and Computation, 170(2): 999-1005, 2005.
[7] Debasish Jena, Sanjay Kumar Jena, and Banshidhar Majhi. A Novel Untraceable Blind Signature Based on Elliptic Curve Discrete Logarithm Problem. IJCSNS International Journal of Computer Science and Network Security, 7(6): 269-275, 2007.
[8] Chun-I Fan, D. J. Guan, Chih-I Wang, and Dai-Rui Lin. Cryptanalysis of Lee-Hwang-Yang Blind Signature Scheme. Computer Standards & Interfaces, 31(2):319-320, 2009.
[9] S. A. Vanstone, "Elliptic curve cryptosystem-the answer to strong, fast public-key cryptography for securing constrained environments," Information Security Technical Report, vol. 2, no. 2, pp. 78-87, 1997.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] F. Amounas, H.Sadki and E.H. El Kinani, "An Efficient Signcryption Scheme based on the Elliptic Curve Discrete Logarithm Problem", International Journal of Information & Network Security (IJINS), Vol.2, No.3, pp. 253-259 (2013).
[15] L. Uhsadel, A. Poschmann, and C. Paar, "An Efficient General Purpose Elliptic Curve Cryptography," In ECRYPT Workshop, SPEED - Software Performance Enhancement for Encryption and Decryption 2007, pp. 95-104, 2007.
[16] ANSI X9.62: "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", 1998.
[17] Neal Koblitz, Alfred J. Menezes, and Scott A.Vanstone. The State of Elliptic Curve Cryptography. Designs, Codes and Cryptography, 19(2-3):173-193, 2000.

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)

ISSN: 2252-4274 (Print)
ISSN: 2252-5459 (Online)