Proposed Developments of Blind Signature Scheme Based on ECC

F. Amounas¹ and E.H. El Kinani²
¹R.O.I Group, Computer Sciences Department Moulay Ismaïl University, Faculty of Sciences and Technics Errachidia, Morocco
E-mail: F_amounas@yahoo.fr

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

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
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.
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 $\mathbb{F}_p$ 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 $\mathbb{F}_p$. 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 $\mathbb{F}_p$. 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 $\mathbb{F}_p$ has the property $a \cdot a^{-1} = 1$. 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 $E(\mathbb{F}_p)$ can be defined as:

$$y^2 = x^3 + ax + b,$$  \hspace{1cm} (1)

where $a \in \mathbb{F}_p$ and $b \in \mathbb{F}_p$ are constants such that:

$$4a^3 + 27b^2 \neq 0.$$ \hspace{1cm} (2)

An abelian group [15] is created with the set of points defined by the point addition extended by the point $\Omega$. 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 $\Omega$ serves as the additive identity.

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

153

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:

\[
\begin{align*}
    x_3 &= (t^2 - x_1 - x_2) \mod p, \\
    y_3 &= (t(x_1 - x_3) - y_2) \mod p,
\end{align*}
\]

Where the parameter \(t\) is given by:

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

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 \(nG = \Omega\). 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: \(P_s = v_sG\).
Moreover, the signer selects randomly an integer \( v \in \mathbb{F}_p \). 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 \( \mathbb{EC} \). Then its \( x \)-coordinate is used as blinding factor, which is \( \mathbb{F}_p \) element. Therefore, the requester computes a point \( R \) having coordinates \((x_0, y_0)\) as follows:

\[
R = k_1^{-1}R_1
\]

Note that \( k_1^{-1} \) indicates the inversion in the finite field \([16]\). If \( R \) is equal to \( \Omega \), the requester has to reselect the blinding point \( K \), and then recalculate \( R \).

After calculating \( r = x_0 \mod n \), the requester blinds the message \( m' \) as:

\[
m' = k_1 rm + k_2
\]

and transmits \( m' \) to the signer.

**Signing Phase:** The signer computes the blind signature \( s' \) as:

\[
s' = vsm' + v
\]

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:

\[
S - R = rmP_s + R
\]

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

\[
S - R = k_1^{-1}s'G - k_1^{-1}k_2P_s - k_1^{-1}R_1
\]

\[
= k_1^{-1}(v_s m' + v)G - k_1^{-1}k_2P_s - k_1^{-1}R_1
\]

\[
= k_1^{-1}v_s k_1 rm + k_2 G - k_1^{-1}k_2P_s
\]

\[
= rm(v_s G) + k_1^{-1}k_2(v_s G) - k_1^{-1}k_2P_s
\]

\[
= rmP_s
\]
The different phases are given as following:

<table>
<thead>
<tr>
<th>User</th>
<th>Signer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requesting Phase</strong></td>
<td></td>
</tr>
</tbody>
</table>
Selects K $(k_1, k_2)$ randomly as $K \in E(F_p)$  
Computes $R = k_1^{-1} R_1$  
If $R = \Omega$ then, re-select K  
Otherwise, computes $r = x_0 \mod n$  
$m' = k_1 r m + k_2$ |
|  | $R_1$ |
|  | $m'$ |
| **Extraction Phase** |  
Computes: $S = k_1^{-1} s' G - k_1^{-1} k_2 P$  
Publish: $(R, S)$ |
|  | $s'$ |

| Initialisation Phase |  
Selects his private key $v$ randomly  
 Declares $P_v = v G$ as his public key  
 Selects $v$ randomly and computes $R_1 = v G$ |
|  | $v$ |

| Signing Phase |  
Computes: $s' = v m' + v$ |
|  | $v$ |

<table>
<thead>
<tr>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verification Phase</strong></td>
</tr>
</tbody>
</table>
Check $S = r m P_v + R$ |

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 $m' = k_1 r (m) + k_2$ 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
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 reduce a computational 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 \(29T_{\text{MUL}}\), the elliptic curve point addition needs \(0.12T_{\text{MUL}}\) and the modular exponentiation operation needs \(240T_{\text{MUL}}\) in terms 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 \(T_{\text{MUL}}\)**

<table>
<thead>
<tr>
<th>Various schemes</th>
<th>Modular Exponentiation</th>
<th>Elliptic Curve Point Multiplication</th>
<th>Elliptic Curve Point Addition</th>
<th>Modular Inverse</th>
<th>Modular Multiplication</th>
<th>Modular Addition</th>
<th>Required Computation cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheme [3]</td>
<td>7</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>10</td>
<td>2</td>
<td>1696(T_{\text{MUL}})</td>
</tr>
<tr>
<td>Scheme [4]</td>
<td>-</td>
<td>7</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>203.57(T_{\text{MUL}})</td>
</tr>
<tr>
<td>Our scheme</td>
<td>-</td>
<td>6</td>
<td>2</td>
<td>1</td>
<td>6</td>
<td>2</td>
<td>180.31(T_{\text{MUL}})</td>
</tr>
</tbody>
</table>

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
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


F. Amounas and E.H. El Kinani
Proposed Developments of Blind Signature Scheme Based on ECC