A proxy partially blind signature approach using elliptic curve cryptosystem

Nedal Tahat*
Department of Mathematics,
Faculty of Sciences,
Hashemite University,
P.O. Box 150459,
Zarqa 13115, Jordan
Email: nedal@hu.edu.jo
*Corresponding author

Emad E. Abdallah
Department of Computer Information System,
Faculty of Prince Al-Hussein Bin Abdallah II for
Information Technology,
Hashemite University,
Zarqa, Jordan
Email: emad@hu.edu.jo

Abstract: Partially blind signature is cryptographic system that is used in several protocols including e-cash and e-commerce systems. In proxy partially blind signature, part of the message is approved by the signer and the signature supplicant. Elliptic curve discrete logarithmic (ECDL) is an extremely difficult to solve problem as compared to any standard inverse operation of a one-way-trap door function including discrete logarithm problem or factorisation problem. In this paper, we propose a new proxy partially blind signature scheme based on ECDL. The main attractive features of the proposed scheme are the low computational cost and the low communication overhead. Moreover, the new scheme provides an extra level of security properties of both the partially blind signature and proxy signature. Several security analysis are shown to prove the security and the efficiency of the proposed scheme.

Keywords: partially blind signature; proxy signature; elliptic curve; blind signature.


Biographical notes: Nedal Tahat is currently a Lecturer at the Hashemite University, Jordan, and has taught various undergraduate courses. He received his BSc in Mathematics from Yarmouk University, Jordan in 1994, MS in Mathematics from Al Al-Bayt University, Jordan in 1998 and PhD in Mathematics from Universiti Kebangsaan Malaysia in 2010. His research area is in cryptography, with a focus on both classical and function-based digital signatures. He is currently working on developing function-based signatures systems using hybrid mode problems. In addition, his current work is in the field of fixed point theory for mappings.
1 Introduction

In the blind signature (Chaum, 1983), the receiver gets a message signed by the owner of the private keys without revealing any information about the message being signed (Masayuki and Tatsuaki, 2000). It guarantees that no one can obtain a link between a view and valid blind signature except the signature requester. The security of blind signatures was formalised by Juels et al. (1997). The blindness property has been used in several applications including electronic voting (Porkodi and Vidya, 2011), electronic cash and anonymous fingerprinting (Fujioka et al., 1993; Yan et al., 2003).

Partially blind signature (Abe and Fujisaki, 1996) is a generalised model of the blind signature. The signer imposes some common information such as the signature date or any other information that is known to the signer and the signature requester. Obviously, the information embedded in the signature is used for verification and validation (Jakobsson et al., 1996). Proxy signature scheme allows an original signer to delegate his signing right to a proxy signer to sign the message on behalf of an original signer (Mambo et al., 1996). Other proxy signature schemes have presented in Lee et al. (2001), Okamoto et al. (1999) and Zhang and Kim (2003). Verma and Sharma (2013) proposed proxy signature based on RSA cryptosystem. This kind of algorithms does not consider proxy revocation mechanism, but it is more efficient than the existing RSA-based schemes, i.e., Lee et al. (2001) and Shao (2003) schemes.

A proxy blind signature scheme is a digital signature scheme that ensures the properties of proxy signature and blind signature. The first proxy blind signature scheme was introduced by Lin and Jan (2000). The algorithm allows a user to obtain a proxy signature on a message without illuminating anything about the message or its signature to the proxy signer. Lal and Awasthi (2003) and Tan et al. (2002) proposed two proxy blind signature schemes based on Schnorr blind signature and Mambo et al. (1996) signature respectively. Verma and Birendra (2012) proposed a proxy blind signature scheme based on discrete logarithmic problem. Most of the latest schemes are based on factoring problem or discrete logarithms. Although these schemes are secure but they are very slow and for several applications it is inefficient to be used. To overcome this problem, several schemes are proposed passed on the elliptic curve discrete logarithms (Koblitz, 1987; Miller, 1986; Haija and Badawi, 2013; Ciss and Sow, 2012). Obviously, the ECDL offers a smaller key size. Hence, it is faster in terms of computational problem with a comparable security (Vanstone, 1997; Tzeng and Hwang, 2004; Hwang and Liao, 2005; Chung et al., 2007; Tahat, 2013; Indra and Taneja, 2014).
In this paper we proposed a new proxy partially blind signature based on ECDL. A partially blind signature using proxy key permits a proxy signer to explicitly embed any agreed common information into a blind signature. Our scheme has two advantages over the proxy blind signature schemes that use the discrete logarithmic problem. Firstly, the new technique extended the notion of proxy blind signature to proxy partially blind signatures. Secondly, the proposed scheme uses the elliptic curves with smaller security parameters. Clearly, using elliptic curves would improve the efficiency because of the reduced involvement of the bit-lengths. Proxy partially blind signature scheme should satisfy the following properties given by Tahat et al. (2009) and Zuowen (2002):

- **distinguishability**: the proxy signature must be distinguishable from the standard signature
- **no-repudiation**: the origin and the proxy cannot deny their signatures against anyone
- **enforceability**: only a designated proxy signer can create a valid proxy signature for the original signer
- **identifiability**: the verifier can recognise the proxy and the original signers
- **partial blindness**: it allows a user to obtain a signature on a message without illuminating anything about the message to the signer.

The rest of this paper is organised as follows. In the Section 2, we introduce our proxy partially blind signature based on ECDL problem. In Section 3, we analyse the security and the performance of the new scheme and finally we conclude in Section 4.

### 2 Proposed proxy partially blind signature scheme

In this section, we propose the new proxy partially blind signature. The proposed scheme is divided into four phases: notations, proxy delegation, partially blind signature, and signature verification phase.

#### 2.1 Notations

For the convenience of describing our proposed technique, we define the parameters as follows:

- **E**: elliptic curve defined on finite field size \( q \), where either \( q = p \) in case of \( p \) is an odd prime (the common practice), or \( q = 2^m \) in case that \( p \) is a prime power.

- Two parameter \( a, b \in \mathbb{F}_p \) to define the elliptic curve equation over:

\[
E : y^2 \equiv (x^3 + ax + b)(\mod p)
\]

\( E \) should be divisible by a large prime number with regard to the security issue raised by Pohling and Hellman (1978).

- A finite point \( G \) whose order is a large prime number in \( E(\mathbb{F}_p) \), where \( G \neq \mathcal{O} \) (\( \mathcal{O} \) denotes the point at infinity) such that the order of \( G \) is \( n \).
90  N. Tahat and E.E. Abdallah

- $U_o$: original signer.
- $U_p$: proxy signer.
- $U_r$: signature requester.
- $h()$: secure one-way hash function.
- $x_o$: original signer’s secret key.
- $y_o$: original signer’s public key, $y_o = x_oG$.
- $x_p$: proxy signer’s secret key.
- $y_p$: original signer’s public key, $y_p = x_pG$.

### 2.2 Proxy delegation phase

- Original signer $U_o$ choose a random number $\bar{k} \in \mathbb{Z}^*_n$ and then compute
  \[ \overline{\alpha} = \bar{k}G = (\overline{\alpha}_1, \overline{\alpha}_2), \text{ where } \overline{\alpha} = \overline{\alpha}(\text{mod } n) \]  
  \[ \overline{\delta} = (x_o\overline{\alpha} + \bar{k})(\text{mod } n) \]  
  Original signer $U_o$ sends $(\overline{\delta}, \overline{\alpha})$ to the proxy signer $U_p$ in a secure manner.

- $U_p$ verifies
  \[ \overline{\delta}G = (\overline{\alpha}y_p + \overline{\alpha})(\text{mod } n) \]  
  If the result is correct, then $(\overline{\delta}, \overline{\alpha})$ will be accepted. The correctness of equation (3) can be proved by
  \[ (\overline{\alpha}y_p + \overline{\alpha}) = (\overline{\alpha}x_pG + \bar{k}G) = (\overline{\alpha}x_p + \bar{k})G = \overline{\delta}G \]
- $U_p$ computes $S_p = (\overline{\delta} + x_p)(\text{mod } n)$, so $U_p$ has a proxy signature with a private key $S_p$ and the corresponding proxy signature public key $y_o$.

### 2.3 Partially blinding phase

- The requester computes $h(M) = m$, where $M$ is the message and $h: \{0,1\}^* \rightarrow \mathbb{Z}^*_n$.
- Suppose that $m$ is the signature of $U_r$. $U_r$ chooses a blind elements $\omega$, $\rho \in \mathbb{Z}^*_n$ and computes
  \[ \sigma = om\rho (\text{mod } n) \]  
  Moreover, $U_r$ prepares common information $c$, according to a pre-defined format. Then the value ‘$c$’ is a common input of both the requester $U_r$ and proxy signer $U_p$. $U_r$ sends $(\sigma, c)$ to $U_p$.
- $U_p$ uses the cut-choose method to determine the confidence degree of $\sigma$. If it is beyond the set one, blind signing is done.
A proxy partially blind signature approach using elliptic curve cryptosystem

- \( U_P \) chooses \( k \in \mathbb{Z}_n^* \) randomly, and computes
  
  \[
  \alpha = kG = (\alpha_1, \alpha_2), \text{ where } u \equiv \alpha_1 (\text{mod } n)
  \]

  \( \mu \equiv (k^{-1}S_p) (\text{mod } n) \)

  \[
  \overline{\delta} = (\sigma c - S_pu) k^{-1} (\text{mod } n)
  \]

  \( U_P \) sends \((\sigma, \overline{\delta}, \alpha, \overline{\alpha}, \mu)\) to \( U_r \).

- \( U_r \) verifies using
  
  \[
  (\sigma c)G = (u\alpha_p + uy_p + u\overline{\alpha} + \overline{\delta} \alpha) (\text{mod } n)
  \]

  If it is not correct, \( U_r \) reject the signature of partially blind message \( M \) from \( U_P \). The correctness of the equation (8) can be proved by

  \[
  (u\alpha_p + uy_p + u\overline{\alpha} + \overline{\delta} \alpha) = \left( \overline{\alpha_p} + \overline{\alpha} \right) u + \overline{\delta} kG = \left( \delta + x_p \right) u + \overline{\delta} kG = (S_pu + \overline{\delta} k)G = (\sigma c)G
  \]

2.4 Extraction phase

- \( U_r \) computes
  
  \[
  \delta = \left( \overline{\delta} + \mu u \right) \omega, \rho - \mu u (\text{mod } n)
  \]

  So \((h(M), \delta, \alpha, \overline{\alpha}, c)\) is the signature of message \( h(M) = m \).

- Anyone can distinguish the truth of \((h(M), \delta, \alpha, \overline{\alpha}, c)\) through verifying
  
  \[
  h(M)cG = (u\alpha_p + uy_p + u\overline{\alpha} + \overline{\delta} \alpha)
  \]

  The correctness of the equation (10) can be proved by

  Let \( \delta \) to be the equation of \( h(M) \). The equation

  \[
  \delta = \left( \overline{\delta} + \mu u \right) \omega, \rho - \mu u (\text{mod } n), \delta k = (h(M)c - S_pu)
  \]

  must be valid. Because:
3 Security analysis and performance evaluation

In this section we carefully discuss some of the security properties and the performance evaluation (Bruce, 2007) of our proposed partially blind signature scheme.

3.1 Security analysis

The proposed scheme satisfies the following security properties:

- **Unforgeability**: An adversary (including the original signer and the requester) wants to impersonate the proxy signer to sign the message $m$. He/she can intercept the delegation information $(\overline{\delta}, \overline{\alpha})$ but he/she cannot obtain the proxy secret key $SP$. So for this scheme forgery is extremely hard.

- **Identifiability**: In the agreement, when $U_o$ sends $(\overline{\delta}, \overline{\alpha})$ to $U_P$, $U_o$ keep $\overline{\alpha}$ and $U_P$ together. When $U$ meets a valid strong blind signature, it is easily to identify $U_P$ through $\overline{\alpha}$. In addition, there is other important information $(\overline{\alpha}, y_P)$ in the equation, through which $U_o$ also can identify $U_P$.

- **Non-repudiation**: In this scheme the original signer does not know the proxy signer’s secret key $x_P$. Moreover, the proxy signer does not know the original signer’s secret key $x_o$. Thus, neither the original signer nor the proxy signer can sign in place of each other.

- **Unlinkability**: Message $h(M) = m$ is blinded before it got signed by the proxy signer $U_P$. The blinded elements $\omega$ are only known to the signature requester $U_r$. To extract the message $m$ from $\sigma \equiv \omega \delta m^{-1} \pmod{n}$, you need to deal with a factorisation problem with a large number.

- **Reliability**: The private key of the proxy signature is a function value of $x_o$ and $x_P$, i.e., it relies on $x_o$ and $x_P$.

- **Partial blindness**: The partial blindness property of all signatures are issued by the signer. The signatures contain clear common information a according to a predefined format negotiated and agreed by all the requester and the proxy signer. Clearly, the requester is unable to change or remove the embedded information $c$ while keeping the verification of signature successful. In the proposed scheme, the requester $U_r$ has to submit the common information $c$ and the blinded data $\sigma$ to the proxy signer. The proxy signer after that computes and sends $\overline{\delta} \equiv (\sigma c - S_P \omega) k^{-1} \pmod{n}$ to $U_r$. It is
possible for \( U_p \) can successfully change or remove the common information \( c \) from
the signature, and then he/she can compute \( \delta = (\sigma_c - S_p)k^{-1} \pmod n \). However,
deriving the secret key \( S_p \) is an extremely difficult and time consuming.

- **Distinguishability:** A proxy signature is composed of \( \delta, \alpha, \sigma, c \) in which there are
two signature \( (\delta, \alpha) \) and \( (\sigma, c) \). The proxy signature could be distinguished from the
normal signature using the extra information which is included in the proxy
signature. Suppose that \( U_p \) is the only one who can generate the proxy signature and
there is another proxy signer \( U_D \). \( U_o \) sends \( (\sigma_D, \sigma_D, c_D) \) to \( U_p \) in which
\[
\sigma_D = \tilde{k}^G, \quad \tilde{k} \neq \bar{k}
\]  
(11)

According to the equation (11), it is easily to make sure that that the signature generated
by \( U_D \) must look like \( (\delta_D, \alpha_D, \sigma_D, c_D) \). Obviously, \( \tilde{k} \neq \bar{k} \), we can know that
\( \alpha_D \neq \sigma_D \). In this case, the two proxy signatures generated by \( U_p \) and \( U_D \) could be easily
distinguished.

**Table 1 Performance evaluation**

<table>
<thead>
<tr>
<th>Items</th>
<th>Time complexity</th>
<th>Complexity in ( T_{mul} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy delegation phase</td>
<td>( 3T_{ec-mul} + T_{mul} )</td>
<td>( 88.12T_{mul} + T_{ec-add} )</td>
</tr>
<tr>
<td>Partially Blinding phase</td>
<td>( 6T_{ec-mul} + 6T_{mul} + T_h + 3T_{ec-add} )</td>
<td>( 180.36T_{mul} + T_h )</td>
</tr>
<tr>
<td>Extraction and verification phase</td>
<td>( 5T_{ec-mul} + 3T_{mul} + T_h )</td>
<td>( 145T_{mul} )</td>
</tr>
</tbody>
</table>

### 3.2 Performance evaluation

In this section, we investigate the performance of our new proposed scheme in terms of
the computational complexity and communication cost. We use the following notation to
analyse the performance of the scheme:

- \( T_{mul} \) time complexity for executing the modular multiplication
- \( T_{exp} \) time complexity for executing the modular exponentiation
- \( T_{add} \) time complexity for executing the modular addition
- \( T_{ec-mul} \) time complexity for executing the elliptic curve multiplication
- \( T_{ec-add} \) time complexity for executing the elliptic curve addition
- \( T_h \) time complexity for executing the hash-function.

The performance of our scheme is described in terms of computational complexity and
communication costs. We ignore the negligible time performing for modular addition.
The performance of the proposed signature is summarised as follows: the computational
complexity for the proxy delegation phase, partially blinding phase and extraction and
verification phase is shown in Table 1. The last column converts various operation units
to \( T_{mul} \), where \( T_{exp} \approx 240T_{mul} \), \( T_{ec-mul} \approx 29T_{mul} \) and \( T_{ec-add} \approx 0.12T_{mul} \) given by Koblitz et al.
(2000). Finally, the communication costs or size of parameters of the scheme
(both signature generation and verification) is \( 11|n| \), where \(|a|\) denotes the bit-length of \( a \)
4 Conclusions

In this paper, we proposed a simple and robust proxy partially blind signature scheme based on elliptic curve discrete logarithm. The key idea is to use elliptic curves with smaller security parameters. Elliptic curves are more secure than any one-way-trapdoor functions and it would improve the efficiency by reducing bit-lengths involvement. The security of the new proxy partially blind signature cryptosystem is equivalent to elliptic curve discrete logarithmic problem with shorter keys and much improved performance. The computational cost is reduced without sacrificing other aspects of security. The extensive experiments and security analyses clearly indicate the high level of security and the good efficiency of the proposed scheme in comparison with partially blind signature and proxy signature.

References


A proxy partially blind signature approach using elliptic curve cryptosystem


