

Proxy Blind Signature Scheme based on Discrete Logarithm Problem and Elliptic Curve Discrete Logarithm Problem

Aung Nway Oo, Ni Lar Thein
University of Computer Studies, Yangon
aungnwayoo78@gmail.com, nilarthein@gmail.com

Abstract

In some applications, it is necessary to protect the privacy of the content of user from signer. Proxy blind signature can be used in these applications which combine the properties of both proxy signature and blind signature. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The proxy blind signature scheme is useful in several applications such as e-voting, e-payment and mobile agent environments. In this paper, firstly, we present proxy blind signature schemes based on discrete logarithm problem (DLP) and compare the complexity with previous scheme. Next, based on this DLP method, we present elliptic curve discrete logarithm problem (ECDLP) based proxy blind signature scheme. All of these satisfy the secure properties of both the blind signature scheme and the proxy signature scheme.

Keywords—blind signature, proxy signature, proxy blind signature, DLP, ECDLP.

1. Introduction

With the growing importance of the mobile transaction, the proxy blind signature scheme has become a very active research area. In 1982, David Chaum invented a blind signature [1], that scheme allows the sender to have a given message signed by the signers, without revealing any information about the message or its signature. In 1996, Mambo, Usudu and Okamoto [5] proposed a new concept, proxy signature. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original singer. Mambo, Usudu and Okamoto [6] proposed complete proxy signature, partial proxy signature and signature with an entitlement certificate. Zhang [7], and Kim, Park, and Won [8] proposed threshold proxy signature.

The first proxy blind signature was proposed by Lin and Jan [3] in 2000. Later, Tan et al.[4] proposed a proxy blind signature scheme based on DLP and ECDLP. However, in 2003, Lal et al.[9] pointed out that Tan et al.'s scheme was insecure and proposed a new proxy blind signature scheme based

on Mambo et al.'s scheme [6]. In 2004, Wang et al.[10] demonstrated that Tan's scheme was insecure and proposed two effective attacks. In 2004, Xue and Cao [11] showed there exists one weakness in Tan et al.'s scheme [4] and Lal et al.'s scheme [9] since the proxy signer can get the link between the blind message and the signature or plaintext with great probability. Xue and Cao introduced concept of strong unlinkability and they also proposed a proxy blind signature scheme. In 2005, Sun et al.[12] showed that Tan et al.'s schemes didn't satisfy the unforgeability and unlinkability properties and they also pointed out that Lal's scheme [9] didn't possess the unlinkability property either. In 2007, Li et al.[13] proposed a proxy blind signature scheme using verifiable self-certified public key, and compared the efficiency with Tan et al.[4]. Recently, Xuang Yang and Zhaoping Yu proposed new scheme and showed their scheme is more efficient than Li et al.[13].

In this paper, we present two proxy blind signature schemes. Our proposed scheme satisfied all the security requirements of both the blind signature scheme and the proxy signature scheme. Compared with previous schemes, our scheme is more efficient and low-computation.

The rest of this paper is organized as follows. In Section 2, we list the security properties of the scheme. And then, our proposed proxy blind signature scheme based on DLP is presented in Section 3. In Section 4, we analyze the security properties and the efficiency of the proposed scheme and compared with previous schemes. Section 5 presents a proxy blind signature scheme based on ECDLP. The performance of the scheme in terms of number of keys, computational complexity has been analyzed section 6. In Section 7, we give the notations used throughout this paper. Finally Section 8 describes the concluding remarks.

2. Required Security Properties

Since proxy blind signatures are combination of the proxy signature and blind signature, they should have the security properties of the proxy signature and blind signature. In this section, we describe the require properties of the scheme as follows.

- 1) Distinguishability: The proxy signature must be distinguishable from the normal signature.

- 2) Nonrepudiation: Neither the original signer nor the proxy signer can sign a message instead of other party. Both the proxy signer and original signer cannot deny their signatures against anyone.
- 3) Unforgeability: Only a designated proxy signer can create a valid proxy signature for the original signer (even the original signer cannot do it).
- 4) Identifiability: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.
- 5) Verifiability: The receiver of the signature should be able to verify the proxy signature in a similar way to the verification of the original signature.
- 6) Prevention of misuse: It should be confident that proxy key pair should be used only for creating proxy signature, which conforms to delegation information. In case of any misuse of proxy key pair, the responsibility of proxy signer should be determined explicitly.
- 7) Unlinkability: When the signature is verified, the signer knows neither the message nor the signature associated with the signature scheme.

3. Proposed Proxy Blind Signature Scheme based on DLP

In the proposed scheme, the original signer delegates his signing capabilities to proxy signer. The proxy signer generates the signature to the requester without knowing the content of the message. The protocol consists of following phases:

- Proxy delegation phase
- BlindSigning phase
- Verification phase

Original signer delegates his signing capability to proxy signer in the delegation phase. To obtain a signature, the requester submits an encrypted version (blinds the message) of the message to the proxy signer in the signing phase, then the proxy signer computes the blind signature of the message, and then sends the result back to the requester. In the extraction phase, the requester extracts the signature from the result received from proxy signer. Lastly, anyone can verify the legitimacy of the digital signature in the verifying phase. The different phases of the signature scheme are explained below.

3.1 Proxy Delegation Phase

Original signer O selects random number $k_o \in_R Z_q^*$ and computes:

$$r_o = g^{k_o} \pmod{p} \quad (1)$$

$$s_o = x_o + k_o h(m_w // r_o) \pmod{q} \quad (2)$$

O sends (r_o, s_o) along with the warrant m_w to the proxy signer. And then proxy signer checks:

$$g^{s_o} = y_o r_o^{h(m_w // r_o)} \pmod{p} \quad (3)$$

If it is correct, proxy signer P accepts it and computes proxy signature secret key s_{pr} as follow:

$$s_{pr} = s_o + x_p \pmod{q} \quad (4)$$

Note: responding proxy public key $y_{pr} = y_o y_p r_o^{h(m_w // r_o)} = g^{s_{pr}} \pmod{p}$.

3.2 Blind Signing Phase

Proxy signer P selects random number $k \in_R Z_q^*$ and computes:

$$r = g^k \pmod{p} \quad (5)$$

and then sends (r_o, r) to signature asker A . To obtain the blind signature of message m , original signer A randomly choose two random numbers $u, v \in_R Z_q^*$ and computes:

$$r^* = r g^u (y_o y_p)^{-v} \pmod{p} \quad (6)$$

$$e^* = h(r^* // m) \pmod{q} \quad (7)$$

$$e = e^* - v \pmod{q} \quad (8)$$

If $r^* = 0$ then A has to select new tuple (u, v) . Otherwise A sends e to P . After receiving e proxy signer P computes

$$s^* = k + e s_{pr} \pmod{q} \quad (9)$$

and sends the sign message s^* to A . After blind signing finish, signature asker A extract the signature as follows :

$$s = g^{s^* + u} r_o^{v h(m_w // r_o)} \quad (10)$$

Finally the signature of message m is (m, m_w, s, e^*, r_o) .

3.3 Verification Phase

The recipient of the signature can verify the proxy blind signature by checking whether

$$e^* = (h(s y_{pr}^{-e^*} \pmod{p} // m)) \pmod{q} \quad (11)$$

Where $y_{pr} = y_o y_p r_o^{h(m_w // r_o)}$

If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects. The comparison of computational cost with previous DLP based schemes is described in section 6.

4. Proof of Security Properties

In this section we discuss the correctness and some of

the properties of our proposed DLP based proxy blind signature scheme, described in section 3.

Proxy Distinguishability: On the one hand, the proxy blind signature (m, m_w, s, e^*, r_o) contains the warrant m_w . On the other hand, anyone can verify the validity of the proxy blind signature, so he can easily distinguish the proxy blind signature from the normal signature.

Nonrepudiation: The original signer does not obtain the proxy signer's secret key x_p and proxy signer does not obtain original signer's secret key x_o . Thus, neither the original signer nor the proxy signer can sign in place of the other party. At the same time, through the valid proxy blind signature, the verifier can confirm that the signature of the message has been entitled by the original signer, because the verifier must use the original signer's public key during the verification. Likewise, the proxy signer cannot repudiate the signature. The scheme offers nonrepudiation property.

Unforgeability: An adversary (including the original signer and the receiver) wants to impersonate the proxy signer to sign the message m . He can intercept the delegation information (m_w, s_o, r_o) but he cannot obtain the proxy signature secret key s_{pr} . From Equation (4), we know that only the proxy signer holds the proxy signature secret key x_p . Because of $x_p \in_R Z_q^*$, the adversary can obtain the proper proxy signature secret key by guessing it with at most a probability $1/q$. That is, anyone else (even the original signer and the receiver) can forge the proxy blind signature successfully with a probability $1/q$.

Identifiability: The proxy blind signature (m, m_w, s, e^*, r_o) contains the warrant m_w . Moreover, in the verification equation $y_{pr} = y_o y_p r_o h(m_w/r_o)$ which includes the original signer O' 's public key y_o and the proxy signer P' 's public key y_p . Hence, anyone can determine the identity of the corresponding proxy signer from a proxy signature.

Verifiability: The proposed scheme satisfies the property of verifiability. The verifier can verify the proxy blind signature by checking:

$$e^* = (h(s y_{pr}^{-e^*} \text{ mod } p // m)) \text{ (mod } q)$$

holds. This is because:

$$\begin{aligned} & s y_{pr}^{-e^*} \text{ mod } p \\ &= g^{s+u} r_o v h(m_w/r_o) y_{pr}^{-e^*} \text{ mod } p \\ &= g^{k+e s_{pr}+u} r_o v h(m_w/r_o) y_{pr}^{-e^*} \text{ mod } p \\ &= g^{k+e^* s_{pr}-v s_{pr}+u} r_o v h(m_w/r_o) y_{pr}^{-e^*} \text{ mod } p \\ &= g^{k+e^* s_{pr}+u} g^{-v} s_o g^{-v} x_p r_o v h(m_w/r_o) y_{pr}^{-e^*} \text{ mod } p \end{aligned}$$

$$\begin{aligned} &= g^{k+u} g^{e^* s_{pr}} (y_o y_p)^{-v} y_{pr}^{-e^*} \text{ mod } p \\ &= g^{k+u} y_{pr} e^{*(y_o y_p)^{-v}} y_{pr}^{-e^*} \text{ mod } p \\ &= r g u (y_o y_p)^{-v} \text{ mod } p \\ &= r^* \end{aligned}$$

Prevention of misuse: The proposed scheme can prevent proxy key pair misuse because the warrant m_w includes original signer and proxy signer identities information, message type to be signed by the proxy signer, delegation period, etc. With the proxy key, the proxy signer cannot sign messages that have not been authorized by the original signer.

Proxy unlinkability: During generation of the signature (m, m_w, s, e^*, r_o) , the proxy signer has the view of transcripts (r, m_w, s^*, e, r_o) . Since (m_w, r_o) are specified by the original signer for all the signatures under the same delegation condition. The proxy unlinkability holds if and only if there is no conjunction between (r, s^*, e) and (m, m_w, s, e^*, r_o) . This is obvious from Equations (5)-(10). The value r is only included in Equation (6) and connected to e^* through Equation (7). For this, one must be able to compute r which is masked with two random numbers. Similarly, e and s^* may be associated with the signature through Equation (8) and (9) respectively. They fail again due to the random numbers. Even they are combined, the number of unknowns is still more than that of the equations. So, the proposed scheme provides indeed the proxy blindness property.

5. Proposed Proxy Blind Signature Scheme based on ECDLP

In this section, we present an ECDLP based proxy blind signature scheme. Elliptic curve cryptosystem is known to provide security equal in level to the discrete logarithm problem (DLP); it also had lower computation overhead and smaller key size. Being applied to the ECC, the proposed scheme reaches high security and efficiency.

The use of Elliptic Curve Cryptography (ECC) was initially suggested by Neal Koblitz [15] and Victor S. Miller [16] and after that many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite fields have some advantages.

For our purposes, an elliptic curve E is a set of points $(x; y)$ with coordinates x and y lying in the field F_q and satisfying a certain cubic equation $y^2 = x^3 + ax + b$ (where $4a^3 + 27b^2 \neq 0$). Let P a point with large prime order n which generates the whole

additive group of E . In other words, F_q has a very large character.

The entities involved are still the same three parties as in the first scheme. The original signee O and proxy signee P have their respective key pair $(x_o; Y_o)$ and $(x_p; Y_p)$, where $x_o; y_o$ are secret keys, $Y_o; Y_p$ are public keys. The scheme is constructed as follows. We make conventions that lowercases denote the elements in F_q and capital letters denote the points in the curve E . The proposed signature scheme is explained below.

3.1 Proxy Delegation Phase

Original signer O selects random number $k_o \in_R Z_q^*$ and computes:

$$R_o = k_o B \quad (12)$$

$$r_o = x(R_o) \quad (13)$$

$$s_o = x_o + k_o h(m_w // r_o) \pmod{q} \quad (14)$$

O sends (r_o, s_o, R_o) along with the warrant m_w to the proxy signer. And then proxy signer checks:

$$R_o h(m_w // r_o) = s_o B - Y_o \pmod{p} \quad (15)$$

If it is correct, P accepts it and computes proxy signature secret key s_{pr} as follow:

$$s_{pr} = s_o + x_p \pmod{q} \quad (16)$$

Note: responding proxy public key $Y_{pr} = Y_o Y_p R_o h(m_w // r_o) = B s_{pr} \pmod{p}$

3.2 Blind Signing Phase

Proxy signer P selects random number $k \in_R Z_q^*$ and computes:

$$T = kB \quad (17)$$

and then sends (r_o, T) to signature asker A . To obtain the blind signature of message m , original signer A randomly choose two random numbers $u, v \in_R Z_q^*$ and computes:

$$r^* = x(T + uB - vY_o - vY_p) \pmod{p} \quad (18)$$

$$e^* = h(r^* // m) \pmod{q} \quad (19)$$

$$e = e^* - v \pmod{q} \quad (20)$$

If $r^* = 0$ then A has to select new tuple (u, v) . Otherwise A sends e to P . After receiving e proxy signer P computes:

$$s^* = k + e s_{pr} \pmod{q} \quad (21)$$

and sends the sign message s^* to A . After blind signing finish, signature asker A extract the signature as follows :

While receiving s^* , A computes:

$$s = B(s^* + u) + v R_o h(m_w // r_o) \quad (22)$$

Finally the signature of message m is (m, m_w, s, e^*, r_o) .

3.3 Verification Phase

The recipient of the signature can verify the proxy blind signature by checking whether

$$e^* = h(x(s - e^* Y_{pr} \pmod{p}) // m) \pmod{q} \quad (23)$$

Where $Y_{pr} = Y_o Y_p R_o h(m_w // r_o)$

Proof:

$$\begin{aligned} & s - e^* Y_{pr} \\ &= B(s^* + u) + v R_o h(m_w // r_o) - (e + v) Y_{pr} \\ &= B(s^* + u) + v R_o h(m_w // r_o) - e Y_{pr} - v Y_{pr} \\ &= B(s^* + u) + v R_o h(m_w // r_o) - e B s_{pr} - v B s_{pr} \\ &= B(s^* + u - e s_{pr}) - v B (s_{pr} - k_o h(m_w // r_o)) \\ &= B(k + u) - v B (s_{pr} - s_o + x_o) \\ &= kB + uB - vB (s_o + x_p - s_o + x_o) \\ &= T + uB - vY_o - vY_p \end{aligned}$$

If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects.

The security of the scheme is strongly related to the security of the first scheme. Furthermore, because ECDLP is much more difficult than DLP, the scheme has stronger security property.

6. Performance Evaluation

The comparison of computational cost of the proposed DLP based scheme and other DLP based schemes is given in Table 1.

	Scheme [13]	Scheme [14]	Our Scheme
Delegation	$3E+2M+2H$	$3E+2M+2H$	$3E+2M+2H$
Signing	$5E+6M+2H$	$5E+4M+2H$	$3E+4M+1H$
Verification	$3E+3M+2H$	$2E+3M+2H$	$2E+3M+2H$
Overall Process costs	$11T+11M+6H$	$10E+9M+6H$	$8E+9M+5H$

Table 1: Comparison of computational cost of DLP based scheme

In this table, E and M denote the running of modulo exponential and multiplication operations, respectively. H denotes the once running of hash operations. The modulo-additions are omitted due to its high performance.

Table 2 compares the equivalent security level for some commonly considered key sizes for DLP and ECDLP method.

Security Level	DLP	ECDLP
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Table 2: Comparable key sizes

ECDLP method requires lower key for higher security level. The performance comparison of

the overall process of DLP based schemes and ECDLP based scheme is presents in figure 1.

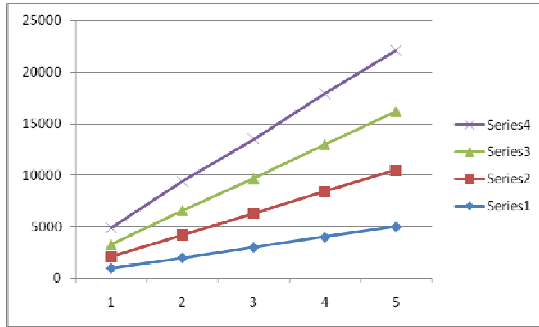


Figure 1: Comparison of the overall process with previous schemes

7. System Parameters and Notations

Throughout this paper, we used the following notations and parameters to explain and analyze the scheme.

O	the original signer
P	the proxy signer
A	the signature asker
p, q	two large prime numbers with $q (p-1)$
x_u	secret key of user u
y_u	public key of user u , $y_u = gx_u \bmod p$
B	base point, $B \in E$
Y_u	public key of user u , $Y_u = x_u B$
$x(Q)$	x coordinate of point Q
m_w	the designated proxy warrant which contains the identities information of the original signer and the proxy signer, message type to be signed by the proxy signer, the delegation limits of authority, valid periods of delegation, etc.
g	generator of order q in Z_p^*
$h(\cdot)$	a secure one-way hash function
//	the concatenation of strings
$O \rightarrow P$	O sends message to P

8. Conclusion

In this paper, we proposed two secure proxy blind signature schemes based on DLP and ECDLP. The schemes satisfy the required secure properties of both proxy signature and the blind signature. Our proposed scheme has less computational cost when comparing with previous schemes. The future work is to design more effective proxy blind signature schemes which provably secure in the standard model.

References

- [1] D. Chaum, "Blind Signature Systems", *Proceedings of Crypto'83*, Plenum, pp.153.
- [2] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its application", *Australasian Conference on Information Security and Privacy (ACISP'2001)*, LNCS2119, Springer-Verlag, Sydney, 2001, pp.603-608.
- [3] W. D. Lin, and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme", *Proc. of Int'l Conference on Chinese Language Computing*, 2000, pp.273-277.
- [4] Z. W. Tan, Z. J. Liu, and C. M. Tang, "A proxy blind signature scheme based on DLP", *Journal of Software*, Vol14, No11, 2003, pp.1931-1935.
- [5] M. Mambo & K. Usuda and E. Okamoto, "Proxy Signatures for delegating signing operation", *Proc. 3rd ACM Conference on Computer and communications Security*, ACM Press, 1996. pp.48-57.
- [6] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages", *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, (9), pp.1338-1354.
- [7] K. Zhang, "Threshold Proxy signature schemes", *1997 Information Security Workshop*, Japan, 1997, pp.191-197.
- [8] S. Kim, S. Park and D. Won, "Proxy signature. *Information and Communication Security*", LNCS, Vol. 1334, Springer-Verlag, 1997, pp.223-232.
- [9] S. Lal, and A. K. Awasthi, "Proxy blind signature scheme", <http://eprint.iacr.org/2003/072.pdf>.
- [10] S. H. Wang, G. L. Wang, F. Bao, and J. Wang, "Cryptanalysis of a proxy blind signature scheme based on DLP", *Journal of Software*, Vol. 16, No. 5, 2005, pp. 911-915.
- [11] Q. S. Xue, and Z. F. Cao, "A new proxy blind signature scheme with warrant", *IEEE Conference on Cybernetics and Intelligent Systems (CIS and RAM 2004)*, Singapore, 2004, pp.1385-1390.
- [12] H. M. Sun, B. T. Hsieh, and S. M. Tseng, "On the security of some proxy signature schemes", *Journal of System and Software*, Vol. 74, 2005, pp.297-302.
- [13] J.G. Li, and S. H. Wang, "New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key", *International Journal of Network Security*, Vol.4, No.2, 2007, pp.193-200.
- [14] Xuan Yang, Zhaoping Yu, "Efficient Proxy Blind Signature Scheme based on DLP", *International Conference on Embedded Software and Systems (ICCESS2008)*.
- [15] Koblitz N., *Elliptic Curve Cryptosystems*, *Mathematics of Computation*, 48, pp.203-209, 1987.
- [16] Miller V., *Uses of Elliptic Curve in Cryptography*, *Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences, 218*, Springer - erlag, 1986, pp.417-426.