Malaya J. Mat. 2(3)(2014) 228–235

Malaya
Journal of
Matematik
www.malayajournal.org

MJM
an international journal of mathematical sciences with computer applications...

ISSN : 2319-3786

An improved proxy blind signature scheme based on ECDLP

Manoj Kumar Chande*

Shri Shankaracharya Institute Of Professional Management & Technology, Raipur, 492015, Chhattisgarh, India.

Abstract

In a proxy blind signature scheme, there is an integration of the properties as well as advantages of both signature schemes namely proxy signature and blind signature. The concept of this signature scheme with a salient feature that, it allows a designated person say proxy signer to sign on behalf of original signer, in such a way that he/she neither has any idea about the content of the message, nor he/she can make a linkage between the signature and the identity of the requester. Therefore, it is very suitable and easily adoptable for electronic commerce, e-cash applications. Recently, Pradhan and Mohapatra et al.'s claims that their proposed signature scheme satisfies all the properties mandatory for a proxy blind signature scheme. Unfortunately, their scheme fails to fulfil the unlinkability property. To overcome with this weakness, an improved proxy blind signature scheme is presented with the same intractable problem ECDLP. The analysis shows that the new scheme resolves the problem in the former scheme and meets all the aspects of security features needed by proxy blind signature scheme. The analytic results prove that the new scheme is more secure and practicable.

Keywords: Digital Signature, Discrete Logarithm Problem, Forward Security, Proxy Blind Signature.

2010 MSC: 94A60.

1 Introduction

David Chaum [1], presented the concept of blind signature in 1983, which allows the signature requester to have a given message signed by the signer without revealing any information about the message or its signature. Firstly, in the year 1996, Mambo [2, 3], introduced the concept of proxy signatures and proposed several constructions. It allows an original signer to delegate his signing power to a designated person, called the proxy signer, who has the power to act on behalf of the original signer. Proxy blind signature is an important extension of basic proxy signature; it can be widely used in many practical applications.

The first proxy blind signature scheme was introduced by Lin and Jan [4]. Later, there are two new schemes have been proposed, one is Tan's scheme [5], using schnorr's blind signature scheme based on discrete logarithm problem (DLP) and elliptic curve discrete logarithm problem (ECDLP) respectively. The other one is Lal et al.'s scheme [6], which is based on Mambo [2, 3], proxy signature scheme. Afterwards, Wang and Wang [7], proposed a proxy blind signature scheme based on ECDLP in 2005. However, Yang and Yu [8], proved that Wang and Wang's scheme did not meet the security properties and proposed an improved proxy blind signature scheme in 2008, but their scheme does not satisfy the unforgeabilty property. The proxy blind signature scheme focuses on both privacy and authentication, it should meet the following security properties -

Distinguishability: The normal signature made by the original signer, and the proxy blind signature made by the proxy signer both are distinguishable.

Identifiability: Anybody can confirm the identities of the original signer and the proxy signer.

E-mail addresses: manojkumarchande@gmail.com (Manoj Kumar Chande) .

Prevention of misuse: The proxy key pair should be used only for creating a proxy signature, which conforms to delegation information.

Nonrepudiation: The original signer and the proxy signer both cannot later falsely claim that they have not performed the signing procedures.

Unforgeability: No one, other than the proxy signer, can produce a valid proxy blind signature.

Unlinkability: The proxy signer or the original signer unable to link the relevance between the blinded message he signed and the revealed signature.

Verifiability: Any arbitrary verifier can be able to verify the proxy blind signature correctly.

Recently, Pradhan and Mohapatra [9], also proposed a new proxy blind signature scheme based on ECDLP. They claim that their scheme is secure and satisfy all the required properties. Unfortunately, their scheme cannot hold the unlinkability property. In this paper the scheme of Pradhan and Mohapatra [9], is improved in such a way, that the presented signature scheme fulfill the unlinkability property.

2 Preliminaries

2.1 Elliptic curve cryptography

The modern-day elliptic curve cryptography (ECC) begins with Koblitz [10] and Miller [11], they provide attractive alternative cryptosystem independently, because its security is based on ECDLP, and it is more efficient as compared with the traditional exponential cryptosystem like RSA [12] and ElGamal [13]. ECC operates over a group of points on an elliptic curve and offers a level of security comparable to classical cryptosystems that uses much larger key's. ECC offers the same security level with a shorter key's [14]. Therefore, the applications that use ECC for such devices will require fewer processor loops, less memory size, smaller key lengths, and less power consumption when compared with the applications using other public key cryptosystem algorithms. With growing potential in e-commerce, ECC systems will be considered to be an important alternative solution to ensure robust security.

2.2 Elliptic curve over finite galois field F_q

Let $q \geq 3$ be any prime number and $a, b \in F_q$, such that $4a^3 + 27b^2 \neq 0$ in F_q, this condition ensures that the defined elliptic curve has no multiple roots of unity. An elliptic curve $E(F_q)$, defined by the parameters a and b is the set of all solutions $(x, y) \in F_q$, to the equation $y^2 = x^3 + ax + b$. These points (x, y) together with an extra point at infinity, form an abelian group.

2.3 Addition law for points on elliptic curve

1. Point of identity - The point O is said to be the point of identity if,
$$P + O = O + P = P, \forall P \in E(F_q).$$
2. Negation of a point - Let a point $P(x, y) \in E(F_q)$, then any point with coordinate values $(x, -y)$ is said to be negation of P. The negation of point P is denoted by $-P$. This is because, their sum gives identity element, particularly $(x, y) + (x, -y) = O$.
3. Addition of points - Let $P(x_1, y_1)$, $Q(x_2, y_2) \in E(F_q)$, then $P + Q = R \in E(F_q)$ and coordinate (x_3, y_3) of R is given by
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$
$$where\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

4. Doubling of point - Let us take a point $P(x_1, y_1) \in E(F_q)$, where $P \neq -P$, then $P + P = 2P = (x_3, y_3)$, and coordinate values (x_3, y_3) are obtained as follows

$$x_3 = (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1$$
$$y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1 \ .$$

2.4 Elliptic curve discrete logarithm problem (ECDLP)

The security of elliptic curve cryptosystem relies on the intractability of ECDLP. Let us consider an elliptic curve $E(F_q)$ over a finite field and a point P of order n. For an element Q $(Q \neq P)$, the problem is to find an integer d such that $Q = dP$, where $1 \leq d \leq n - 1$. The number $d = log_P Q$, is called the discrete logarithm of Q to the base P.

3 Review of Pradhan and Mohaptra's proxy blind signature scheme

In this section, Pradhan and Mohapatra's [9], efficient proxy blind signature scheme based on ECDLP given in detail. The proposed scheme is divided into five phases: (1) System parameters, (2) Proxy delegation, (3) Blind signing, (4) Signature extraction and (5) Signature verification.

(1) **System Parameters and Notations**

U_o – Original Signer
U_p – Proxy Signer
U_r – Signature Requester
B – Base Point
$h(.)$ – Hash Function
x_o – Private key of Original Signer
y_o – Public key of Original Signer, $y_o = x_o B$
x_p – Private key of proxy signer
y_p – Public key of proxy signer, $y_p = x_p B$
m_w – Warrant, contains the identity's information of the original signer and the proxy signer, validation periods of delegation, limits of authority.

(2) **Proxy Delegation**

The proxy signing key pair (S_{pr}, y_{pr}) is generated as follows:

- Original Signer U_o, randomly chooses k_o, where $(1 < k_o < n)$ and computes

$$R_o = k_o B = (x_{R_o}, y_{R_o})$$
$$r_o = x_{R_o} \mod n$$
$$s_o = x_o + k_o h(m_w \| r_o) \mod n$$

- Now U_o, sends (R_o, s_o, m_w) to the proxy signer U_p, through a secure channel.

- Then U_p checks,

$$s_o B = R_o h(m_w \| r_o) + y_o$$

If it is correct, U_p accepts it, and computes the proxy signer's secret key

$$S_{pr} = x_p + s_o$$

and the corresponding proxy public key is

$$y_{pr} = y_o + y_p + R_o h(m_w \| r_o) = BS_{pr}$$

(3) **Blind Signing**

- Proxy signer U_p, select a number k_p randomly, such that $1 < k_p < n$ and compute

$$R_p = k_p B = (x_{R_p}, y_{R_p})$$
$$r_p = (R_p)_x$$

and then send (R_o, R_p, m_w), to signature requester U_r.

- Signature requester U_r randomly select three numbers a, b, c and compute

$$r = R_p + bB - y_{pr}(a + c) \mod n$$

provided $r \neq 0$, otherwise select a, b, c again. Now signature requester U_r computes

$$e^* = h(r\|m)$$
$$e = e^* - c - a \tag{3.1}$$

and sends e to the proxy signer U_p.

- After receiving e, U_p computes

$$S' = eS_{pr} + k_p$$

and send S' to receiver.

(4) **Signature Extraction**

After receiving S', the receiver U_r computes

$$S = S' + b \tag{3.2}$$

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

(5) **Signature Verification**

The recipient of proxy blind signature verifies (m_w, r_o, m, e^*, S), by checking

$$e^* = h((SB - e^* y_{pr})\|m) \tag{3.3}$$

if it is true, then the proxy blind signature is valid one else reject it.

4 Absence of unlinkability in Pradhan and Mohapatra's scheme

In Pradhan and Mohapatra's scheme, the signature requester U_r, uses three blinding factor a, b and c. The signature requester U_r, verify the proxy blind signature (m_w, r_o, m, e^*, S), and after this the signature is made open by the requester. The proxy signer uses his signing data (S'_i, e_i, R_{p_i}), which he stores purposely, to find link between proxy blind signatures and his signed messages. Using stored records, he can find one of the blinding factor b from the equation (3.2), as $b = S - S'_i$. It is difficult to find the rest of the blind factors a and c separately, so he find sum of the blinding factors a and c from the equation (3.1). Let the sum of the blinding factors a and c is, $a + c = e^* - e = \alpha$, so with this sum α and previously calculated blinding factor b, proxy signer compute

$$\bar{R} = SB - e^* y_{pr} \tag{4.1}$$

Finally, the proxy signer can check the equation

$$\bar{R} = R_{p_i} + bB - y_{pr}\,\alpha \tag{4.2}$$

if the values from equations (4.1) and (4.2) are same then, the proxy signer is able to find linkage between the proxy blind signature and his signed blind message. This shows that Pradhan and Mohapatra's scheme is insecure, because there is absence of unlinkability.

5 Improved proxy blind signature based on ECDLP

In this section the proposed improved proxy blind signature is given. The system parameters and notations are same as used in Pradhan and Mohapatra [9].

(1) **Proxy Delegation**

- The original signer U_o , randomly chooses $1 < k_o < n$, and computes

$$\begin{aligned} R_o &= k_o B = (x_1, y_1) \\ r_o &= x_1 \bmod n \\ s_o &= x_o + k_o h(m_w \| r_o) \end{aligned}$$

- The original signer U_o , sends (R_o, s_o, m_w), to the proxy signer U_p , through secure manner.

- When the proxy signer U_p , receives (R_o, s_o, m_w), from the original signer, he checks the following equation

$$s_o B = R_o h(m_w \| r_o) + y_o$$

If this equation holds, the proxy signer accepts the proxy delegation, and computes the proxy secret key as

$$s_{pr} = x_p + s_o \bmod n$$

and the corresponding proxy public key is

$$y_{pr} = y_o + y_p + R_o h(m_w \| r_o) \bmod n$$

(2) **Blind Signing**

- The proxy signer U_p randomly chooses $1 < k_p < n$ and computes $R_p = k_p = (x_2, y_2)$ and $r_p = x_2$ mod n and sends (R_o, R_p, m_w) to the requester.

- The requester U_r, randomly chooses three blinding factors a, b and c, then he computes

$$\bar{R} = aR_p + bB + cy_{pr}$$

If $\bar{R} = O$, then the requester must attempt other combinations of (a, b, c) until $\bar{R} \neq O$. The requester then computes

$$e^* = h(\bar{R} \| m) \bmod n$$

and

$$e = a^{-1}(e^* + c) \bmod n$$

and sends the blind message e to the proxy signer.

- After receiving e, the proxy signer computes

$$S'' = es_{pr} + k_p \bmod n$$

and sends S'' back to the requester.

- The requester computes

$$S = S''a + b \bmod n$$

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

(3) **Verification**

The verifier verifies the validity of the proxy blind signature by checking the following equation

$$e^* = h((SB - e^* y_{pr}) \| m) \tag{5.1}$$

If this equation holds then only the signature is valid otherwise invalid.

6 Security analysis of the proposed scheme

In this section, it is shown that the presented improved proxy blind signature scheme satisfies the security requirements according to the definitions in [9].

(a) **Distinguishbility**

The warrant m_w, is one of the component of the presented proxy blind signature (m_w, r_o, m, e^*, S), so anyone can distinguish the proxy blind signature from the normal signature.

(b) **Identifiability**

Using the verification equation (5.1), and the content of the warrant m_w, the verifier or other users can determine the identity of the corresponding proxy signer U_p, from the proxy signature.

(c) **Nonrepudiation**

In the presented scheme, since only the proxy signer U_p , know the proxy secret key s_{pr}, so no one can else produce S''. Therefore, the proxy signer U_p, cannot deny having signed the message on behalf of original signer.

(d) **Prevention of Misuse**

The message warrant m_w, is very vital part of proposed proxy blind signature scheme. This m_w, includes information regarding the identity of the original signer U_o, the proxy signer U_p, message type to be signed by the proxy signer, and delegation period, etc. Using the proxy key, the proxy signer U_p cannot sign messages that have not been authorized by the original signer. In this way the misuse of key's of original signer and proxy signer is prevented.

(e) **Unforgeability**

If an adversary wants to forge a valid proxy blind signature $(m_w, r_o, \bar{m}, \bar{e}, \bar{S})$, such that it can pass the verification equation $\bar{e} = h((\bar{S}B - \bar{e}y_{pr}) \| \bar{m})$, the adversary has to solve $\bar{S}$. It is difficult to do that because he has to solve the elliptic curve discrete logarithm problem (ECDLP) which is assumed to be infeasible.

(f) **Unlinkability**

Suppose that the proxy signer records all messages he signed (S_i'', e_i, R_{p_i}). After the proxy, blind signature (m_w, r_o, m, e^*, S), is revealed in the public by the requester, the proxy signer still unable to find the blinding factor a, b and c by computing the following equation:

$$\begin{aligned} e_i &= a^{-1}(e^* + c) \mod n \\ S &= S_i'' a + b \mod n \end{aligned}$$

Thus, he cannot check if the equation $\tilde{R} = aR_{p_i} + bB + cy_{pr}$, holds, meaning the proxy signer unable to trace the proxy blind signature with the corresponding signature transcript.

(g) **Verifiability**

The verifier U_r, can verify the proxy blind signature by checking the equation (5.1). The correctness of the proxy blind signature is obtained as follows

$$\begin{aligned} SB - e^* y_{pr} &= (S'' a + b)B - e^* y_{pr} \\ &= (es_{pr} + k_p)aB + bB - e^* y_{pr} \\ &= es_{pr}aB + k_p aB + bB - e^* y_{pr} \\ &= a^{-1}(e^* + c)ay_{pr} + aR_p + bB - e^* y_{pr} \\ &= e^* y_{pr} + cy_{pr} + aR_p + bB - e^* y_{pr} \\ &= aR_p + bB + cy_{pr} \\ &= \bar{R} \end{aligned}$$

In summary, it is shown that the construction based on ECDLP is secure because, it can achieve the unlinkability property. Hence the proposed scheme satisfies all the security requirements of the proxy blind signature.

7 Conclusion

In this article, a linkability attack mounted on Pradhan and Mohapatra's proxy blind signature scheme, and it is demonstrated that how their scheme is insecure due to the absence of unlinkability property. This proposed proxy blind signature scheme holds all the security properties of both proxy and blind signature scheme. The security of the proposed schemes is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP).

References

[1] David Chaum, Blind signature for untraceable payments, *Advances in Cryptology, proceeding of CRYPTO'82, Springer-Verlag, New York*, 199–203, 1983.

[2] M. Mambo, K. Usuda, E. Okamoto, Proxy signatures: delegation of the power to sign message, *IEICE Transactions on Fundamentals*, E79-A(9)(1996), 1338–1354.

[3] M. Mambo, K. Usuda, and E. Okamoto, Proxy signatures for delegating signing operation, *In: Proceeding of 3rd ACM Conference on Computer and Communications Security (CCS'96)*, 48–57, ACM Press, (1996).

[4] W. D. Lin and J.K. Jan, A security personal learning tools using a proxy blind signature scheme, *Proccedings of International Conference on Chinese Language Computing*, Illinois, USA, July 2000, 273–277.

[5] Z. Tan, Z. Liu, C. Tang, Digital proxy blind signature schemes based on DLP and ECDLP, *MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing*, 21, 212–217, (2002).

[6] A.K. Awasthi and S. Lal, Proxy blind signature scheme, *Journal of Information Science and Engineering, 2003, Cryptology ePrint Archive*, Report 2003/072, Available at $< http://eprint.iacr.org >$.

[7] H. Y. Wang and R. C. Wang, A proxy blind signature scheme based on ECDLP, *Chinese Journal of Electronics*, 14(2)(2005), 281–284.

[8] X. Yang and Z. Yu, Security Analysis of a proxy blind signature scheme based on ECDLP, *in Proceeding of* 4th *International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*, Oct. 2008, 1–4.

[9] S. Pradhan and R. K. Mohapatra, Proxy blind signature scheme based on ECDLP, *International Journal of Engineering Science & Technology*, 3(3)(2011), 2244–2248.

[10] N. Koblitz, Elliptic Curve Cryptosystems, *Math. Comp.*, 48(1987), 203–209.

[11] V. S. Miller, Use of elliptic curves in cryptography. *In Advances in Cryptology-CRYPTO'85, Santa Barbara, CA, 1985, Lecture Notes in Computer Science, 218, Springer-Verlag, Berlin*, 417–426, 1986.

[12] R.L. Rivest, A. Shamir and L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* (2)(21)(1978), 120–126.

[13] T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, 31(1985), 469–472.

[14] A. Lenstra, E. Verhuel, Selecting cryptographic key sizes, *Journal of Cryptography*, 14(2001), 255–293.

Received: January 19, 2013; *Accepted*: February 16, 2013

UNIVERSITY PRESS

Website: http://www.malayajournal.org/