Security Analysis and Enhanced Construction on ECDLP-Based Proxy Blind Signature Scheme

Chih-Hung Wang and Meng-Zhe Liao

***Abstract*—Nowadays, the proxy blind signature is an important issue in E-commerce system. In the proxy blind signature scheme, the delegation relationship can be established between the original signer and the proxy signer. That means an original signer, due to the special reasons, delegates his signing capability to a proxy signer who can thus sign a message on behalf of the original signer. The blindness property indicates that the proxy signer does not know the content of his signing message. In the past years, many researchers have proposed proxy blind signature schemes based on DLP (Discrete Logarithm Problem) and ECDLP (Elliptic Curve DLP). This paper demonstrates that Alghazzawi *et al*.'s and Pradhan-Mohapatra's proxy blind signature schemes based on ECDLP are insecure because both of them do not meet the unlinkability property. Therefore, we present an enhanced construction based on the ECDLP which can satisfy all security requirements of the proxy blind signature.**

***Index Terms*—Proxy blind signature, discrete logarithm problem, elliptic curve, cryptography, network security.**

I. Introduction

In 1996, Mambo *et al.* [1] first proposed the concept of proxy signature. In a proxy signature scheme, an original signer delegates his signing capability to a person named the proxy signer, who can signs the message or document on behalf of the original signer. Moreover the concept of blind signature was proposed by Chaum [2] in 1982. In a blind signature scheme, the signer cannot know the content of the message, and even the signature is revealed by the requester later, the signer still cannot link the relationship between the blind message he recorded and the blind signature.

Proxy blind signature was first proposed by Lin and Jan [3] in 2000. It combines the concept of the proxy signature and the blind signature. The proxy blind signature scheme is useful and practical in the topics of the e-commerce, such as e-voting and e-cash schemes. Since the proxy blind signature scheme focuses on both privacy and authentication, it should meet the following security properties [4]:

1) Verifiability: the proxy blind signature can be correctly verified by the arbitrary verifier.
2) Unforgeability: no one, except for the proxy signer, can produce a valid proxy blind signature.
3) Distinguishability: Both the normal signature made by the original signer and the proxy blind signature made by the proxy signer are distinguishable.
4) Identifiability: anyone can confirm the identities of the original signer and the proxy signer.
5) Nonrepudiation: Both the original signer and the proxy signer cannot later falsely claim that they have not performed the signing procedures.
6) Unlinkability: After the requester revealing the unblinded version signature for the verification, the proxy signer (or the original signer) unable to link the relevance between the blinded message he signed and the revealed signature.
7) Prevention of misuse: The proxy key pair should be used only for creating proxy signature, which conforms to delegation information.

Elliptic curve cryptography (ECC), proposed by Koblitz [5] and Miller [6] in 1985, is an important mathematical technique in public key cryptosystem. The key size of ECC is much smaller than other cryptosystems like RSA encryption or Diffie-Hellman key exchange scheme. Since the Elliptic Curve Discrete Logarithm Problem cannot be solved by the subexponential time algorithm, the strength-per-key-bit in elliptic curve systems is substantially greater than one in conventional discrete logarithm systems.

The security of our system is based on ECDLP. The main advantage of ECC is that it provides the same security level with smaller key size. In 2002, by applying Schnorr blind signature, Tan *et al*. [7] proposed a new proxy blind signature schemes based on DLP and ECDLP. Afterwards, Wang and Wang [8] proposed a proxy blind signature scheme based on ECDLP in 2005. However, Yang and Yu [9] proved that Wang and Wang's scheme did not meet the security properties and proposed an improved proxy blind signature scheme in 2008. Nevertheless, their scheme does not satisfy the unforgeabilty property. In 2009, Qi and Wang [10] proposed a proxy blind signature scheme based on Factoring and ECDLP, but their scheme is still insecure since it cannot meet the unforgeability and unlinkability properties. Later Pradhan-Mohapatra [4] and Alghazzawi *et al*. [11] also proposed new proxy blind signatures based on ECDLP, and they claimed their schemes are secure and efficient. In this paper, we will show that their schemes are insecure against linkability attacks. Up to now, for our best knowledge, there is no secure and practical proxy blind signature scheme based on ECDLP security assumption. This paper intends to propose a new enhanced construction on it and shows the security evaluation of the proposed scheme.

The rest of the paper is organized as follows. First in Section II we briefly describe the theory of Elliptic Curve. Next we review two proxy blind signature schemes based on

Manuscript received June 1, 2013; revised August 11, 2013. This work was supported in part by the National Science Council under the Grant NSC 102-2219-E-415-001.

Chih-Hung Wang and Meng-Zhe Liao are with the Department of Computer Science and Information Engineering, National Chiayi University, Chiayi City 60004, Taiwan (e-mail: wangch@mail.ncyu.edu.tw, s1000451@mail.ncyu.edu.tw).

ECDLP in Section III. In Section IV, we demonstrate that both schemes listed in Section III are insecure, and also present a new enhanced construction in Section V. Then we show the security analysis of our proposed scheme in Section VI and the performance comparison is shown in Section VII. Finally Section VIII gives the concluding remarks and future works.

II. Elliptic Curves over Finite Field

In Koblitz's article [5], the concepts of elliptic curves are introduced. We simply explain them as follows. The elliptic curve can be represented as the equation:

$$E(F_p): y^2 = x^3 + ax + b \quad (1)$$

where $a, b \in F_p$, and $4a^3 + 27b^2 \neq 0$.

An elliptic curve group consists of the points on the curve and a special point *O*, and elliptic curves are additive groups. Suppose that $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ are two different points on an elliptic curve *E*. Then to add *P* and *Q*, we can obtain the point denoted $R = (x_3, y_3)$ through the following equation:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}, \quad (2)$$

where

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, \text{ if } P \neq Q \\ \lambda = \dfrac{3x_1^2 + a}{2y_1}, \text{ if } P = Q \end{cases}. \quad (3)$$

Moreover, suppose given two known points *P* and *Q*, we want to find a number *k* such that *Q*= *k P*, where *k* is a very large number regarded as the private key, finding the value of *k* is difficult. Therefore, it is called the elliptic curve discrete logarithm problem. The point *Q* can be calculated as the equation:

$$Q = kP = P + P + ... + P \ (k \text{ times}). \quad (4)$$

III. Review of the Recent Two Proxy Blind Signature Schemes

In this section, we review the recent results of the two proxy blind signature schemes based on ECDLP and demonstrate that their schemes are insecure. The followings are the common used mathematical notations.

P : the base point

h, H : secure one way hash functions

n : the order of P

x_o : the secret key of the original signer

y_o : the public key of the original signer ($y_o = x_o P$)

x_p : the secret key of the proxy signer

y_p : the public key of the proxy signer ($y_p = x_p P$)

m : the message to be signed

m_w : the proxy warrant

A. Alghazzawi et al.'s Scheme

The followings are the brief descriptions of Alghazzawi *et al.*'s scheme [11].

1) Proxy delegation stage

1) The original signer randomly chooses k_o ($1 < k_o < n$), and computes $R_o = k_o P = (x_1, y_1)$, $r_o = x_1 \bmod n$ and $s_o = x_o + k_o r_o \bmod n$.
2) The original signer sends (r_o, s_o) to the proxy signer through a secure manner.
3) When the proxy signer receives (r_o, s_o) from the original signer, he checks the following equation:

$$s_o P = y_o + r_o R_o. \quad (5)$$

If the equation holds, the proxy signer accepts the proxy delegation, otherwise he rejects it.

2) Blind signing stage

1) The proxy signer randomly chooses k_p ($1 < k_p < n$) and computes $R_p = k_p P = (x_2, y_2)$ and $r_p = x_2 \bmod n$, and then sends (r_o, r_p) to the requester.
2) The requester randomly chooses two blinding factors *a* and *b*, and then he computes $\tilde{R} = R_p + aP - bs_o P$. If $\tilde{R} = O$, the requester must choose another tuple (*a*, *b*) until $\tilde{R} \neq O$. The requester then computes

$$e^* = h(\tilde{R} \| m) \quad (6)$$

and

$$e = (e^* + b) \bmod n, \quad (7)$$

and sends the blind message *e* to the proxy signer.
3) After receiving *e*, the proxy signer computes $S'' = (k_p - s_o e) \bmod n$ and sends S'' back to the requester.
4) The requester computes

$$S = (S'' + a) \bmod n. \quad (8)$$

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

3) Verification stage

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

$$e^* = h((SP + e^* s_o P) \| m). \quad (9)$$

B. Pradhan and Mohapatra's Scheme

Pradhan and Mohapatra's approach is to select an extra blind factor to make more robust security protection. The followings are the brief description [4].

1) Proxy delegation stage

1) The original signer randomly chooses k_o ($1 < k_o < n$) and computes $R_o = k_o P = (x_1, y_1)$, $r_o = x_1 \bmod n$, and $s_o = x_o + k_o h(m_w \| r_o) \bmod n$.
2) The original signer sends (R_o, s_o, m_w) to the proxy signer through a secure manner.

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

$$s_o P = R_o h(m_w \| r_o) + y_o. \quad (10)$$

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

$$S_{pr} = x_p + s_o \bmod n, \quad (11)$$

and the corresponding proxy public key is

$$Y_{pr} = y_o + y_p + R_o h(m_w \| r_o) = PS_{pr}. \quad (12)$$

2) Blind signing stage

1) The proxy signer randomly chooses k_p $(1< k_p < n)$ and computes $R_p = k_p P = (x_2, y_2)$ and $r_p = x_2 \bmod n$, and then sends (R_o, R_p, m_w) to the requester.
2) The requester randomly chooses three blinding factors *a*, *b* and *c*, and then he computes $\tilde{R} = R_p + bP - Y_{pr}(a+c)$. If $\tilde{R} = O$, the requester must choose another tuple (*a*, *b*, *c*) until $\tilde{R} \neq O$. The requester then computes

$$e^* = h(\tilde{R} \| m) \quad (13)$$

and

$$e = e^* - c - a \bmod n, \quad (14)$$

and sends the blind message *e* to the proxy signer.
3) After receiving *e*, the proxy signer computes $S'' = eS_{pr} + k_p \bmod n$ and sends S'' back to the requester.
4) The requester computes $S = S'' + b \bmod n$.

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

3) Verification stage

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

$$e^* = h((SP - e^* Y_{pr}) \| m). \quad (15)$$

II. The Weaknesses of the Two Schemes

In this section, we demonstrate that both Alghazzawi *et al.*'s and Pradhan-Mohapatra's schemes are insecure since they suffer from the linkability attacks.

A. Analysis of Alghazzawi et al.'s Scheme

Suppose that the proxy signer records all messages he signed (S_i'', e_i, R_{p_i}). After the proxy blind signature (m, e^*, S) is revealed to the public by the requester, the proxy signer can try to find the corresponding signing record by computing the blinding and unblinding equations of their scheme. Refer to (7) and (8), the calculations are shown as follows.

$$b = e_i - e^* \bmod n \quad (16)$$

and

$$a = S - S_i'' \bmod n, \quad (17)$$

where (e^*, S) is the signature that requester revealed, and (e_i, S_i'') is the signing record of the proxy signer. Therefore the proxy signer knows all the parameters. After finding the two blinding factors *a* and *b*, refer to (6) and (9), he can obtain the following equation:

$$\tilde{R} = (SP + e_i^* s_o P). \quad (18)$$

That means the proxy signer gets $\tilde{R}$ from the above equation. Finally, he can check the following equation:

$$\tilde{R} = R_{p_i} + aP - bs_o P. \quad (19)$$

If (19) holds, the proxy signer can link the association between the revealed proxy blind signature and his recording blind message. So Alghazzawi *et al.*'s scheme cannot meet the unlinkability property of proxy blind signature.

B. Analysis of Pradhan and Mohapatra's Scheme

In Pradhan and Mohapatra's scheme, the requester chooses three blinding factor *a*, *b* and *c* .When the proxy blind signature (m_w, r_o, m, e^*, S) is revealed by the requester. The proxy signer uses his signing record (S_i'', e_i, R_{p_i}) to find blinding factors, he can only find *b* but unable to find *a* and *c* from the following equation

$$e_i = e^* - c - a \bmod n \quad (20)$$

and

$$S = S_i'' + b \bmod n. \quad (21)$$

However, he can still find (*a*+*c*) and *b* to compute $\tilde{R} = SP - e^* Y_{pr}$.

Finally the proxy signer can check the equation:

$$\tilde{R} = R_{p_i} + bP - Y_{pr}(a+c) \quad (22)$$

to discover the linkability between the revealed proxy blind signature and his recording blind message. Thus Pradhan and Mohapatra's scheme is also insecure since it is also unable to resist against linkability attack.

III. The Enhanced Construction on the ECDLP-based Proxy Blind Signature Scheme

In this section, we propose an enhanced construction which can meet the security requirements of proxy blind signature (also see Fig. 1).

A. Proxy Delegation Stage

1) The original signer randomly chooses k_o $(1< k_o < n)$ and computes $R_o = k_o P = (x_1, y_1)$, $r_o = x_1 \bmod n$, and $s_o = x_o + k_o H(m_w \| r_o) \bmod n$.
2) The original signer sends (R_o, s_o, m_w) to the proxy signer through a secure manner.
3) When the proxy signer receives (R_o, s_o, m_w) from the original signer, he checks the following equation:

$$s_o P = R_o H(m_w \| r_o) + y_o. \quad (23)$$

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

$$S_{pr} = x_p + s_o \bmod n, \tag{24}$$

and the corresponding proxy public key is

$$Y_{pr} = y_o + y_p + R_o H(m_w \| r_o) = PS_{pr}. \tag{25}$$

B. Blind Signing Stage

1) The proxy signer randomly chooses k_p $(1< k_p < n)$ and computes $R_p = k_p P = (x_2, y_2)$ and $r_p = x_2 \bmod n$, and sends (R_o, R_p, m_w) to the requester.
2) The requester randomly chooses three blinding factors *a*,*b* and *c*, then he computes $\tilde{R} = aR_p + cP - bY_{pr}$.

If $\tilde{R} = O$, the requester must choose another tuple (*a*, *b*, *c*) until $\tilde{R} \neq O$. The requester then computes

$$e^* = h(\tilde{R} \| m) \tag{26}$$

and

$$e = a^{-1}(e^* - b) \bmod n, \tag{27}$$

and sends the blind message *e* to the proxy signer.

3) After receiving *e*, the proxy signer computes $S'' = eS_{pr} + k_p \bmod n$ and sends S'' back to the requester.
4) The requester computes $S = S''a + c \bmod n$.

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

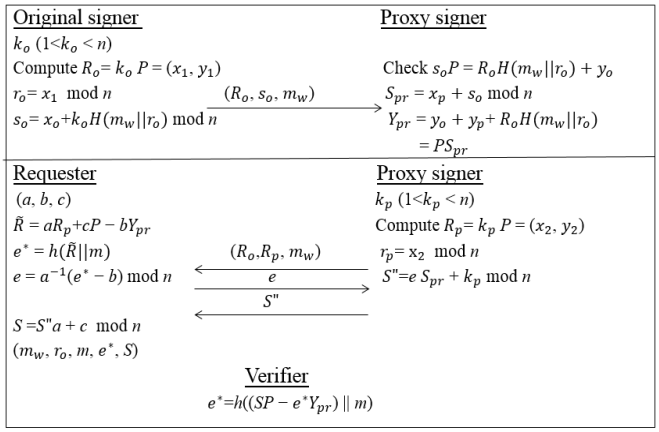

Fig. 1. Our proposed scheme.

C. Verification Stage

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

$$e^* = h((SP - e^* Y_{pr}) \| m). \tag{28}$$

IV. Security Analysis of Our Proposed Scheme

In this section, we demonstrate that our proposed construction method can satisfy the security requirements of the proxy blind signature according to the definitions in [4].

A. Verifiability

The verifier can verify the proxy blind signature by checking the equation of (28).

The correctness of the proxy blind signature is shown as follows.

$$\begin{aligned} & SP - e^* Y_{pr} \\ &= (S''a + c)P - e^* Y_{pr} \\ &= (eS_{pr} + k_p)aP + cP - e^* Y_{pr} \\ &= eS_{pr} aP + k_p aP + cP - eY_{pr} \\ &= aY_{pr} a^{-1}(e^* - b) + aR_p + cP - e^* Y_{pr} \\ &= e^* Y_{pr} - bY_{pr} + aR_p + cP - e^* Y_{pr} \\ &= aR_p + cP - bY_{pr} \\ &= \tilde{R} \end{aligned} \tag{29}$$

B. 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 $\bar{e} = h((\bar{S}P - \bar{e}Y_{pr}) \| \bar{m})$, 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.

C. Distinguishability

Since the proxy blind signature (m_w, r_o, m, e^*, S). of our scheme contains the warrant m_w, we can distinguish the proxy blind signature from the normal signature.

D. Identifiability

According to the warrant m_w and the verification equation, refer to (28), where $Y_{pr} = y_o + y_p + R_o H(m_w \| r_o)$, since y_o and y_p denote the public key of the original signer and the proxy signer, the verifier or other users can determine the identity of the corresponding proxy signer from the proxy signature.

E. Nonrepudiation

In our scheme, since the proxy secret key is denoted by (24) only the proxy signer knows S_{pr} if x_p, the secret key of the proxy signer, has not been compromised.

No one can produce S'' by computing $S'' = eS_{pr} + k_p \bmod n$ except for the proxy signer, therefore he cannot deny having signed the message on behalf of original signer.

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 to the public by the requester, the proxy signer still unable to find the blinding factor *a*, *b* and *c* by computing the following equation:

$$e_i = a^{-1}(e^* - b) \bmod n, \tag{30}$$

$$S = S_i'' a + c \bmod n. \tag{31}$$

TABLE I: COMPARISON OF COMPUTATIONAL COST AND SECURITY WITH OTHER SCHEMES

Schemes	Proxy Delegation	Blind Signing	Verification	Total	Security Problems
Tan *et al.*'s scheme [7]	4M+2A	11M+9A+H	3M+2A+H	18M+13A+2H	Forgery & Linkability
Wang and Wang's scheme [8]	4M+2A	11M+7A+H	3M+3A+H	18M+12A+2H	Forgery & Linkability
Yang and Yu's scheme [9]	4M+3A	8M+4A+H	2M+3A+H	14M+10A+2H	Forgery
Alghazzawi *et al.*'s scheme [11]	3M+2A	4M+3A+H	2M+A+H	9M+6A+2H	Linkability
Pradhan and Mohapatra's scheme [4]	4M+3A+2H	4M+4A+H	2M+H	10M+7A+4H	Linkability
Our scheme	4M+3A+2H	7M+3A+H	2M+H	13M+6A+4H	None

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

G. Prevention of Misuse

Our proposed construction method can avoid proxy key pair misuse since the warrant m_w includes the identity information of the original signer and the proxy signer, 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.

In summary, we show that our construction based on ECDLP is secure because it can achieve the unlinkability property such that our scheme satisfy all the security requirements of the proxy blind signature.

V. PERFORMANCE COMPARISON

In this section, we compare the performance of our proposed scheme and the previous schemes. As shown in Table I, the notations of M and A denote the computational costs for multiplication and addition in elliptic curve (additive group) respectively. Moreover, H denotes the generic hash operation. It can be seen that although our scheme has three multiplications more than the previous schemes of [4] and [11], their schemes are insecure due to the forgery and/or linkability attacks while our proposed scheme can resist against these threats. From the view point of practicality, our scheme can meet the security requirements of proxy blind signature and provide acceptable performance compared with the other schemes.

VI. CONCLUSIONS

In this paper, we have indicated that Alghazzawi *et al.*'s [11] and Pradhan-Mohapatra's [4] signature schemes based on ECDLP are insecure, because they cannot satisfy the unlinkability properties. Thus, we propose an enhanced construction in blind signing stage which can meet the security requirements of the proxy blind signature. In the future work, we are planning to extend this construction technique to apply it on other kinds of digital signature schemes and their corresponding applications.

REFERENCES

[1] M. Mambo, K. Usuda, and E. Okamot, "Proxy signatures: delegation of the power to sign messages," *IEICE Transaction on Fundamentals*, vol. E79-A, no. 9, pp. 1338–1353, 1996.

[2] D. Chaum, "Blind signature for untraceable payments," in *Proc. CRYPTO'82, Advances in Cryptology,* Springer-Verlag, 1983, pp. 199-203.

[3] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," in *Proc. of Intl Conference on Chinese Language Computing*, 2000, pp. 273-277.

[4] S. Pradhan and R. K. Mohapatra, "Proxy blind signature scheme based on ECDLP," *International Journal of Engineering Science & Technology*, vol. 3, issue 3, pp. 2244, 2011.

[5] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.

[6] V. Miller, "Uses of elliptic curves in cryptography," in H. C. Williams, ed., *Advances in Cryptology-CRYPTO 85, Proceedings, Lecture Notes in Computer Science*, Springer-Verlag, no. 218, 1985, pp. 417-426.

[7] Z. Tan, Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," *MM Research Preprints*, no. 21, 2002, pp.212-217.

[8] H. Y. Wang and R. C. Wang, "A proxy blind signature scheme based on ECDLP," *Chinese Journal of Electronics*, vol. 14, no. 2, pp. 281-284, 2005.

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

[10] C. Qi and Y. Wang , "An Improved proxy blind signature scheme based on factoring and ECDLP," in *Proc. International Conference on Computational Intelligence and Software Engineering*, 2009, Dec. 11-13, 2009, pp. 1-4.

[11] D. M. Alghazzawi, T. M. Salim and S. H. Hasan, "A new proxy blind signature scheme based on ECDLP," *IJCSI International Journal of Computer Science Issues*, vol. 8, issue 3, no. 1, May 2011.

Chih-Hung Wang was born in Kaohsiung, Taiwan in 1968. He received the BS degree in Information Science from Tunghi University and MS degree in Information Engineering from National Chung Cheng University, Taiwan in 1991 and 1993, respectively. He received the Ph.D. degree in Information Engineering from National Cheng Kung University, Taiwan in 1998. He is presently an associate professor of Department of Computer Science and Information Engineering, National Chiayi University, Taiwan. His research interests include cryptography, information security and data compression.

Meng-Zhe Liao is presently a master student of Department of Computer Science and Information Engineering, National Chiayi University, Taiwan. His research interests include cryptographic protocols and information security.