An Enhanced Proxy Blind Signature with Two Intractable Problems

Manoj Kumar Chande
Shri Shankaracharya Institute of Professional Management & Technology
Raipur, 492015, Chhattisgarh, India

ABSTRACT

A proxy blind signature scheme is combination of two signature schemes particularly proxy signature and blind signature. In this signature scheme the original signer delegate his/her signing authority to some other entity named proxy signer. The proxy signer signs the documents or messages, but he cannot be able to find any link between the blind signature and the identity of the signature requester. In the open literature the majority of the existing digital signature schemes were developed based on intractability of a single hard problem like integer factoring problem (IFP), discrete logarithm problem (DLP) or elliptic curve discrete logarithm problems (ECDLP). This paper analyzes Qi and Wang et al's scheme, which is based on multiple hard problems namely IFP and ECDLP. But their scheme has security weaknesses and cannot hold some of the basic properties of signature scheme. Improvements are suggested to overcome with these weaknesses, such that the proposed signature scheme satisfies the security standards of a proxy blind signature scheme. The security of the improved scheme is also analyzed, which shows that this signature scheme is more secure than that schemes based on single intractable problem.

General Terms:

Digital Signature Scheme, Elliptic Curve Cryptography.

Keywords:

Blind Signature, Elliptic Curve Discrete Logarithm Problem (ECDLP), Integer Factorization Problem (IFP), Proxy Signature.

1. INTRODUCTION

The first proxy blind signature was proposed by Lin and Jan [1], in the year 2000. It combines the concept of the proxy signature and the blind signature. The proxy blind signature scheme is useful and practical in the field of the e-commerce, e-voting and e-cash schemes. The proxy blind signature scheme focuses on both privacy and authentication, it should satisfy the following security properties:

Distinguishability: The original signature created by original signer and proxy blind signature generated by proxy signer both must be distinguishable.

Identifiability: Anybody can identify the proxy signer easily from his/her proxy signature.

Nonrepudiation: It is not possible for the original signer or the proxy signer, to deny that they have not generated the signature. It means no entity can be able to sign in place of some other entity.

Prevention of misuse: The private and public keys of the proxy signer should be used only to generate proxy signature, which conforms to delegation information. The proxy signer solely responsible in case of any kind of misuse of his/her proxy signature or proxy key's.

Unforgeability: No one other than authorized proxy signer, even the original signer can not create a valid proxy signature for himself/herself.

Unlinkability: After the signature verification, the proxy signer can't able to link blinded message he/she signed with the revealed proxy blind signature.

Verifiability: The receiver or verifier of the signature should be able to verify the proxy signature in the same manner as the verification of the original signature.

Elliptic Curve Cryptosystem (ECC) was introduced by Victor Miller [2] and Neal Koblitz [3], independently in 1985. In this elliptic curve defined over a finite field and the points on elliptic curve form a group. The security of the system is based on ECDLP. The main advantage of ECC is that the key size in ECC, is much smaller than other cryptosystems like RSA encryption [4] and Diffie-Hellman key exchange scheme [5]. Interestingly it provides the same security level and required smaller storage space. Since the ECDLP cannot be solved by the sub-exponential time algorithm, the strength-per-key-bit in elliptic curve systems is substantially greater than one in conventional discrete logarithm systems.

Tan [6], in the year 2002, presented two proxy blind signature schemes. The security of the signature schemes are based on DLP and ECDLP respectively. In 2003, Lal et al. [7], pointed out the security attacks in Tan et al's scheme and suggested a new proxy blind signature scheme based on mambo et al's [8]. In 2005, Wang and Wang [9], presents a proxy blind signature scheme based on ECDLP. Yang et al. [10], proved that Wang and Wang [9], scheme fail to satisfy, strong unllinkability, nonrepudiation, strong unforgeability properties and they proposed an improved proxy blind signature scheme. In the year 2009, Hu [11], pointed that the Yang's [10], proxy blind signature scheme is not secure. There

were security failures against original signer's forgery attack, the universal forgery attack and it also fail to hold the strong identifiability property. To overcome the weaknesses of Yang's scheme Hu [11], gives an improved proxy blind signature scheme based on ECDLP. In the year 2009, Qi and Wang [12], construct a proxy blind signature scheme based on factoring and ECDLP, and claim that their scheme follows all the security properties of both the schemes namely, the blind signature scheme and the proxy signature scheme. This paper analyzes the security of Qi and Wang [12], proxy blind signature scheme. Outcome of the analysis is that this scheme is also insecure against universal forgery attack and does not holds the unlinkability as well as identifiability property. A more secure and efficient signature scheme is proposed by making improvement in signature stage of Qi and Wang [12].

2. MATHEMATICAL BACKGROUND

2.1 Elliptic Curve Over Finite Field

Let $GF(p)$, be a prime field and let $a, b \in GF(p)$ are constant such that $4a^3 + 27b^2 \neq 0$. An elliptic curve $E(a, b)$, over $GF(p)$ is defined as the set of points $(x, y) \in GF(p) * GF(p)$ which satisfy the equation:

$$E(a, b) : y^2 = x^3 + ax + b \, mod \, p$$

together with a special point O, called the point at infinity. This will referred as weierstrass equation for an elliptic curve. The field size p is a large odd prime and the parameter $n = \#E$ is the order of elliptic curve $E(a, b)$, which is equal to the number of points on the elliptic curve. G is a randomly selected element on the elliptic curve $E(a, b)$, which is called as the base point, whose order r is a large prime divisor of n. To understand algebra of elliptic curves and its applications refer the book of Blake, Seroussi and Smart [13].

2.2 Intractable Mathematical Problems

(1) **Elliptic Curve Discrete Logarithm Problem (ECDLP)**
For a group G, the elliptic curve discrete logarithm problem is to find the integer $x \in Z_n^*$, for group generator P and some other point on the curve $Q \in G$, such that Q=xP.

(2) **Integer Factoring Problem (IFP)**
Suppose a large number n is product of two integer p and q. The integer factoring problem is that, if value of n is known, then to find its factors p and q.

3. REVIEW OF SIGNATURE SCHEME PROPOSED BY QI AND WANG

The signature scheme given by Qi and Wang [12], consist of three steps - (I) Proxy Delegation, (II) Blind Signing and (III) Signature Verification.

(1) **Proxy Delegation**

The original signer select two prime numbers p, q and calculate compound value $n = pq$. The original signer A, next computes public and private keys of the scheme and sends the public keys to proxy signer B and keeps private keys secret. The original signer A generates the following system parameters
(i) Selects randomly an integer $\bar{e} \in Z_n$, such that $gcd(\bar{e}, n) = 1$.
(ii) A secret d such that, $\bar{e}d \equiv 1 \; mod \; \phi(n)$.
(iii) Selects randomly an integer $\bar{x}$, such that $0 < \bar{x} < n$.
(iv) A large prime number N which is the order of the elliptic curve cryptosystem, where $\#E(GF(p))$ lies between $p + 1 - 2\sqrt{p}$ and $p + 1 + 2\sqrt{p}$.
(v) A public key $\bar{y} \equiv g^{\bar{x}} \, mod \, p$.
(vi) Randomly chooses $\bar{k}$, such that $1 < \bar{k} < n$.
(vii) Two integer w and u such that $w, u < n$.

Then original signer A publishes the public keys $(\bar{y}, \bar{e})$ and computes
$K \equiv g^{h(m)^w} \, mod \, p$ and $R \equiv g^{h(m)^u} \, mod \, p$
$\hat{s} \equiv (\bar{x}h(m) + Kh(m)^u + Rh(m)^w)^d \, mod \, p$
$\bar{R} = \bar{k}P$ and $\bar{r} = \bar{R}_x$
$\bar{s} = k_A \bar{r} + k \, mod \, n$

Then original signer A sends $(\bar{r}, \bar{s}, \bar{R}, K, R, \hat{s})$ to proxy signer B. Proxy signer B verify whether

$$\bar{R} = \bar{s}P - \bar{r}P_A$$

$$g^{\hat{s}^e} \equiv y^{h(m)} K^R R^K \, mod \, p$$

If these equations hold, B computes $\dot{s} = \bar{s} + k_B \, mod \, n$.

(2) **Blind Signing**

Proxy signer B randomly chooses k, where $1 < k < n$, and computes $T = kP$. Then he/she sends $(\bar{r}, \bar{s}, T)$ to Requester. After this requester randomly chooses a, b, where $1 < a, b < n$,

$$R = T + bP + (-a - b)P_B + (-a)\bar{R} + (-a\bar{r})P_A$$

$$r = R_x$$

$$e = H(r \| m) \, mod \, n$$

$$e^* = e - a - b \tag{1}$$

$$U = (-e + b)R + (-e + b)\bar{r}P_A - eP_A \tag{2}$$

Proxy signer B computes

$$s'' = e^* \dot{s} + k \, mod \, n$$

using e^* and returns s'' to requester. Requester computes

$$s = s'' + b \, mod \, n \tag{3}$$

and the resulting signature is (m, s, e, U).

(3) **Signature Verification**

The signature (m, s, e, U), can be verified by checking whether

$$e = h((sP - eP_B + eP_A + U)_x \, \| \, m) \, mod \, n \tag{4}$$

holds or not. The verification equation follows from

$$R = sP - eP_B + eP_A + U$$

4. THE WEAKNESSES OF QI AND WANG SCHEME

The outcome of security analysis of Qi and Wang [12], is that their scheme is insecure because of some weaknesses which are described as follows:

(1) **Unlinkability of Messages Signed and Proxy Blind Signature**

In signature scheme of Qi and Wang [12], when a signature is verified, the proxy signer can associate the signature with the corresponding signature scheme. Using proxy blind signature tuple (m, s, e, U), the proxy signer B can find its corresponding signing data $(r, R, T, e^*, s^{''})$ by computing a from equation (1), with the help of value of b from equation (3). After this checks the equation (2), if it is valid then, he can link (m, s, e, U) to $(r, R, T, e^*, s^{''})$ correctly.

(2) **Universal Forgery of Proxy Blind Signature**

In signature scheme of Qi and Wang [12], anyone can forge a valid proxy blind signature on any message $\tilde{m}$ he/she select randomly. An adversary (Adv) can forge a valid proxy blind signature of message m as follows:
Adv selects, $\tilde{k}, \tilde{s} \in F_q$, where $1<\tilde{k},\ \tilde{s}< n$ and compute

$$\tilde{R} = (\tilde{k} + \tilde{s})P,\ \ \tilde{r} = \tilde{R}_x$$

$$\tilde{e} = H(\tilde{r} \| \tilde{m})$$

$$\tilde{U} = \tilde{k}P - \tilde{e}P_A + \tilde{e}P_B$$

and obtain the forged proxy blind signature $(\tilde{m}, \tilde{s}, \tilde{e}, \tilde{U})$. This signature is valid and it is because of

$$H((\tilde{s}P - \tilde{e}P_B + \tilde{e}P_A + U)_x \| \tilde{m}) \, mod \, n$$

$$H((\tilde{s}P - \tilde{e}P_B + \tilde{e}P_A - \tilde{e}P_A + \tilde{e}P_B + \tilde{k}P)_x \| \tilde{m}) \, mod \, n$$

$$H(\tilde{R}_x \| \tilde{m}) \, mod \, n = \tilde{e}$$

so in this way the proxy blind signature $(\tilde{m}, \tilde{s}, \tilde{e}, \tilde{U})$ is a forged but valid one.

(3) **Identifiability of Proxy Signer**

In Qi and Wang [12] signature scheme, the proxy blind signature is (m, s, e, U). The signature is verified if equation (4) holds. In this equation of signature verification the public key P_A of original signer and public key P_B of proxy signer appears in the same position. Because of this, identification of proxy signer from the proxy blind signature is difficult. Thus the scheme does not hold identifiability property.

5. ENHANCED PROXY BLIND SIGNATURE WITH TWO INTRACTABLE PROBLEMS

The proposed scheme is also consist of three steps - (1) Proxy Delegation, (2) Blind Signing and (3) Signature Verification. For the proposed signature scheme the following system parameters and notation are used:

Two large prime integers p and q such that $q/p - 1$.
An additive group $Z_p = \{0, 1, 2, ...p - 1\}$.
$g \in Z_p^*$, is of order q.
P is the generator of elliptic curve group of order n.
P_x is the x coordinate of point P on the elliptic curve $E(a, b)$.
Private key of original signer is k_A and pubic key is $P_A = k_A P$.
Private key of proxy signer is k_B and pubic key is $P_B = k_B P$.
$H(.)$ is a collision free cryptographic function.
m, is the message which is to be signed.
Euler-phi function $\phi(.)$.

(1) Proxy Delegation

The original signer A generates the parameters as follows:
(i) Selects $\bar{e} \in Z_p^*$ such that $gcd(\bar{e}, \phi(p-1)) = 1$.
(ii) Chooses d such that $\bar{e}d \equiv 1 \, mod \, \phi(p-1) = 1$.
(iii) Selects $1 < \bar{x} \leq p - 2$, computes $\bar{y} = g^{\bar{x}} \, mod \, p$, and make $(\bar{y}, \bar{e})$ public.
(iv) Chooses $1 < w, u \leq p - 2$, and computes $K = g^{H(m_w)^w} \, mod \, p$, and $R = g^{H(m_w)^u} \, mod \, p$, then $\hat{s} = (\bar{x}H(m_w) + KH(m_w)^u + RH(m_w)^w)^d \, mod \, \phi(p)$,
(v) Select $\bar{k} \in Z_n^*$, computes $\bar{R} = \bar{k}P,\ \bar{r} = \bar{R}_x$.
(vi) Computes $\hat{e} = H(\bar{r} \| m_w)$, and $\bar{s} = k_A \hat{e} + \bar{k} \, mod \, n$.
A sends the delegation parameter $(m_w, \bar{s}, \bar{R}, K, R, \hat{s})$ to B. Proxy signer B checks, whether $\bar{R} = \bar{s}P - \hat{e}P_A$ and $g^{\hat{s}^{\bar{e}}} = (\bar{y})^{H(m_w)} K^R R^K \, mod \, p$. If these equations hold, B computes $s' = \bar{s} + k_B \, mod \, n$.

(2) Blind Signing

Proxy signer B chooses $k \in Z_n^*$ and computes $T = kP$, then he sends $(m_w, \bar{R}, \bar{s}, T)$ to owner C. Owner C chooses $a, b, c \in Z_n^*$ and computes

$$R = aT + b(P_B + \bar{R} + \hat{e}P_A) - cP \tag{5}$$

$$r = R_x$$

$$e = H(r \| m) \, mod \, n$$

$$e^* = a^{-1}(e + b) \, mod \, n \tag{6}$$

and sends e^* to B. Proxy signer B computes $s'' = e^* s' + k \, mod \, n$ and returns s'' to C. Owner C computes

$$s = as'' - c \, mod \, n \tag{7}$$

The resulting proxy blind signature is $(m_w, m, \bar{R}, e, s)$.

(3) Signature Verification

The signature verification equation is

$$e = H((sP - e(P_B + \bar{R} + \hat{e}P_A))_x \| m) \, mod \, n \tag{8}$$

The verification calculation is like

$$e = H((sP - e(P_B + \bar{R} + \hat{e}P_A))_x \| m)$$

$$= H(((as'' - c)P - e(P_B + \bar{R} + \hat{e}P_A))_x \| m)$$

$$= H((a(e^* s' + k)P - cP - e(P_B + \bar{R} + \hat{e}P_A))_x \| m)$$

$$= H((ae^*(\bar{s} + k_B)P + akP - cP - e(P_B + \bar{R} + \hat{e}P_A))_x \| m)$$

$$= H((aa^{-1}(e+b)(P_B + \bar{R} + \hat{e}P_A) + akP - cP - e(P_B + \bar{R} + \hat{e}P_A))_x \| m)$$

$$= H((aT + b(P_B + \bar{R} + \hat{e}P_A) - cP))_x \| m)$$

$$= H(R_x \| m) \, mod \, n = H(r \| m) \, mod \, n = e.$$

6. SECURITY ANALYSIS OF PROPOSED SCHEME

The security analysis of the proposed signature scheme is as follows:

(1) **Distinguishability**

A regular signature does not contains message warrant m_w, while the proposed proxy blind signature contains the message warrant m_w. Public keys of both the original signer and proxy signer with m_w are used to verify the proxy blind signature. Therefore the signature can be distinguish from other regular signatures.

(2) **Identifiability**

The message warrant m_w is used in proposed signature scheme and it is public. The m_w having details about original signer, proxy signer and delegation etc. So with the help of m_w, the original signer and the proxy signer can be easily identified by anyone. As it is appears from the verification equation (8) the public keys P_A, P_B are asymmetrical in position. In this way the identity of proxy signer can be distinguish from proxy blind signature.

(3) **Nonrepudiation**

To generate a valid proxy blind signature, it requires private key k_A, of original signer and k_B, of proxy signer respectively. Because of this reason, the original signer and proxy signer can not deny that they participated in creation of proxy blind signature.

(4) **Prevention of Misuse**

To delegate his signing rights to proxy signer, original signer generate the delegation parameters and sends them to proxy signer. So it is difficult to forge the valid delegation parameters. Proxy signer cannot delegate his rights further to some third person. To do this he will have to provide the proxy private key s' to that person. In addition, warrant m_w contains the limit of delegated signing capability. So in this way the misuse of signature as well as secret parameters is prevented.

(5) **Unforgeability**

The valid proxy signer is the only entity, who is responsible to create a valid proxy blind signature. It is because the proxy private key s' includes the private key k_B of proxy signer. Obtaining k_B, is only feasible, when someone able to solve ECDLP. If any adversary attempt to forge secret keys $(\bar{x}, d)$, then he has to encounter DLP as well as IFP. If there is an adversary Adv, having a valid proxy blind signature $(m_w, m, \bar{R}, e, s)$ and he attempts to forge a valid proxy blind signature on message $\tilde{m}$, other than the original message m. For this the Adv do the following computations:

(i) Adv first compute $\tilde{r} = \tilde{R}_x$ and $\hat{e} = H(\tilde{r} \| m_w) \, mod \, n$.

(ii) Then Adv selects randomly $k'' \in Z_n^*$, and calculate $R = k''P$.

(iii) The Adv compute $r = R_x$, $e' = H(r \| \tilde{m}) \, mod \, n$. If $(m_w, \tilde{m}, \tilde{R}, \tilde{e}, \tilde{s})$ is a valid proxy blind signature, then it must satisfy the verification equation (8). For this the Adv needs to solve

$$\tilde{s}P - \tilde{e}(P_B + \tilde{R} + \hat{e}P_A) = R$$

to find $\tilde{s}$. This is possible only when ECDLP is solvable.

(6) **Unlinkability**

To find linkage between the signature and requester, the proxy signer can store the data which he generate during the signing step. For the proxy blind signature, the proxy unlinkability holds, if and only if there is no conjunction between signing data of proxy signer and proxy blind signature. In proposed signature scheme the signing data (T, e^*, s'') is attached with signature via following equations (5),(6) and 7. If anyone knows the value of R, then by checking equation $e = H(R_x \| m) \, mod \, n$, he can link signing data to the proxy blind signature. But to find unknown constants a, b, c, R, it is difficult for anyone. In this way the scheme holds unlinkability property.

(7) **Verifiability**

The verifier of the signature, can check whether verification equation (8) holds or not. How this signature verification works is already shown.

7. CONCLUSION

In this paper to overcome with security flaws of the proxy blind signature proposed by Qi and Wang, the improvements are being done in signing stage. Due to these modifications, the security flaws like linkability attack, universal forgery and absence of identifiability are removed. Security analysis shows that the proposed scheme provide a better level of security and at the same time fulfill all the properties of an ideal proxy blind signature. To forge the signature scheme, the attacker has to face these dual problems IFP and ECDLP simultaneously, so it is almost infeasible for him to challenge security measures of proposed scheme. In this way the presented scheme is more adoptable in real time applications.

8. REFERENCES

[1] 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, (2000).

[2] V. S. Miller, Use of elliptic curves in cryptography, In Advances in Cryptology-CRYPTO'85, Santa Barbara, CA, 1985, Lecture Notes in Comput. Sci., 218, Springer-Verlag, Berlin, 417–426, (1986).

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

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems Communications, ACM, vol. 21, pp. 120–126, Feb. 1978.

[5] W. Diffie, M. E. Hellman, New directions in cryptography. IEEE Trans. Inform. Theory, 22(6), 644–654, (1976).

[6] Z. Tan, Z. Liu, C. Tang, Digital proxy blind signature schemes based on DLP and ECDLP, MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, No. 21, 212–217, (2002).

[7] S. Lal, and A. K. Awasthi, Proxy Blind Signature Scheme, Cryptology ePrint Archive, Report2003/072. Available at: http://eprint.iacr.org/.

[8] M. Mambo, K. Usuda, E. Okamoto, Proxy signatures: Delegation of the power to sign messages, IEICE Transactions Fundamentals, E79-A(9), 1338–1353, (1996).

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

[10] X. Yang, Z. Yu, Security Analysis of a Proxy Blind Signature Scheme Based on ECDLP, In The 4^{th} International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008), 1–4, (2008).

[11] L. Hu, K. Zheng, Z. Hu and Y. Yang, A Secure Proxy Blind Signature Scheme Based on ECDLP, In 2009 International Conference on Multimedia Information Networking and Security, IEEE (2009).

[12] C. Qi, Y. Wang, An Improved Proxy Blind Signature Scheme Based on Factoring and ECDLP, In Computational Intelligence and Software Engineering, IEEE, 1–4, (2009).

[13] Blake I. F., Seroussi G., Smart N. P., Elliptic curves in cryptography, London Math. Soc. Lecture Notes Ser. 265, Cambridge University Press, (1999).