Security Analysis of Proxy Blind Signature Scheme Based on Factoring and ECDLP

Namita Tiwari and Sahadeo Padhye

Department of Mathematics,
Motilal Nehru National Institute of Technology,
Allahabad-211004, India
{namita.mnnit,sahadeomathrsu}@gmail.com

Abstract. Proxy blind Signature is a digital signature where an original signer delegates his/her signing capability to a proxy signer who performs message signing blindly, on behalf of original signer but he cannot make a linkage between the blind signature and the identity of the message's owner. Recently, Qi et al proposed an improved proxy blind signature scheme based on factoring and elliptic curve discrete log problem (ECDLP). In this paper we show that Qi et al's scheme does not hold the identifiability and unlinkability properties. Moreover, we also point out that their scheme is not secure against universal forgery attack. Furthermore, we propose an improved proxy blind signature scheme to remedy the weaknesses of Qi et al.'s scheme. The security and performance of the improved scheme are also analyzed.

Keywords: Proxy Signature, Blind Signature, Elliptic Curve Discrete-log problem, Integer Factorization.

1 Introduction

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. A lot of researches have been contributed to this field using various cryptographic primitives [8]. However, there are many practical environments where digital signatures do not possess specific requirements, and thereby digital signatures appear in several other forms viz. proxy signatures, blind signatures etc. For example, a manager of the company needs to go on a business trip which does not have very good computer network accesses, he expects to receive his e-mail and has instructed his secretary to respond accordingly. Question is, how a manager gives secretary the power, to sign message for her without giving him, her private key? Proxy signature is the solution of this problem. The concept of proxy signature was firstly introduced by Mambo et al [9]. Proxy signature enables a proxy signer to sign messages, on behalf of an original signer.

On the other hand, blind signature also has its own importance for specific situations and purposes. The notion of blind signature was firstly introduced by

N. Meghanathan et al. (Eds.): CCSIT 2012, Part II, LNICST 85, pp. 100–108, 2012.

David Chaum [2] in 1982. Blind Signature is a signature on a message, signed by another party without having any information about the message. Its name is so, because the message is blind to the signer. Blind signatures are applicable where sender's privacy is important, like: digital cash scheme, electronic voting *etc.*

A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature and blind signature schemes. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. This is a typical untraceable scheme which allows a user to withdraw a valid e-coin from a proxy bank and spend the coin anonymously at a shop. It is very important in electronic cash payment system [1,3,4], anonymous proxy electronic voting *etc.* Proxy blind signature must satisfy the security properties of proxy signature and blind signature.

Distinguishability- The proxy blind signature must be distinguishable from the normal signature.

Verifiability- The verifier should be able to verify the proxy signature in a similar way to the verification of the original signature.

Unforgeability- Only the designated proxy signer can create a valid proxy signature, for the original signer (even the original signer can not do it).

Nonrepudiation- Neither the original signer nor the proxy signer can sign in place of the other party. In other words, they cannot deny their signatures against anyone.

Identifiability- Anyone can determine the identity of the corresponding proxy signer from a proxy signature.

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.

Unlinkability- After proxy blind signature is created, the proxy signer knows neither the message nor the signature associated with the signature scheme.

Elliptic curve cryptography (ECC) is considered as an important topic in public key cryptography. In 1985, Koblitz [6] and Miller [7], independently proposed it using the group of points on an elliptic curve defined over a finite field. The security of the system is based on ECDLP. The main advantage of ECC is that it provides the same security level with smaller key size [11]. Smaller key means less management time and smaller storage, which supplies convenience to realization by software and hardware. In 2002, by applying Schnorr blind signature, Tan et al. [12] presented two proxy blind signature schemes, which are respectively based on discrete logarithm problem (DLP) and ECDLP.

In 2005, Wang et al. [13] proposed a proxy blind signature scheme based on ECDLP. In 2008, Yang et al. [14] proved that Wang et al.'s scheme did not possess the strong nonrepudiation, strong unforgeability and unllinkability properties and proposed an improved proxy blind signature scheme, to remedy the weaknesses of Wang et al.'s scheme. In 2009, Hu et al [5] presented a security analysis on Yang's proxy blind signature scheme [14], and demonstrated that scheme is insecure. It suffers from the original signer's forgery attack and the universal forgery attack. It didn't possess the strong identifiability property in addition. Furthermore, an improved proxy blind signature scheme based on ECDLP was given to overcome the weaknesses of Yang's scheme.

Recently, Qi et al [10] introduced a proxy blind signature scheme based on factoring and ECDLP, which ensures security properties of both the schemes, namely, the blind signature schemes and the proxy signature schemes. In this paper, we analyze the security of Qi et al's proxy blind signature scheme [10] and demonstrate that this scheme is insecure against universal forgery attack. We also show that it does not satisfy the unlinkability requirement and identifiability property. To overcome the weaknesses of Qi et al's scheme [10], we propose an improved proxy blind signature scheme which satisfies all the security requirements for a proxy blind signature. At the same time, the performance of the new scheme is superior to Qi et al's scheme [10].

The rest of this paper is organized as follows. In section 2, we briefly introduce some preliminary works. Brief review of Qi et al's [10], with security analysis is summarized in section 3. Section 4 includes improved scheme with security and comparative analysis. The last section concludes this paper.

2 Preliminaries

2.1 Background of Elliptic Curve Group

The symbol E/F_p denotes an elliptic curve E over a prime finite field F_p, defined by an equation

$$y^2 = x^3 + ax + b,\ a, b \in F_p, \text{ and}$$

discriminant $\Delta = 4a^3 + 27b^2 \neq 0$.

The points on E/F_p together with an extra point O called the point at infinity form a group $G = \{(x, y) : x, y \in F_p, E(x, y) = 0\} \cup \{O\}$.

Let the order of G be n. G is a cyclic additive group under the point addition "$+$" defined as follows: Let $P, Q \in G$, l be the line containing P and Q (tangent line to E/F_p if $P = Q$), and R, the third point of intersection of l with E/F_p. Let $l^{'}$ be the line connecting R and O. Then $P + Q$ is the point such that $l^{'}$ intersects E/F_p at R and O and $P + Q$.

Scalar multiplication over E/F_p can be computed as follows:
$tP = P + P + ... + P(t\ times)$.

2.2 Complexity Assumption

The following problems assumed to be intractable within polynomial time in the proposed scheme.

Elliptic curve discrete logarithm problem (ECDLP)- For $x \in_R {Z_n}^*$ and P the generator of G , given $Q = x.P$ compute x.

Integer Factoring Problem (IFP)- For a given composite integer n, compute prime factors p' and q' such that $n = p'q'$.

3 Brief Review of Qi et al's Scheme

In this section, we present a brief review of the scheme [10], with security analysis. Further, we demonstrate that this scheme is insecure against universal forgery attack. We also show that it does not satisfy the unlinkability and identifiability property.

3.1 Scheme Description

Qi et al's Scheme [10] with notations used in [10], is given below.

Delegation Phase- The original signer initializes the scheme by first generating two modulus: a prime p and a composite $n = p'q'$. The signer A next computes public and secret keys of the scheme and sends the public keys to proxy signer B and keeps secret keys secretly. The original signer A generates the following system parameters :

- chooses $e' \in_R Z_n$ such that $gcd(e', n) = 1$,
- selects d such that $e'd \equiv 1 mod \phi(n)$,
- chooses randomly an integer x' from $0 < x' < n$, computes $y' = g^{x'} mod(p)$, then publishes (y', e').
- chooses randomly w, u such that $w, u < n$
computes $M = g^{h(m)^w} \bmod (p)$, $N = g^{h(m)^u} \bmod (p)$,
then $s^* = (x'h(m) + Mh(m)^u + Nh(m)^w)^d \bmod (p)$,
- 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 $p + 1 + 2\sqrt{p}$,
- chooses randomly k' such that $1 < k' < n$, computes $R' = k'P$, $r' = x(R')$
- computes $s' = k_A r' + k' \bmod n$.

A sends the delegation parameter (r', s', R', M, N, s^*) to B.
Proxy signer B checks whether $R' = s'P - r'P_A$ and $g^{s^*e'} = {y'}^{h(m)} M^N N^M \bmod (p)$. If these equations hold, B computes $\overline{s} = s' + k_B \bmod n$.

Signing Phase- Proxy signer B chooses $1 < k < n$, computes $T = kP$, Then he/she sends (r', s', T) to owner C.
Owner C chooses $1 < a, b < n$, computes
$R = T + bP + (-a - b)P_B + (-a)R' + (-ar')P_A$,
$r = x(R)$, $e = h(r||m) mod\ n$, $e^* = e - a - b$
$U = (-e + b)R + (-e + b)r'P_A - eP_A$ and send e^* to B.
Proxy signer B computes $s'' = e^*\overline{s} + k \bmod n$ and returns s'' to C.
Owner C computes $s = s'' + b \bmod n$. The resulting signature is (m, s, e, U).

Verification Phase- It can be verified by checking whether $e = h(x(sP - eP_B + eP_A + U)||m) \bmod n$ holds. Here, P_A and P_B are public keys of original and proxy signer respectively.

3.2 Security Analysis of Qi et al's Scheme

We demonstrate here that scheme [10] is insecure.

Universal Forgery Attack- Suppose there is an adversary E, who wants to forge a valid proxy blind signature on any message of his choice (say m'),
E chooses $k', s' \in_R Z_n^*$ and computes

$R' = (k' + s')P$

$r' = x(R')$ and $e' = h(r'||m') \bmod n$

$U' = k'P + e'P_B - e'P_A$, and outputs the forged proxy blind signature (m', s', e', U'). Here, P_A and P_B are public keys of original and proxy signer respectively.
Indeed,

$$\begin{aligned} & h[x(s'P - e'P_B + e'P_A + U')||m'] \bmod n \\ = \; & h[x(s'P - e'P_B + e'P_A + k'P + e'P_B - e'P_A)||m'] \bmod n \\ = \; & h[x(s'P + k'P)||m'] \bmod n \\ = \; & h(r'||m') \bmod n \\ = \; & e' \end{aligned}$$

Therefore, the tuple (m', s', e', U') is a valid proxy blind signature.

Absence of Unlinkability- The proxy signer can save the signing transcripts $(T, e^*, s")$ during generation of the signature. With a proxy blind signature tuple (m, s, e, U), the proxy unlinkability holds, if and only if there is no conjunction between $(T, e^*, s")$ and (m, s, e, U). In the above scheme [10], with (m, s, e, U), proxy signer B can find its corresponding signing transcripts as follows:
B computes $b = (s - s") \bmod n$,

$a = (e - b - e^*) \bmod n$,

$R = T + bP + (-a - b)P_B + (-a)R' + (-ar')P_A$,

Now B checks

$U = (-e + b)R + (-e + b)r'P_A - eP_A$,

If it does, B can link (m, s, e, U) to $(T, e^*, s")$ successfully.

Absence of Identifiability- In Qi et al's scheme, the proxy blind signature is (m, s, e, U) and the verification equation is $e = h(x(sP - eP_B + eP_A + U)||m) \bmod n$. The public keys P_A and P_B of original signer and the proxy signer respectively are in the same position. Therefore, it is difficult to distinguish the identity of proxy signer from proxy signature. The scheme does not satisfy identifiability.

4 Improved Scheme

To remedy the weakness of Qi et al's scheme [10], we propose an improvement on [10], and present the security analysis and efficiency comparisons of proposed scheme with [10].

4.1 Scheme Description

Our scheme is described as follows.

System Parameters- System Parameters used in the scheme are as follows.
- p and q are two large primes such that $q/p-1$.
- An additive group $Z_p = \{0, 1, 2, ..., p-1\}$.
- $g \in Z_p^*$ having order q.
- P is the generator of elliptic curve group of order n.
- (k_A, P_A): private & pubic key pair of original signer A such that $P_A = k_A P$.
- (k_B, P_B): private & pubic key pair of proxy signer B such that $P_B = k_B P$.
- $H : \{0,1\}^* \rightarrow Z_n^*$ is a public cryptographically strong hash function.
- $||$ is the concatenation of strings.
- a message m represents a monetary value which the customer can spent.
- $\phi(.)$ is the phi-Euler function.
- $gcd(a, b)$ is the greatest common divisor of a and b.
- $x(Q)$ is the x coordinate of a point Q on the elliptic curve E..

Proxy Phase- The original signer A generates the following system parameters.
- chooses $e' \in_R Z_p^*$ such that $gcd(e', \phi(p-1)) = 1$,
- selects d such that $e'd \equiv 1 mod \phi(p-1)$,
- chooses $x' \in \{2, 3, ...p-2\}$, computes $y' = g^{x'} mod(p)$, then publishes (y', e').
- chooses $w, u \in \{2, 3, ...p-2\}$ and computes $M = g^{H(m_w)^w} \bmod (p)$, $N = g^{H(m_w)^u} \bmod (p)$, then $s^* = (x'H(m_w) + MH(m_w)^u + NH(m_w)^w)^d \bmod \phi(p)$,
- chooses $k' \in_R Z_n^*$, computes $R' = k'P$, $r' = x(R')$
- computes $h = H(r'||m_w)$ and $s' = k_A h + k' \bmod n$.

A sends the delegation parameter (m_w, s', R', M, N, s^*) to B.

Proxy signer B checks, whether $R' = s'P - hP_A$ and $g^{s^* e'} = y'^{H(m_w)} M^N N^M \bmod (p)$. If these equations hold, B computes $\overline{s} = s' + k_B \bmod n$.

Signing Phase- Proxy signer B chooses $k \in_R Z_n^*$, computes $T = kP$, Then he/she sends (m_w, R', s', T) to owner C.
Owner C chooses $a, b, c \in_R Z_n^*$, computes
$R = aT + bP + c(P_B + R' + hP_A)$,
$r = x(R)$, $e = H(r||m) \bmod n$, $e^* = a^{-1}(e + c) \bmod n$ and sends e^* to B.
Proxy signer B computes $s'' = e^* \overline{s} + k \bmod n$ and returns s'' to C.
Owner C computes $s = as'' + b \bmod n$. The resulting proxy blind signature is (m_w, m, R', e, s).

Verification Phase- The verifier can verify the validity of the proxy blind signature by checking that $e = H(x(sP - e(P_B + R' + hP_A))||m) \bmod n$ holds.

4.2 Security Analysis

We analyze the security of our scheme as follows.

Distinguishability- The proposed proxy blind signature (m_w, m, R', e, s) contains the warrant m_w while the normal signature does not, so both are different in the form. Also in the verification equation of proxy blind signature, public keys P_A, P_B and warrant m_w are used. So anyone can distinguish the proxy blind signature from normal signature easily.

Verifiability- The verifier of proxy blind signature, can check whether verification equation $e = H(x(sP - e(P_B + R' + hP_A))||m) \bmod n$ holds or not. We prove this as follows.

$e = H(r||m) \bmod n$
$= H[x(R)||m] \bmod n,$
$= H[x(aT + bP + c(P_B + R' + hP_A))||m] \bmod n,$
$= H[x(aa^{-1}(e + c)(P_B + R' + hP_A) + akP + bP - e(P_B + R' + hP_A))||m] \bmod n,$
$= H[x(ae^*(k_B + s')P + akP + bP - e(P_B + R' + hP_A))||m] \bmod n,$
$= H[x(a(e^*\overline{s} + k)P + bP - e(P_B + R' + hP_A))||m] \bmod n,$
$= H[x((as" + b)P - e(P_B + R' + hP_A))||m] \bmod n,$
$= H[x(sP - e(P_B + R' + hP_A))||m] \bmod n.$

Unforgeability- In our scheme, only the designated proxy signer can create a valid proxy blind signature, since proxy private key $\overline{s} = s' + k_B$ includes the private key k_B of proxy signer and to compute k_B, is equivalent to solve ECDLP. In addition, if anyone wishes to forge secret keys (x', d), then he needs to solve $e'd \equiv 1 mod \phi(p-1)$ and $y' = g^{x'} mod(p)$ respectively, for d and x'. But solving both congruences, is as difficult as solving IFP and DLP.

On the other hand, our scheme can withstand the universal forgery attack. Suppose, there is an adversary E, having a valid proxy blind signature (m_w, m, R', e, s) and he attempts to forge a valid proxy blind signature on message m', of his choice as (m_w, m', R', e', s'). Then E does as follows.

- computes $r' = x(R')$, $h = H(r'||m_w) \bmod n$
- selects $k_2 \in_R Z_n^*$, computes $R = k_2 P$
- computes $r = x(R)$, $e' = H(r||m') \bmod n$

then (m_w, m', R', e', s') being a valid proxy blind signature must satisfy the verification equation $e' = H[x(s'P - e'(P_B + R' + hP_A))||m'] \bmod n$.
E needs to solve $s'P - e'(P_B + R' + hP_A) = R$ for s'. But to do so, is as difficult as solving ECDLP.

Nonrepudiation- As in the verification equation, warrant m_w and public keys P_A, P_B are used. Also generation of proxy blind signature needs original and proxy signer's private key k_A, k_B respectively. It is already proved that neither the original signer nor the proxy signer can sign in place of other party. So the original signer can not deny his delegation and proxy signer can not deny having signed the message m on behalf of original signer to other party.

Identifiability- In the proposed scheme, it can be checked who is original signer and who is proxy signer, from warrant m_w. Also seeing from the verification

equation, $e' = H[x(s'P - e'(P_B + R' + hP_A))||m']$ mod n, the public keys P_A, P_B are asymmetrical in position. So anyone can distinguish the identity of proxy signer from proxy blind signature.

Prevention of Misuse- Original signer generates the delegation parameter (m_w, s', R', M, N, s^*) and sends it to B. So the values of (m_w, s', R', M, N, s^*), can not be modified or forged. Also it is not possible for proxy signer B to transfer his proxy power to other party D, unless he provides proxy private key $\overline{s}$ to D. In addition, warrant m_w contains the limit of delegated signing capability. So it is not possible to sign the messages that have not been authorized by original signer.

Unlinkability- The proxy signer can save the signing transcripts $(T, e^*, s")$ during generation of the signature. With a proxy blind signature tuple (m_w, m, R', e, s), the proxy unlinkability holds if and only if there is no conjunction between $(T, e^*, s")$ and (m_w, m, R', e, s). In our scheme $(T, e^*, s")$ is associated with signature through following three equations

$R = aT + bP + c(P_B + R' + hP_A)$,
$e^* = a^{-1}(e + c)$ mod n,
$s = as'' + b$ mod n.

If anyone knows the value of R, then by checking equation $e = H(x(R)||m)$ mod n, he can link $(T, e^*, s")$ to (m_w, m, R', e, s). But it is infeasible to find four unknowns a, b, c, R using three equations. Hence our scheme achieves unlinkability property.

4.3 Comparative Analysis

While maintaining the security, our scheme is more efficient as compared to Qi et al's [10]. The detailed costs in each phase are compared in the given table, where T_H denotes the once running of hash operation, M_E and A_E denote the once running of multiplication and addition operations on non-singular elliptic curve E.

Computational Cost Comparison:

Scheme	signing phase	verification phase	Total
scheme [10]	$8M_E + 6A_E + 1T_H$	$3M_E + 3A_E + 1T_H$	$11M_E + 9A_E + 2T_H$
Our scheme	$5M_E + 4A_E + 1T_H$	$3M_E + 3A_E + 2T_H$	$8M_E + 7A_E + 3T_H$

From the given table, we notice that the improved scheme has less computational cost than Qi et al's [10], except one more operation of hash function needed in the improved scheme. Even in this way, the improvement is still much more efficient ($3M_E + 2A_E$ - $1T_H$ computation less) than Qi et al's [10].

5 Conclusion

In this paper, We analyzed the security and improvement given in Qi et al's proxy blind signature scheme [10]. We demonstrated that scheme [10] is insecure against universal forgery attack. It also does not satisfy the unlinkability and identifiability property. To remedy the weaknesses of scheme [10], we proposed an improvement on it and proved that the improved scheme is secure, effective and more efficient than Qi et al's scheme [10].

References

1. Brands, S.: Untraceable Off-Line Cash in Wallets with Observers. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 302–318. Springer, Heidelberg (1994)
2. Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology- Crypto 1982, pp. 199–203. Springer, Heidelberg (1983)
3. Chaum, D., Fiat, A., Naor, M.: Untraceable Electronic Cash. In: Goldwasser, S. (ed.) CRYPTO 1988. LNCS, vol. 403, pp. 319–327. Springer, Heidelberg (1990)
4. Chaum, D., den Boer, B., van Heyst, E., Mjoelsnes, S.F., Steenbeek, A.G.: Efficient Offline Electronic Checks. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 294–301. Springer, Heidelberg (1990)
5. Hu, L., Zheng, K., Hu, Z., Yang, Y.: A Secure Proxy Blind Signature Scheme Based on ECDLP. In: 2009 International Conference on Multimedia Information Networking and Security. IEEE (2009), doi:10.1109/MINES.2009.220
6. Koblitz, N.: Elliptic curve cryptosystems. Mathenmatics of Computation 48(177), 203–209 (1987)
7. Miller, V.S.: Use of Elliptic Curves in Cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
8. Menezes, A., Oorschot, P.C.V., Vanstone, S.: Handbook of Applied Cryptography. CRC Press (1996)
9. Mambo, M., Usuda, K., Okamoto, E.: Proxy signatures: Delegation of the power to sign messages. IEICE Transactions Fundamentals E79-A(9), 1338–1353 (1996)
10. Qi, C., Wang, Y.: An Improved Proxy Blind Signature Scheme Based on Factoring and ECDLP. In: Computational Intelligence and Software Engineering, pp. 1–4. IEEE (2009), doi:10.1109/CISE. 2009.5365847
11. SECI. Elliptic Curve Cryptography, Standands for Efficient Cryptography (September 2000), `http://www.secg-talklistscerticom.com`
12. Tan, Z., Liu, Z., Tang, C.: Digital proxy blind signature schemes based on DLP and ECDLP. MM Research Preprints, No.21, MMRC, AMSS, Academia, Sinica, Beijing, No. 21, 212–217 (2002)
13. Wang, H.Y., Wang, R.C.: A proxy blind signature scheme based on ECDLP. Chinese Journal of Electronics 14(2), 281–284 (2005)
14. Yang, X., Yu, Z.: Security Analysis of a Proxy Blind Signature Scheme Based on ECDLP. In: The 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2008), pp. 1–4 (2008)