Available online at www.elixirpublishers.com (Elixir International Journal)

Cryptology

Elixir Cryptology 36 (2011) 3248-3250

ISSN: 2229-712X

Proxy blind signature based on ECDLP for multiple signers

Satarupa Pradhan[1] and Ramesh Kumar Mohapatra[2]

[1]Department of Information Technology, Institute of Technical Education and Research, Siksha 'O' Anusandhan University, Bhubaneswar, India.

[2]Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan University, Bhubaneswar, India.

ARTICLE INFO

Article history:

Received: 4 May 2011;

Received in revised form:

19 June 2011;

Accepted: 28 June 2011;

Keywords

Cryptography,
Blind Signature,
Proxy Signature,
ECDLP,
Proxy Blind Signature,
Multiple Original Signers.

ABSTRACT

Proxy blind signature combines the properties of both proxy signature and blind signature. In a proxy signature scheme, a signer delegates his signing power to a proxy, who signs a message on behalf of the original signer. In a blind signature scheme, the signer cannot link the relationship between the blind message and the signature of the chosen message. Therefore, it is very suitable for electronic commerce application. In this paper, a proxy blind signature scheme based on ECDLP for multiple signer has been proposed, which satisfy the security properties of both the blind signature and the proxy signature. In this proposed scheme multiple original signers are delegates their signing power to one proxy signer, who give signature on behalf of them. Analysis shows that our scheme is secure and efficient.

Introduction

The blind signature scheme was first proposed by Chaum in 1982 [1]. In a blind signature scheme a user obtains an original signer's signature for a message without revealing any information to the signer. With such properties, the blind signature scheme is useful in several applications as such e-voting and e-payment. A proxy signature scheme enables a proxy signer to sign messages on behalf of an original signer. Mambo et al. [2] first introduced the concept of proxy signature. In proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. Proxy blind signature was introduced by W.D. Lin and J.K. Jan in 2000.

In our proposed model multiple original signers' delegates their signing power to one proxy signer, who is able to give signature on a single message. This concept was first proposed by L. Yi and G. Bai in 2000.

Generally when an original signer delegates his signing power to a proxy signer, he uses secure channel for transformation. Lu et al. [10] proposed a proxy blind multi signature scheme which did not need a secure channel and satisfy verifiability, Unforgeability, Unlinkability properties only. The proxy blind signature should satisfy the following properties:

- Distinguishability: The proxy signature must be distinguishable from the original signature.
- Unforgeability: Only the designated proxy signer can generate a valid proxy signature.
- Non-repudiation: The original and proxy signer can't deny their signatures against any one.
- Verifiability: The receiver should be able to verify the proxy signature. dentifiability: Anyone can determine the identity of the corresponding proxy signer and original signer from the signature.
- Prevention of misuse: The proxy key pair should be used only for creating proxy signature.
- Unlinkability: When the signature is revealed the proxy signer cannot identify the association between the message and the blind signature he generated.

Elliptic Curve

In 1985, Elliptic Curve Cryptography (ECC) was proposed independently by cryptographers Victor Miller (IBM) [8] and Neal Koblitz (University of Washington) [9]. ECC is based on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP). Like the prime factorization problem, ECDLP is another "hard" problem that is deceptively simple to state: Given two points, P and Q, on an elliptic curve, find the integer n, if it exists, such that P = nQ. To provide the same level of security ECC requires 160 bits where as RSA requires 1024 bits [10]. The security of ECC depends on the elliptic curve logarithm problem, a solution which is infeasible if the modulus is large.

A non singular Elliptic curve E can be written as:

$$E : y2 = x3 + ax + b \pmod q$$

Where $4a3 + 27b \neq 0 \pmod q$

The point P in the Elliptic curve is described by the coordinates (x1, y1).

The negative of the point P = (x1, y1) is the point –P = (x1, -y1).

Addition of two distinct points P and Q

If P (xp, yp) and Q (xq, yq) are two distinct points such that P is not –Q, then

$$P + Q = R$$

Where R = (xr, yr)

$$\lambda = (yq - yp) / (xq - xp) \bmod q$$

Where, λ is the slope of the line passing through P and Q

$$xr = (\lambda 2 – xp – xq) \bmod q$$

$$yr = (\lambda * (xp - xr) – yp) \bmod q$$

Tele:
E-mail addresses: satarupapradhan@gmail.com, rkmohapatraiter@gmail.com

Doubling the point P
Provided that yp is not 0
2P = R(xr, yr)
λ = ((3xp2 + a) / (2yp)) mod q
xr = (λ 2 – 2xp) mod q
yr = ((λ * (xp – xr)) – yp) mod q (I)

The elliptic curve discrete logarithm problem is defined as follows:

Definition: Let E be an elliptic curve over a finite field Fq and let P □ E (Fq) be a point of order n. Given Q □ E (Fq), the elliptic curve discrete logarithm problem is to find the integer d □ [0, n-1], such that Q = d*P. (II)

Proposed Model

In this section, we propose an efficient proxy blind signature scheme based on ECC. The proposed scheme is divided into six phases: system parameter, generation of proxy sub-secret key, verification of proxy sub-secret key, generation of proxy secret key, signing phase and validation phase.

System parameter

Ai: Original Signer (1 ≤ i ≤ n)
p, q: are two prime integers, q | (p-1)
B: proxy signer
C: signature requester
xi: Original signers private key
yi: Original signers public key
xb: Proxy signers private key
yb: Proxy signers public key
H (), H1 (), H2 () : 3 Hash Function
mw: is the proxy warrant negotiated by all original signers

Generation of Proxy Sub-secret Key

Original signer Ai Selects a random number Ki (Ki□Zq*) then computes
Again Ai selects Ki' randomly, Ki'□Zq* and computes
Then Ai publishes (ri, mw) and sends

Verification of Proxy Sub-secret Key

After B received he validates it and recovers Si
(I)Now B computes
(II)Then checks, whether holds or not. If yes, B accept else reject it.
(III)Once is validated, B use his private key xb to recover Si, as follows
(IV)Finally, checks if .
If it is true, Si will be accepted, else rejected.

Generation of Proxy Secret Key

After proxy signer B received n valid Si (1 ≤ i ≤ n), he computes the proxy secret key Sk

Signing Phase

After proxy secret key Sk has been generated proxy signer B can make blind signature on behalf of all original signers Ai. A requester C asks proxy signer B to generate a blind signature on message m as follows:

(I) Proxy signer B selects w1 □ Zq* randomly and computes and send it to C.
(II) Requester C first computes a
Then chooses randomly, w2, w3aq* and computes

$$x^* = w_2 B + w_3 \propto + x \pmod p$$
$$e^* = H_2(x^*, m)$$
$$e = e^* + w_3 \pmod q$$

Finally, signature requester C sends *e* to the proxy signer B.
After B received *e* he computes $y = w_1 + eS_k \pmod q$ and send *y* to C.
When C received *y*, he computes

$$y^* = y + w_2 \pmod q$$

Then (e^*, y^*) is the proxy blind signature of message m.

1. **Validation Phase**

When the proxy blind signature (e^*, y^*) was generated, anyone can validate it, as following:
Compute α in the same way of requester C

$$\alpha = y_b + \sum_{i=1}^{n} \{R_i + (H(m_w, r_i) y_i)\} \pmod p$$

Check $e'^* \stackrel{?}{=} H_2(y^* B - e^* \propto, m)$
If $e'^* = e^*$, then anyone can be convinced (e^*, y^*) is a valid proxy blind multi signature on message m.

Security Properties of the Proposed Scheme

Nonrepudiation: In this scheme the original signer does not know the proxy signer's secret key x_b and proxy signer does not know original signer's secret key x_i. Thus, neither the original signer nor the proxy signer can sign in place of the other party.

Unforgeability: An adversary (including the original signers and the receiver) wants to forge the proxy signer's signature to sign the message *m*. The original signers do not know the proxy signer secret key S_k. The requester can able to know the delegation information (C_i, r_i'', S_i') but he cannot obtain S_i which is secret and proxy signer's secret key S_k. So for this scheme forgery is hard.

Distinguishability: For the generation of proxy secret key S_k, both original signers and proxy signer's secret keys are responsible i.e. Original signers and proxy signer's secret keys are required. So the proxy signature is easy to be distinguishable from the normal signature.

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

$$e'^* \stackrel{?}{=} H_2(y^* B - e^* \propto, m)$$

Because,

$$y^* B - e^* \propto$$
$$= B(y + w_2) - e^* \alpha$$
$$= B(w_1 + eS_k + w_2) - e^* \alpha$$
$$= B(w_1 + (e^* + w_3) S_k + w_2) - e^* \alpha$$
$$= w_1 B + e^* S_k B + w_3 S_k B + w_2 B - e^* \alpha$$
$$= x + w_2 B + w_3 \alpha + (e^* \alpha) - (e^* \alpha)$$
$$= x + w_2 B + w_3 \alpha$$
$$= x^*$$

Identifiability: In the verification equation α is used, which includes the original signer A_i's public key y_i and the proxy signer B*'s* public key y_b . Again m_w is public. So, anyone can determine the identity of the corresponding proxy signer from a proxy signature.

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, delegation period, etc. With the proxy key, the proxy signer cannot sign messages that have not been authorized by the original signer.

Unlinkability: The proxy signer is allowed to give signature on behalf of the original signer when he receives the delegation message (C_i, r_i'', S_i') from the original signer.During signature generation i.e. (e^*, y^*) the proxy signer only have knowledge on $(C_i, r_i'', S_i', S_i, r_i', S_k, w_1, x, e, y)$. The signature requester uses two random secret keys w_1, w_2 to make the message blind. Hence the requester can only unblind the message. The original signer and the proxy signer has no knowledge about the secret

random numbers, therefore this scheme achieves the unlinkability property.

Conclusion

This system presents a secure and efficient proxy blind signature scheme based on ECDLP for multiple signer. The proposed scheme satisfies the given security properties. The scheme uses fewer numbers of bits, for the properties of elliptic curve, than RSA. Again, the proposed scheme does not use secure channel in the communication between the original signer and the proxy signer. Thus it is suitable for e-case and e-commerce.

Reference

[1] D. Chaum, "Blind signature for untraceable payments", Advances in Cryptology, proceeding of CRYPTO'82, Springer-Verlag, pp.l99-203, 1983.

[2] M. Mambo, K. Usuda, E. Okamoto, "Proxy Signature: Delegation of the power to sign message", IEICE Transaction on Fundamentals, vol. E79-A (9), pp. 1338-1354, 2003.

[3] Z. Tan, Z. Liu, C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP", MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, vol. 21, pp. 212-217, 2002.

[4] S. Lal, A.K. Awasthi, "Proxy blind signature scheme", Cryptology ePrint Arechive: Report 2003/072, Available from <http://eprint.iacr.org/>.

[5] Hung-Min Sun, Bin-Tsan Hsieh, Shin-Mu Tseng, "On the security of some proxy blind signature schemes", Systems and software, Elsevier, vol.74, pp.297-302, 2005.

[6] J.G. Li, S. H. Wang, "New Efficient Proxy Blind Signature Scheme Using Verifiable Self certified Public Key", International Journal of Network Security, vol.4, No.2, pp.193–200, 2007.

[7] F. Y. Yang, Z. W. Liu, "Improvement of an efficient proxy blind signature scheme", International Conference on Innovative Computing, Information and Control, pp.733-736, 2009.

[8] V. Miller, "Uses of Elliptic Curve in Cryptography", Advances in Cryptography, Proceedings of Crypto'85, Lectures notes on Computer Sciences, Springer-Verlag, pp. 417-426, 1986.

[9] N. Koblitz, "Elliptic Curve Cryptosystems", Mathematics of Computation, vol. 48, pp. 203-209, 1987.

[10] R. Lu, Z. Cao, Y. Zhou, "Proxy Blind multi signature scheme without a secure channel", Applied mathematics and computation, vol.164, pp.179-187, 2005.

[11] Baoyuan Kang, Jinguang Han, Qingiu Wang, "On the security of proxy blind multi-signature scheme without a secure channel", 2nd IEEE international conference on Computer Engineering and Technology, vol.1, pp.62–64, 2010.

[12] Ying Sun, C. Xu, Qi Xia, Y. Yu, "Analysis and improvement of a proxy blind multi-signature scheme without a secure channel", fifth IEEE international conference on Information Assurance and Security, pp.661-664, 2009.

(Figure 1: shows the message flow of the proposed scheme)