Stamped Proxy Blind Signature Scheme

Suryakanta Panda
Department of Computer Science
NIT Rourkela, Odisha, India

Ramesh Kumar Mohapatra
Department of Computer Science
NIT Rourkela, Odisha, India

ABSTRACT
This paper presents two types of digital signature schemes combinely that are blind signature and proxy signature. In the proxy blind signature scheme, a signer other than the original signer signs the document as the agent of the original signer not knowing the meaning of the message. In this paper, an enhanced proxy blind signature is proposed, in which a time stamp approach is added to the proxy blind signature scheme which is based upon the discrete logarithm problem (DLP).

Keywords
Proxy Blind Signature, Proxy Signature, DLP.

1. INTRODUCTION
Blind signature was first introduced by David Chaum [1] in 1983 in which the signer signs the message but he/she is ignorant about the contents of the message. Blind signature schemes are widely used in such applications where the privacy of the sender is important e.g. e-vote, e-cash, etc. Later, in 1996 Mambo et al [2], by analyzing the concept of seal in our day to day life introduced the proxy signature scheme. In proxy signature scheme, the original signer delegates his power to the proxy signer and the proxy signer signs the message or document as the agent of the original signer. By applying both blind signature and proxy signature schemes concurrently Lin and Jan in 2000, proposed a new digital signature scheme that is proxy blind signature scheme.

The proxy blind signature should meet the following security requirements:

- Strong Unforgeability:

  No one other than the designated proxy signer can produce a valid proxy blind signature.

- Distinguishability:

  The proxy blind signature must be differentiable from the normal signature.

- Nonrepudiation:

  The original signer and the proxy signer cannot refuse their signatures against anyone.

- Identifiabiability:

  Anyone can find out the identification of the corresponding original signer and proxy signer from the signature.

- Verifiability:

  The verifier should be able to examine the proxy signature.

- Prevention of misuse:

  The proxy key pair is used only for generating the proxy signature.

- Unlinkability:

  During the verification of the signature the signer cannot relate the message and the generated blind signature.

2. RELATED WORK
In 2000, Lin et al. first project the proxy blind signature by combining the proxy signature and the blind signature scheme. Later, Tan et al. [3] suggested a proxy blind signature scheme which was based on Schnorr blind signature scheme. In 2003, Lal et al. [4] 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 scheme. In 2004, Wang et al [5] showed two attacks on Tan et al scheme. Later Xue et al [6] pointed out one fault in both Tan et al's scheme and Lal et al's scheme since the proxy signer can get the link between the blind message and the signature or plain text. In 2005, Sun et al. [7] demonstrated that Tan et al's scheme failed to satisfy the unlinkability and unforgeability properties and also showed that Lal et al's scheme failed to satisfy unlinkability property. In 2008, Yang et al [8] demonstrated a new scheme and proved that their scheme is efficient and secure.

3. PROPOSED WORK
In this section, we propose a new efficient and secured proxy blind signature scheme. The scheme is divided into following five stages

(i) System parameter initialization

(ii) Proxy delegation

(iii) Blind signing

(iv) Signature extraction

(v) Signature verification

3.1 System Parameter Initialization
A: Original Signer

B: Proxy Signer

R: Signature Requester

p, q: two large prime numbers such that q | p-1

g: generator of order q in Z_p^*

$x_A, x_B \in Z_q^*$: the original signer A's secret key and the proxy signer B's secret key respectively

$y_A = g^{x_A} \pmod p$:A's public key

$y_B = g^{x_B} (\mathrm{mod}\ p)$: B's public key

H(.): a cryptographically secure one way hash function

□: which denotes the concatenation of two strings

m_w : Message warrant

m: message

3.2 Proxy Delegation

The original signer A randomly picks out $\bar{k} \in Z_q^*$ and computes,

$$r = g^{\bar{k}} (\mathrm{mod}\ p) \quad (1)$$

$$s = x_A + \bar{k}.H(m_w \square r) \bmod q \quad (2)$$

A sends (r, s) along with the warrant m_w to the proxy signer B via a secure channel

The proxy signer B, then verifies the equation

$$g^s = y_A r^{H(m_w \square r)} \bmod p \quad (3)$$

If it is correct, B accepts and computes

$$s_{pr} = s + x_B y_A \bmod q \quad (4)$$

as his/her proxy blind signature secret key

3.3 Blind Signing

Proxy signer, B randomly selects an integer $k \in z_q^*$, and computes

$$t = g^{k + x_B + H(time \square place)} \bmod p \quad (5)$$

B, then sends (r, t) to the receiver R

R selects two random numbers u, v $\in z_q^*$,

R computes,

$$r' = t g^{u + x_R} y_{pr}^v \quad (6)$$

Where, x_R is the private key of R and $y_{pr} = g^{s_{pr}}$

$$e = H(r' \square m) \bmod q \quad (7)$$

$$e^* = v - e \bmod q \quad (8)$$

If r'=0, then R needs to select a new tuple (u, v) otherwise, R sends e* to B

After receiving e*, the proxy signer B computes

$$s' = k + e^* s_{pr} + H(time \square place) \bmod q \quad (9)$$

As, the signed message and sends it to the receiver R.

3.4 Signature Extraction

After receiving s' from B, the receiver R computes,

$$s^* = g^{u+s'} \bmod q \quad (10)$$

thus, the proxy blind signature on m becomes finally (m, m_w, s*, e).

3.5 Verification

Verifier can verify the proxy blind signature by checking whether

$$e = H(s^* y_B y_R y_{pr}^e \square m) \bmod q \quad (11)$$

4. SECURITY ANALYSIS OF THE PROPOSED SCHEME

(i) If the original signer has an intention to forge a proxy blind signature with forgery attack for the message m', he/she have to create a secret key s_{pr}' and calculate

$$y_A' = g^{s_{pr}'} (\mathrm{mod}\ p)$$

He/she has to calculate

$$s^* y_B y_R y_{pr}^e (\mathrm{mod}\ p) = t g^{u + x_R} y_{pr}^v (\mathrm{mod}\ p)$$

By using the previous equations we can find

$$g^{k + x_B + x_R + u + H(time \square place) + e^* s_{pr}'} y_{pr}^e = t g^{u + x_R} y_{pr}^v$$

$$\Rightarrow g^{v-e} s_{pr}' = y_{pr}^{v-e}$$

To find the value of s_{pr}' the original signer must find a solution to the above equation which is a discrete logarithm problem. Thus, the original signer fails to forge a signature.

(ii) The receiver cannot forge the signature after receiving (m, m_w, s*,e) on message m. when a receiver tries to forge a signature (m', s*, e') for message m', he/she must verify that the equation given below is correct.

$$s^* y_B y_R y_{pr}^e (\mathrm{mod}\ p) = t g^{u + x_R} y_{pr}^v (\mathrm{mod}\ p)$$

By using previous equations we can find

$$s^* y_B y_R y_{pr}^e = g^{u+s'} g^{x_B} g^{x_R} y_{pr}^{e'}$$

$$= g^{u + s' + x_B + x_R} g^{s_{pr} e'}$$

$$= t g^{u + (v-e) s_{pr} + x_R} g^{s_{pr} e'}$$

$$= t g^{u + x_R} y_{pr}^v$$

From the above we can get,

$$g^{(v-e)s_{pr}} g^{s_{pr}e'} = g^{s_{pr}v}$$

This cannot hold true, as e ≠ e'. Thus the receiver fails.

(iii) The proxy linkability holds if there is a conjuction between (t, e*, s') and (m, m_w, s*, e). t is only in equation (6) and relate to e through equation (7). Proxy signer cannot find out the value of it as it is masked by two random numbers u and v. Hence, the proposed scheme satisfies the unlinkability property.

(iv) As the proxy blind signature (m, m_w, s*, e) on the message m, contains m_w (message warrant) any one can easily differentiate between the proxy blind signature and normal signature. Hence, it satisfies the distinguishability property.

(v) From the warrant m_w, anyone can mark original signer and proxy signer. On the other hand, as the verification equation contains the public key of the proxy signer and original signer one can identify them. Hence, it satisfies the identifiability property.

(vi) The original signer cannot get the proxy signer's secret key, and similarly the proxy signer cannot get the original signer's secret key. So, one cannot sign on behalf of another. Hence, it satisfies the non repudiation property.

(vii) Due to the inclusion of the original signer and proxy signer identity information, message type to be signed by the proxy signer, delegation period, etc. in the warrant itself the proposed scheme is capable of preventing proxy key pair misuse.

(viii) Verification:

The proposed scheme satisfies the property of verifiability.

$$H(s^* y_B y_R y_{pr}^e \| m) \bmod q$$

$$= H(s^* g^{x_B} g^{x_R} y_{pr}^e \| m) \bmod q$$

$$= H(g^{k+x_B+x_R+u+H(time\|place)+e^* s_{pr}} y_{pr}^e \| m) \bmod q$$

$$= H(g^{k+x_B+x_R+u+H(time\|place)+s_{pr}v} y_{pr}^e y_{pr}^{-e} \| m) \bmod q$$

$$= H(g^{k+x_B+x_R+u+H(time\|place)+s_{pr}v} \| m) \bmod q$$

$$= H(g^{k+x_B+H(time\|place)} g^{u+x_R} y_{pr}^v \| m) \bmod q$$

$$= H(t g^{u+x_R} y_{pr}^v \| m) \bmod q$$

$$= H(r' \| m) \bmod q = \text{e}$$

(ix) Efficiency Analysis:

Let M and E denote computational load for multiplication and exponentiation respectively. The computational load for addition is omitted due to the high performance. The table given below gives the details of the comparison of computational loads of the proposed scheme with other existing schemes.

Scheme	Phase			Total
	Proxy Generation	Blind Signing	Verification	
Scheme [3]	4E+3M	7E+6M	3E+3M	14E+12M
Scheme [8]	3E+2M	5E+4M	2E+3M	10E+9M
Scheme [9]	3E+2M	3E+4M	2E+3M	8E+9M
Scheme[10]	4E+2M	4E+5M	2E+M	10E+8M
Proposed Scheme	3E+3M	5E+3M	E+3M	9E+9M

The proposed scheme is also efficient as other schemes in addition it guarantees that the signing is done within the delegation period.

5. CONCLUSION

During the verification of a proxy blind signature scheme the verifier cannot know whether signing (done by proxy signer) is within the delegation period or not. Proxy signer can make fool to the verifier by signing the message or document after the delegation period is over as there is no such provision to record the timestamp during the proxy signing phase. In the proposed scheme verifier can verify that the proxy signature was signed during a valid delegation period and it satisfies all the security requirements.

6. REFERENCES

[1] Chum, D. "Blind Signatures for Untraceable Payments," New York: Crypto'82, Plenum Press, 1983, pp. 199-203.

[2] Mambo, M., Usada, K., Okamoto, E. "Proxy Signatures for Delegating Signing Operation," Proc 3rd ACM Conference on Computer and Communication Security. New York: ACM Press, 1996, pp. 48-57.

[3] Tan, Z.W., Liu Z.J., Tang C.M. "A Proxy Blind Signature Based on DLP", Journal of Software, Vol. 14, No. 11, 2003, pp. 1931-1935.

[4] Lal, S., Awasthi, A.K. "Proxy blind signature scheme", http://eprint.iacr.org/2003/072.pdf.

[5] Wang, S., Fan, H., Cui, G. "A proxy blind signature schemes based DLP and applying in e-voting", ICEC, 2005, pp. 641-645.

[6] Xue, Q., Cao Z. "A new proxy blind signature scheme with warrant", IEEE Conference on Cybernetics and Intelligent Systems, Singapore, 2004, pp. 1386-1391.

[7] Sun, H., Hsieh, B., Tseng, S. "On the security of some proxy signature schemes", Journal of System and Software, Vol. 74, 2005, pp. 297-302.

[8] Yang, X., Yu, Z. "An efficient proxy blind signature scheme based on DLP", ICESS 2008, pp. 163-167.

[9] Oo, A.N., Thein, N. "DLP based proxy blind signature schemes with low-computation", 5th International Joint Conference on INC, IMS and IDC, 2009, pp. 285-288.

[10] Su, J., Liu J. "A proxy blind signature scheme based on DLP", International Conference on Internet Technology and Applications, 2010, pp. 1-4.