SECURED PROXY BLIND SIGNATURE SCHEME BASED ON DLP WITH MINIMUM COMPUTATION COST

Shradhananda Beura , Muralidhar Behera , Asis Kumar Tripathy
Department of Computer Science and Engineering
NM Institute of Engineering and Technology
Orissa, India 751019

Abstract: **Proxy blind signature is a combination 0f both the properties of proxy signature and blind signature scheme. This scheme is useful in many applications like e-voting, e-payment and mobile agent environments. This paper presents a new proxy blind signature scheme based on discrete logarithm problem(DLP), which satisfies the secure properties of both the blind signature scheme and the proxy signature scheme. As compared with existing typical schemes, this scheme is more secured and efficient with minimum cost.**

Keyword: **blind signature, proxy signature, proxy blind *signature, DLP***

1 INTRODUCTION

A proxy blind signature scheme is a protocol played by two parties in which a user obtains a proxy signer's signature for a desired message and the proxy signer learns nothing about the message. With such properties, the proxy blind signature scheme is useful in several applications such as e-voting, e-payment and mobile agent environments. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The security properties for a good proxy blind signature scheme are as follows:

1) **Distinguish-ability:** The proxy blind signature must be distinguishable from the normal signature.
2) **Non-repudiation:** Neither the original signer nor the proxy signer can sign message instead of the other party. Both the original signer and the proxy signer can not deny their signatures against anyone.
3) **Verifiability:** The proxy blind signature can be verified by everyone.
4) **Unforgeability:** Only the designated proxy signer can create the proxy blind signature.
5) **Identifiability**: Anyone can determine the identity of the corresponding proxy signer from a proxy signature.
6) **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.
7) **Unlinkability**: When the signature is verified, the signer knows neither the message nor the signature associated with the signature scheme.

2 RELATED WORK

In 1982, David Chaum invented a blind signature [1], that scheme allows the sender to have a given message signed by the signers, without revealing any information about the message or its signature. In 1996, Mambo, Usudu and Okamoto [5] proposed a new concept, proxy signature. In a proxy signature scheme, the original signer delegates his signing capacity to a proxy signer who can sign a message submitted on behalf of the original singer. Mambo, Usudu and Okamoto [6] proposed complete proxy signature, partial proxy signature and signature with an entitlement certificate. Zhang [7], and Kim, Park, and Won [8] proposed threshold proxy signature. The proxy signature and blind signature have respective advantages. In some real situations, we must apply them both concurrently, for example, in an anonymous proxy electronic voting. The first proxy blind signature was proposed by Lin and Jan [3] in 2000. Later, Tan et al.[4] proposed a proxy blind signature scheme. In 2001 B. Lee, H. Kim, and K. Kim shown that not only the proxy signer but also the original signer can generate valid proxy signatures. However, in 2003, Lal et al.[9] pointed out that Tan et al.'s scheme was insecure and proposed a new proxy blind signature scheme based on Mambo et al.'s scheme [6]. In 2004, Wang et al.[10] demonstrated that Tan's scheme was insecure and proposed two effective attacks. In 2005, Sun et al.[11] showed that Tan et al.'s schemes didn't satisfy the unforgeability and unlinkability properties and they also pointed out that Lal's scheme [9] didn't possess the unlinkability property either. In 2004, Xue and Cao [12] showed there exists one weakness in Tan et al.'s scheme [4] and Lal et al.'s scheme [9] since the proxy signer can get the link between the blind message and the signature or plaintext with great probability. Xue and Cao introduced concept of strong unlinkability and they also proposed a proxy blind signature scheme. In 2007, Li et al.[13] proposed a proxy blind signature scheme using verifiable self-certified public key, and compared the efficiency with Tan et al.[4]. In 2008 Xuang Yang and Zhaoping Yu proposed new scheme [14] and showed their scheme is more efficient than Li et al.[13] which is again modified by Aung Nway Oo and Nilar Thein in 2009[15] and shown that their scheme is more efficient with low computation. This paper shows the scheme is more efficient and takes very less computational cost than the previous one.

3 PROPOSED PROXY BLIND SIGNATURE SCHEME

In this section, we propose an efficient proxy blind signature scheme based on DLP. The proposed scheme is divided into five stages: System Parameter initialization, proxy delegation stage, blind signing stage, signature extraction stage and signature verification stage.

(A) System Parameter initialization:-

p,q :Two large prime numbers, such that q| (p-1).

g :An element of ***,k*** and the order of g is p.

Infow:It contains the identification information and the available delegation periods for both original and proxy signer.

PRos PBos:Private and public key of Original Signer (OS) such that,

$PRos = g^{PBos} \pmod p$

PRps PBps:Private and public key of Proxy signer (PS) such that,

$PRps = g^{PBps} \pmod p$

H(-),h(.): Public cryptographic collision resistant hash function.

ZP :Set of integers of modulo p.

Zq :Set of integers of modulo q.

$Z^{*}p$:Multiplicative group of order p.

$Z^{*}q$:Multiplicative group of order q.

(B)Proxy Deligation Stage:

Origional Signer (OS) selects random numbers $l \in_R Z^{*}q$

$L = g^{l} \pmod p$ …………………………………………….. (1)

Now the authorization signature sgn is generated as:

$sgn = PBos + l_1 . H(Info_w \| L) \pmod q$ ……………………….. (2)

Now again original signer (OS) transmits (L, sgn) with warrant $Info_w$ to the proxy signer via a secure channel.

After (L, sgn) and warrant $Info_w$ received by proxy signer, the proxy signer (PS) examines sgn for the correctness.

$g^{sgn} = PBos . L^{H(Info_w \| L)} \pmod p$ ..……………………….. (3)

If it is found that the examined signature is legally authorized by original signer (OS) and proxy signer (PS) accepts the proxy deligation and computes proxy signature secrete key S_K as,

$S_K = sgn + PRps$ ……………………………..............….. (4)

note: Where the corresponding proxy public key

$S_{K1} = PBosPBps L^{h(I\, Info_w \| L)} = g^{S_k} \pmod p$

(C)Blind Signing Stage:

Proxy Signer (PS) selects a random number $l \in_R Z^{*}q$ and computes,

$d = g^{l} \pmod p$..............……………………………………(5)

and then sends d to the Original Signer (OS). After receiving the message (d), O.S. choose two random numbers called blinding factors $m,n \in_R Z^{*}q$ and computes, the blind signature of the message **msg**.

$d^{*} = d\, g^{m} (PBos\ PBps)^{n} \pmod p$……...........…….……....….... (6)

$e = h(msg \| d^{*}) \pmod q$ ………………......……………….. (7)

$e' = e + n \pmod q$.....………….............……………… (8)

If d*=0 then O.S. has to select a new tuple (m,n). Otherwise the OS sends **e'** to Proxy Signer (PS). After receiving blinded message e’ Proxy Signer uses its own secret key as:

$S_K = sgn + PR_{PS}$

To generate blind signature S_{K2} as :

$S_{K2} = e' . S_K + l$.....................……………………………….. (9)

(D) Signature Extraction Stage:

$S = g^{S_{K2} + m} . L^{-nh(Infow \| L)}$ ………………………………… (10)

Finally the signature message msg is $(msg, Info_W, s, e, L)$

(E) Verification Phase:

The recipient of the signature can verify the proxy blind signature by checking whether

$e = (h(s\, sk_1^{-e} \pmod p) \| m)) \pmod q$ ……………. (11)

Where $sk_1 = PbosPBps\, L^{h(Infow \| L)}$

If it is true, the verifier accepts it as a valid proxy blind signature, otherwise rejects. The message flows of the proxy blind signature scheme is described in following Figure1.

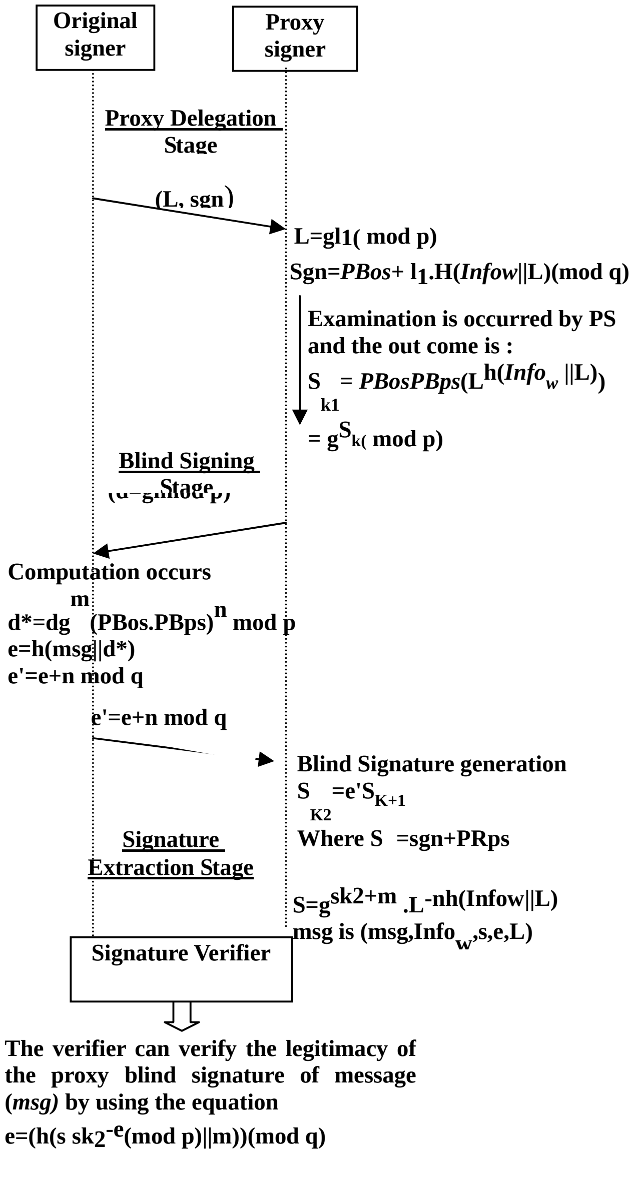
Original signer
Proxy signer
Proxy Delegation Stage
(L, sgn)
L=gl1(mod p)
Sgn=PBos+ l1.H(Infow||L)(mod q)
Examination is occurred by PS and the out come is :
S k1 = PBosPBps(Lh(Infow ||L))
= gSk(mod p)
Blind Signing Stage
(d=glmod p)
Computation occurs
d*=dgm (PBos.PBps)n mod p
e=h(msg||d*)
e'=e+n mod q
e'=e+n mod q
Blind Signature generation
S K2 =e'SK+1
Where S =sgn+PRps
Signature Extraction Stage
S=gsk2+m .L-nh(Infow||L)
msg is (msg,Infow,s,e,L)
Signature Verifier
The verifier can verify the legitimacy of the proxy blind signature of message (msg) by using the equation
e=(h(s sk2-e(mod p)||m))(mod q)

Table 1: Comparison of computational cost with previous scheme [4],[13], [14] and [15]

Schemes	Delegation	Blind signing	Verification	Total costs
Scheme [4]	4*TE*+3*TM*	*7TE+6TM +1TH*	3*TE*+3*TM* +1*TH*	14*TE*+12*TM* +2*TH*
Scheme [13]	3*TE*+2*TM* +2*TH*	5*TE*+6*TM* +2*TH*	3*TE*+3*TM* +2*TH*	11*TE*+11*TM* +6*TH*
Scheme [14]	3*TE*+2*TM* +2*TH*	5*TE*+4*TM* +2*TH*	2*TE*+3*TM* +2*TH*	10*TE*+9*TM* +6*TH*
Scheme [15]	3*TE*+2*TM* +2*TH*	3*TE*+4*TM* +1*TH*	2*TE*+3*TM* +2*TH*	8*TE*+9*TM* +5*TH*
Our Scheme	3*TE*+2*TM* +2*TH*	*2TE+4TM +1TH*	2*TE*+3*TM* +2*TH*	*7TE+9TM +5TH*

4. PROOF OF PROPERTIES OF PROPOSED SCHEME

In this section we discuss the correctness and some of the properties of our proposed proxy blind signature scheme.

Proxy Distinguishability: On the one hand, the proxy blind signature ***(msg,$Info_W$,s,e,L)*** *contains* the warrant ***$Info_W$***. On the other hand, anyone can verify the validity of the proxy blind signature, so he can easily distinguish the proxy blind signature from the normal signature.

Nonrepudiation: The original signer does not obtain the proxy signer's secret key PBps and proxy signer does not obtain original signer's secret key PBos . Thus, neither the original signer nor the proxy signer can sign in place of the other party. At the same time, through the valid proxy blind signature, the verifier can confirm that the signature of the message has been entitled by the original signer, because the verifier must use the original signer's public key during the verification. Likewise, the proxy signer cannot repudiate the signature. The scheme offers nonrepudiation property.

Unforgeability: An adversary (including the original signer and the receiver) wants to impersonate the proxy signer to sign the message *msg*. He can intercept the delegation information (***$Info_W$*** *,sgn ,L*) but he cannot obtain the proxy signature secret key sk . From Equation (4), we know that only the proxy signer holds the proxy signature secret key *PBps*. Because of *PBps* $\in_R$ *Z* q* , the adversary can obtain the proper proxy signature secret key by guessing it with at most a probability1/*q* .That is, anyone else (even the original signer and the receiver) can forge the proxy blind signature successfully with a probability1/*q*.

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

$e=(h(s\,sk_1^{-e}(mod\ p)||m))(mod\ q)$ …………….. (11)
this is because,
$s.sk_1^{-e}$ mod p
by equation 10 (substituting the value of s)
$=g^{sk_2+m}.L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 9 (substituting the value of sk_2)
$=g\ e'sk +l+m .L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 8 (substituting the value of e')
$=g\ (e+n)sk+l+m .L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
$=g\ esk+nsk+l+m .L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
$=g\ l+m\ g\ eskg\ nsk .L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 4 (substituting the value of sk)
$=g\ l+m\ g\ eskg\ n(sgn+PRps) .L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
$=g\ l+m\ g\ eskg\ nsgn\ g\ PRps.L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 2 (substituting the value of sgn)
$=g\ l+m\ g\ eskg\ (PRos+l\ H(Infow||L)\ mod\ q)n\ g\ PRps.L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
$=g\ l+m\ g\ esk(g\ PRosg\ PRps\ )n.\ (g\ l\ mod\ q)nH^{(Infow||L)}.L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 1 (substituting the value of g l mod q)
$=g\ l+m\ g\ esk(g\ PRosg\ PRps\ )n.L^{nh(Infow||L)}.L^{-nh(Infow||L)}.sk_1^{-e}$ mod p
by equation 4(ii) (substituting the value of g sk)
$=g\ l+m\ sk_1^{e}\ (g\ PRosg\ PRps\ )nsk_1^{-e}$ mod p
=g l gm(PBos PBps)n mod p
by equation 5 (substituting the value of g l)
=d gm(PBos PBps)n mod p
by equation 6
=d*

Identifiability*: The proxy blind signature (msg, $Info_W$, s, e,L)* contains the warrant ***$Info_W$*** . Moreover, in the verification equation sk_1 = ***PBosPBps***$L^{h(Infow\ ||L)}$ which includes the original signer's public key PBos and the proxy signer's public key PBps. Hence, 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 ***$Info_W$*** includes original signer and proxy signer identities information, 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.

Proxy Unlinkability: During generation of the signature (msg, $Info_W$, s, e,L) , the proxy signer has the view of transcripts(d, **$Info_W$**, sk_2, e', L).Since ($Info_W$, L) are specified by the original signer for all the signatures under the same delegation condition. The proxy unlinkability holds if and only if there is no conjunction between (d, sk_2,e') and (msg, $Info_w$, s, e,L) . This is obvious from Equations (5)-(10). The value d is only included in Equation (6) and connected to *e* through Equation (7). For this, one must be able to compute d which is masked with two random numbers. Similarly, e' and sk_2 may be associated with the signature through Equation (8) and (9) respectively. They fail again due to the random numbers. Even they are combined, the number of unknowns is still more than that of the equations. So, the proposed scheme provides indeed the proxy blindness property.

5. EFFICIENCY OF PROPOSED SCHEME

In Table 1, we can see that our scheme is more efficient and low computation cost than previous scheme [4], .[13], [14] and [15]. The detailed costs in each phase are compared with previous schemes. In this table, *T E* and *T M* denote the once running of modulo exponential and multiplication operations, respectively. *T H* denotes the once running of hash operations. In equation-6 d* is computed with out inverse calculation which eliminates extra computational complexity.

6. CONCLUSION

The system presents a new proxy blind signature scheme based on DLP. The proposed scheme satisfies the given security requirements and our proposed scheme has minimum computational cost when comparing with previous schemes. The future work is to design more effective proxy blind signature schemes and proxy blind signature schemes which provably secure in the standard model with satisfiable lower computational cost.

REFERENCES

[1] D. Chaum, "Blind Signature Systems", *Proceedings of Crypto'83*, Plenum, pp.153. [2] B. Lee, H. Kim, and K. Kim, "Strong proxy signature and its application", *Australasian Conference on Information Security and Privacy(ACISP'2001)*, LNCS2119, Springer-Verlag, Sydney, 2001, pp.603-608.

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

[4] Z. W. Tan, Z. J. Liu, and C. M. Tang, "A proxy blind signature scheme based on DLP", *Journal of Software*, Vol14, No11, 2003, pp.1931-1935.

[5] M. Mambo& K. Usuda and E. Okamoto, "Proxy Signatures for delegating signing operation", *Proc. 3rd ACM Conference on Computer and communications Security* , ACM Press, 1996. pp.48-57.

[6] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages", *IEICE Trans. Fundamentals*, 1996, Vol. E79-A, (9), pp.1338-1354.

[7] K. Zhang, "Threshold Proxy signature schemes", *1997 Information Security Workshop* , Janpan, 1997, pp.191-197.

[8] S. Kim, S. Park and D. Won, "Proxy signature. *Information and Communication Security"*, LNCS, Vol. 1334, Springer-Verlag, 1997, pp.223-232.

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

[10] S. H. Wang, G. L. Wang, F. Bao, and J. Wang, "Cryptanalysis of a proxy blind signature scheme based on DLP", *Journal of Software*, Vol. 16, No. 5, 2005,pp. 911–915.

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

[12] Q. S. Xue, and Z. F. Cao, "A new proxy blind signature scheme with warrant", *IEEE Conference on Cybernetics and Intelligent Systems (CIS and RAM 2004)*, Singapore, 2004, pp.1385-1390.

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

[14] Xuan Yang, Zhaoping Yu , "Efficient Proxy Blind Signature Scheme based on DLP", International Conference on Embedded Software and Systems (ICESS2008).

[15] Aung Nway Oo and Nilar Thein, "DLP based Proxy Blind Signature Scheme with Low-Computation", 2009 Fifth International Joint Conference on INC, IMS and IDC.