International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 3, ISSN 2249 –071X

A Secure and Efficient of Some New Blind Signature, Proxy and Partial Blind Signature Scheme Based on Discrete Logarithm Problem

Pankaj Sarde
[1]Department of Mathematics
Rungta College Of Engg. & Technology, Bhilai (C.G), India
Email: pnsarde@gmail.com

Amitabh Banerjee
Department of Mathematics
Govt. D. B. Girls' P.G. College, Raipur (C.G), India
Email: amitabh_61@yahoo.com

Abstract **- A blind signature scheme is a protocol for obtaining a signature from a signer such that the signer' view of the protocol can't be linked to the resulting message-signature pair. A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature and blind signature scheme. Partial blind signature scheme are an extension of blind signature scheme that allows a signer to explicitly include necessary information in the resulting signatures under some agreement with the receiver. In this paper we propose a secure and efficient of some new blind signature, proxy and partial blind signature scheme based on discrete logarithm problem.**

Keywords **- Blind signature, Proxy blind signature, Partially blind signature.**

I. INTRODUCTION

Digital signature is an essential component in cryptography. Depending on its application purpose, the digital signature can provide the required cryptographic properties: The concept of blind signature was introduced by Chaum in 1983 [1]. They allow a receiver to get a signature without giving the signer any information about the actual message or the resulting signature. This blindness property plays a central role in application such as electronic voting [2,3] and electronic cash schemes [1,4] where anonymity is of great concern. Recently, several blind signature schemes based on discrete logarithm problem have been proposed and discuss in [5, 6, 7]. In 1994, Carmenish et al. [5] introduced a blind signature scheme based on discrete logarithm problem. In 1995, Harn [6] pointed out that Carmenish et al's scheme can't satisfy the requirement of untraceability. In 2005, Lee et al [7] proposed an improved blind signature scheme. A secure blind signature scheme should satisfy the blindness and unforgeabilitry properties. The most important property of blind signature differing from the other signature is blindness which allows a user to acquire a signature on a message without revealing anything about the message to the signer. Blindness property ensures that no one can derive a link between a view and a valid blind signature except the signature requester. The other property is unforgeability; it means that only the signer can generate valid signature. On the other hand in 1996, Mambo, Usudo and Okamoto [8,9] proposed a new concept, called proxy signature. In this scheme an original signer delegates his signing authority to another signer in such a way that the proxy signer can sign any message on behalf of the original signer and the verifier can verify and distinguish between normal signature and proxy signature. As a result, the verifier can be convinced of the original signer's agreement on the signed message. Proxy signature schemes have been shown to be useful in many applications. For example, a manager can delegate his secretaries to sign document when he is on vacation. Proxy signature schemes can also be used in electronics transaction [10] and mobile agent environment [11]. A proxy blind signature schemes is a digital signature schemes which contains the properties of proxy signature and blind signature. In a proxy blind signature scheme, the proxy signer is allowed to generate a blind signature on behalf of the original signer. The proxy blind signature consists of the following properties:

- **Distinguish-ability:** The proxy blind signature must be distinguishable from the normal signature.
- **Unforgeability:** Only the designated proxy signer can create the proxy blind signature.
- **Unlinkability:** When the signature is revealed, the proxy signer can't identify the association between the message and blind signature be generated.
- **Verifiabilty:** The proxy blind signature can be verified by everyone.

In 2002, Tan, Liu and Tang [12] proposed two proxy blind signature scheme based on DLP and ECDLP respectively. In 2003, Lal and Awasthi [13] proposed a more efficient and secure proxy blind signature scheme. On the other hand, the blindness property of the blind signature is undesirable in some situation. For example, in an e-cash system, the expiration date and the value of an e-cash should be imposed on the blind signature. Therefore the concept of partially blind signature was first introduced by Abe and Fujusaki [14] and allows a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. The common information is known and pre-agreed by the both the signer and the requester before the signing process. The partial blindness property preserves the untraceabilty of the blind signature and embeds the pre-agreed common information on the blind signature. Many Partial blind signature schemes [15, 16, 17, 18, 19] have been proposed to improve the security in the last few years. In this paper, we present three new signature schemes. The first is blind signature scheme based on discrete logarithm problem. The second is proxy blind signature scheme based on discrete logarithm

problem and third is partially blind signature scheme based on schnorr signature.

II. BASIC SETTING

O: the original signer
P: the proxy signer
p: a large prime number
q: a large prime factor of p-1
g: an element of Z^*_P
h(.): a secure one way hash function
F:$\{0,1\}^* \rightarrow$ <g> be public hash function
y: g^x is public key, x is private key of the signer

III. BLIND SIGNATURE SCHEME

First signer randomly select k_1, k_2, b_1, $b_2 \in Z_q$ such that gcd(k_1,k_2)=1 then

by extension Euclid algorithm there exist an integer e and w such that $k_1e+k_2w=1$. Now signer compute $r_1=g^{k_1} \bmod p$ and $r_2 = g^{k_2} \bmod p$ send it to the user.

- Now user select randomly $\alpha,\ \beta,\ \gamma \in Z_q$ and compute $R_1 = g^{\frac{\alpha}{2}} r_1^{\beta} \bmod p$, $R_2 = g^{\frac{\alpha}{2}} r_2^{\gamma} \bmod p$ such that gcd (R_1, q) =1, gcd(R_2, q)=1 otherwise again chooses α, β, γ . Next user unblind the message m1=h(m)R_1 mod q, m_2=h(m)R_2 mod q and send it to the signer.
- Now signer computes
  $m_{11}=m_1k_1ex + b_1x \bmod q$
  $m_{22}=m_2k_2wx+b_2x \bmod q$
  $T_1 = g^{b_1x} \bmod p$
  $T_2 = g^{b_2x} \bmod p$
  and send (m_{11}, m_{22}, T_1, T_2) to the user.
- Now user computes
  $s_1 = m_{11} R_2 \bmod q$
  $s_2 = m_{22} R_1 \bmod q$
  $s_{11} = g^{s_1} T_1^{-R_2} \bmod p$
  $s_{22} = g^{s_2} T_2^{-R_1}$
  $s = s_{11} s_{22}$
  $R = R_1 R_2$

and publish message signature pair [h(m), R, S] to the public. Then verifier verify the relation $S \equiv y^{h(m) R} \bmod p$. If this relation is true then [h (m), R, S] is a valid blind signatures.

IV. SECURITY ANALYSIS

Our scheme based on discrete logarithm problem. Signer computes r_1, r_2 any forger can't determine the secret value of k_1, k_2 since it is based on discrete logarithm problem. Suppose any forger randomly select $\alpha, \beta, \gamma \in Z_q$ and compute R_1, R_2, m_{11}, m_{22} but they can't compute m_1, m_2, T_1, T_2 because they don't have secret key x and also they didn't knew the secrete value of b_1, b_2, it is based on discrete logarithm problem. Thus our scheme is secure and efficient.

V. PROXY DELEGATION PHASE

- The original signer O compute $r_0 = g_0^{\ k} \bmod p,\ k_0 \neq 1$ and $R = x_0 + k_0 y_p \bmod q$, where k_0 is a random number, x_0 is private key of original signer; y_p is the public key of the proxy signer. Now O sends (R, r_0) to the proxy signer in a secure way.
- After receiving the secret value (R, r_0), proxy signer checks the validity of the secret value with the following congruence $g^R \equiv y_0 r_0^{y_p} \bmod p$ If (R, r_0) satisfies this congruence, he accept it as a valid proxy, otherwise reject it. In the later case the requests for another key. Proxy signer chooses randomly integer $k \in Z_q$ such that $r_1=g^k$ mod p send (R, r) to the user.
- User chooses randomly integer $\alpha, \beta, b_1, b_2 \in z_q$ such that gcd(b_1, b_2)=1, then by extension Euclid algorithm there exist an integer e and w such that $b_1e+b_2w=1$. Now user computes
  $r = g^{\alpha\beta R+\beta} r_1^{\alpha} \bmod p$
  $d = g^{R\alpha s+\beta} \bmod p$
  $s' = s - \beta \bmod q$
  where s=h(r//m) and send s' to the proxy signer.
- Proxy signer compute $T = k - s's_p \bmod q$ where $s_p = R + x_p \bmod q$ and x_p is the private of the proxy signer. Then signer sends T to the user.
- **Signing Phase:** Now user computes
  $u_1 = \alpha.b_1.e.T \bmod q$
  $u_2 = \alpha.b_2.w.T \bmod q$
  $v_1 = \alpha.s'.b_1.e \bmod q$
  $v_2 = \alpha.s'.b_2.w \bmod q$
  and
  $w_1 = g^{u_1} y_p^{v_1} \bmod p$, ...(1)
  $w_2 = g^{u_2} y_p^{v_2} \bmod p$
  and also computes

$w=w_1w_2$. Thus proxy blind signature is (m, u_1, u_2, v_1, v_2, d, s).

- **Verification Phase:** Any verifier first recover r. For this he/she compute w_1 and w_2 then recover $r = w_1w_2d$ and compute $s_1=h(r//m)$ then check the relation $s=s_1$ if this hold then (m,u_1,u_2,v_1,v_2,d,s) is a valid proxy blind signature.
- **Correctness:** To check the correctness of (1)

$$w_1 = g^{u_1} y_p^{v_1} \bmod p$$
$$= g^{\alpha b_1 eT} g^{x_p v_1}$$
$$= g^{\alpha b_1 eT} g^{x_p \alpha s' b_1 e}$$
$$= g^{\alpha b_1 e(k - s' s_p)} g^{x_p \alpha s' b_1 e}$$
$$= g^{\alpha b_1 ek} g^{-\alpha b_1 es' s_p} g^{x_p \alpha s' b_1 e}$$
$$= g^{\alpha b_1 ek} g^{-\alpha b_1 es'(R + x_p)} g^{x_p \alpha s' b_1 e}$$
$$= g^{\alpha b_1 ek} g^{-\alpha b_1 es' R}$$

and

$$w_1 = g^{u_2} y_p^{v_2} \bmod p$$
$$= g^{\alpha b_2 wT} g^{x_p v_1}$$
$$= g^{\alpha b_2 wT} g^{x_p \alpha s' b_2 w}$$
$$= g^{\alpha b_2 w(k - s' s_p)} g^{x_p \alpha s' b_2 w}$$
$$= g^{\alpha b_2 wk} g^{-\alpha b_2 ws' s_p} g^{x_p \alpha s' b_2 w}$$
$$= g^{\alpha k_2 wk} g^{-\alpha b_2 ws'(R + x_p)} g^{x_p \alpha s' b_2 w}$$
$$= g^{\alpha b_2 wk} g^{-\alpha b_2 ws' R}$$

VI. Security Analysis

- Here we use different congruence to check the validity of original signature and the proxy signature. Thus the original signature is distinguishable from the proxy signature.
- **Unforgeability:** Unforgeability means the original signer can't forge valid proxy signature, since we have

  s=h(r//m)

  where $r = g^{\alpha\beta R + \beta + \alpha k}$

  Without knowing the random integer $\alpha, \beta, k \in Z_q$, the original signer can't forge proxy blind signatures. Thus the designated proxy signer can create the proxy blind signature.
- **Undeniablity:** The proxy secret value compute from the relation $s_p=R+x_p \bmod q$ where x_p is the private key of the proxy signer. Since $R=x_0+k_0y_p \bmod q$ without knowing the secret value of x_0 and k_0, proxy signer can't determine the value of R. Thus proxy signer can't deny proxy blind signature that he has created on a given message on behalf of the original signer.
- **Verifiability:** We have proxy blind signature (m, u_1, u_2, v_1, v_2, d, s). Any verifier who has proxy public key y_p can easily check proxy blind signature on message m.

VII. Partial Blind Signature Scheme

7.1 Key generation

- First signer randomly select an integer $r, s, t \in_R z_q$ and z=F(info), compute $\alpha = g^t, \beta = g^s z^r$ and send it to the user.
- User randomly select an integer $u, v, w \in_R z_q$ and compute z= F(info), $p = \alpha^v g^u y^w$, $q = \beta z^{v+u} g^u$, $\alpha = H(p // q // z // msg)$, b=u-a and send (b v) to the signer in a secret channel.

7.2 Signing Phase:

- Now signer compute $c_1=b+s$, $c_2=s-bx+vt$, $c_3=b+r+v$ and send (c_1, c_2, c_3) to the user.
- Next user compute $d_1=c_1+a$, $d_2=c_2-d_1$, $d_3=w+b$, $d_4=c_3+a$, $d_5=w+u$ and publishes the signature (d_1, d_2, d_3, d_4, d_5) on message m with common information.

7.3 Verification: The signer can verify a given signature (d_1, d_2, d_3, d_4, d_5, info) by checking whether z= F(info), d_5-d_3=H ($g^{d2}y^{d3}//z^{d4}g^{d1}//z//msg$) if relation is true then (d_1, d_2, d_3, d_4, d_5, info) is valid partial blind signature on message m.

VIII. Security Analyses

Here we show partial blind signature scheme based on schnorr signature. In our scheme both the signer and user three parameters. A secure partial blind signature should satisfy the following properties and we show that our proposed scheme satisfies the following properties.

- **Partially Blindness:** Except for the common information, the signer can neither learn the message he sign nor recognize the signature the user obtains afterwards. In proposed Scheme user and signer first agreed on common information. Then signer selects randomly an integer $r, s, t \in_R Z_q$ and compute z=F(info), $\alpha = g^t \bmod p$, $\beta = g^s z^r \bmod p$ and send it to the user. Then user selects randomly an integer $u, v, w \in Z_q$ and compute z=F(info), $p=g^{vt-u+xw} \bmod p$, $q=g^{s+u} z^{v+u+r} \bmod p$ and a=h(p//q//z//msg). If user can successfully change or remove the common information from the signature (d_1, d_2, d_3, d_4, d_5, info) but he can't compute $c_2=s-bx+vt$, it is difficult to derive secret key x and value t since it is based on discreet logarithm problem. Suppose signer can change or remove the common information but without but without knowing u and w, he can't compute p and q. Thus signer and user is unable to change or remove the

common information while keeping the verification of signature successfully.

- **Unforgeablity:** Any attacker or user can't forge a signature that passes the verification in a partially blind signature scheme. It means that only the signer can generate the valid signature. Suppose any attacker tries to derive the signature (d_1, d_2, d_3, d_4, d_5) with common information for a given message. For example attacker taken d_1 and d_2 and check the value $d_1+d_2-2=c_2=s-bx+vt$. But they can't determine the value of x and t since it is based on discrete logarithm problem.

REFERENCES

[1] D.Chaum. Blind signature for untraceable payments. In. D. Chaum, R. Rivest, and A. sherman, editors, Advances in cryptology-Proceedings of crypto'82, pages 199-204. Prenum Publishing Co-operation, 1982.

[2] D. Chaum. Election with unconditionally-secret ballots and disruption equivalent to breaking RSA. In C. G. Gunther, editor, Advances in cryptology- Eurocrypt'88, volume 330 of lecture notes in computer sciences, pages 177-189. Springer-verlag, 1988

[3] A Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale election. In J. Seberry and Y. Zheng, editors, Advances in cryptology- AUSCRYPT'92, volume 718 of lecture notes in computer sciences, pages 244-251. Springer-verlag, 1993.

[4] D. Chaum, A. Fiat, and M. Naor. Untraceable electronic cash. Ins. Goldwasser, editor, Advances in cryptology-CRYPTO'88, volume 403 of lecture notes in computer sciences, pages 319-327. Springer-verlag, 1990.

[5] J. carmenisch, J. Piveteau and M. Stadler, "Blind signature based on discrete logarithm problem", Advances in cryptology EUROCRYPT'94, pp 428-432, 1994

[6] L. Harn, "Crytanalysis of the blind signatures based on discrete logarithm problem", Electronics letters, vol. 31 no. 14, pp 1136-1137, 1995.

[7] C. C. Lee, M. S. Hwang and W. P. Yang, "A new blind signature based on discrete logarithm problem for untraceability," Applied mathematics and computation,vol. 16 no.3, pp. 837-841, 2005.

[8] M. Mambo. K. Usada, and E. Okamoto 'Proxy signature delegation of the power to sign messages'. IEICE Trans. Fundamentals. Sep. 1996. Vol E79-A. No. 9 pp 1338-1353.

[9] M. Mambo, K. Usuda, E. Okamoto. Proxy signatures for delegating signing operation. In: 3rd ACM conference on computer and communications security (ccs'96), pp. 48-57. New York: ACM press. 1996.

[10] Kotzanikolaons, P., Burmcster, M. and chrisskopoulos, V.(2000).secure transactions with mobile agents in hostile environments, in 'proc. ACISP', LNCS 1841, pp. 289-297

[11] Lee. B., Kim H. and Kim K. (2000), secure mobile agent using strong non designated proxy signature, in' proc. of ACISP. LNCS 2119', Springer- Verlag pp. 474-486.

[12] Tan, Z. Liu, Z. and Tang, C. (2002), Digital proxy blind signatures cheme based on LP and ECDLP in 'MM Resarch preprints', No-21 MMRC, AMSS, Academia, Sinica, ejing, PP. 212-217.

[13] Lal, S. And Awathi. A. K.(2003), 'Proxy blind signature scheme', to appear in journal of informations science and Engineering. Cryptology e print Archive, Report 2003/072 Available at http:// eprint.iacr. org/

[14] Abe, M., E. Fujisaki, 1996. How to date b blind signatures. advances in cryptology-Asiacrypt 1996, LNCS 1163. Springer-Verlag, PP:244-251.

[15] C. I. Fan and C. I. Lei, "Low-computations partially blind signatures for electronic cash," IEICE Transactions on fundamentals of Electronics communications and computer science, 1998, Vol 81, no. 5. pp 818-824.

[16] M. Abe and T. Okamoto, " Provably secure partially blind signatuires, "Advances in cryptology- Crypto'00, Springer-Verlag, 2000, LNCS 1880, pp 271- 286.

[17] H. Y. Chien, J. K. Jan and Y. M. Tseng. "RSA- based partially blind Signature with low computation," IEEE International conference on parallel and distributed system, IEEE press, 2001. pp. 385-389.

[18] Q. H. Wu, W. Susilo and Y. Mu, "Efficient partially blind signature with provable security," ACIS' o6. Springer- Verlag, 2006, LNCS 3982, pp 345-354.

[19] T. Okamoto, "Efficient blind and partially blind signatures without random oracles," Tcc'06 Springer-verlag 2006, LNCS 3876, pp 80-99.

AUTHOR'S PROFILE

Pankaj Sarde

is a Senior Lecture in Rungta College of Engg. and Technology, Bhilai, Chhattisgarh, India. He has completed his B.Sc. degree in Mathematics from Science College of Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India in 1999 and his M.Sc. degree in pure Mathematics from Govt. Chhattisgarh College of Pt. Ravishankar Shukla University, Raipur, Chhattisgarh, India in 2001. He is perusing Ph.D. in the field of public key cryptography and digital signature under the guidance of Amitabh Banerjee.

Amitabh Banerjee

was awarded Ph.D. in 1996 by Pt. Ravishankar Shukla University, Raipur Chhattisgarh, India. At present he is Professor and Head, department of Mathematics in Govt. D. B. Girls' P.G. College, Raipur, Chhattisgarh, India. He has experienced himself in teaching under graduate and post graduate classes for 27 years. He has published many research papers in journal of National and International repute. His area of research is functional analysis, fixed point theory and now he has moved to the field of cryptography.