IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-7, Issue-6, June 2019 E-ISSN: 2347-2693

# Cloning attack on a Proxy Blind Signature Scheme over Braid Groups

**Manoj Kumar**

Dept. of Mathematics, Rashtriya Kishan Post Graduate College, Meerut Karnal Road Shamli, Utter Pradesh.-India- 247776

*Corresponding Author: yamu_balyan@yahoo.co.in*

DOI: https://doi.org/10.26438/ijcse/v7i6.152155 | Available online at: www.ijcseonline.org

Accepted: 09/Jun/2019, Published: 30/Jun/2019

***Abstract* -** Proxy blind signature scheme is a combination proxy signature and blind signature scheme. Verma proposed a proxy blind signature scheme over braid groups and claimed that his scheme is secure against all possible security lapses and also satisfy all essential security attributes. This paper analyzes Verma's proposed scheme and found that this scheme suffers with the serious security vulnerabilitie: cloning attack.

***Keywords*—**Public Key Cryptography, Braid group, Public key, Private key, Digital signature, Proxy signature

## I. INTRODUCTION

Concept of blind signature scheme was introduced by Chaum [4] in 1984. In a blind signature scheme, a protocol is played by two entities/parties in such a way that a user can obtain the signature of a valid signer on a message of his/her choice and on the other side the signer is not able to learn nothing about the signed message. However with such properties, a blind signature scheme is very much useful in several applications such as e-voting and e-payment [5] etc. For more detail on blind signature schemes, please refer to [4, 14, 20, 21, 25, 28, 37, 38].

On the other side, concept of proxy signature scheme was introduced by Mambo Usuda and Okamoto [29]. In a proxy signature scheme, an entity called original signer to transfer/ delegate its signing power/capabilities to a different entity called proxy signer and that proxy signer signs message on behalf of the original signer. Once the signature verifier receives the proxy signature, she /he can check the validity of the signature and identify the proxy signer and also verifies the original signer's agreement on the signed message. Based on delegation type, Mambo et al. [29] classified proxy signatures as

- Full Delegation
- Partial Delegation
- Delegation by Warrant

In case of full delegation, the original signer gives his/her private key to the proxy signer in a secure way. In case of partial delegation, original signer generates a proxy signature key by using his private key and then transfers securely this key to the proxy signer, who uses this proxy key to sign the message on behalf of original signer. In case of delegation by warrant, the proxy signer first obtains the warrant, which is a certificate comprised of a message part and a public signature key from the original signer, and then proxy signer uses the corresponding private key to sign the all concern messages. The final signature consists of the created signature and the warrant. For more detail on proxy signature schemes, please refer to [1, 2, 3, 8, 16, 24, 26, 27, 29, 30, 31, 32, 33, 34, 35, 36, 37]. A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature with 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. For more detail, please refer to [7, 14, 15].

This paper is organized as follows. Section II provides a brief idea of braid group and explains the difficulty of the computational version. In section III, we review Verma's proxy blind signature scheme over braid group. The securities flaw of Verma's proposed scheme are discussed in section IV. Finally, we conclude the work in section V.

## II. BRAID GROUPS

In this section, we give the basic definitions of braid groups and discuss some hard problems on those groups. For more information on braid groups, word problem and conjugacy problem, refer to the papers [5, 6, 7, 8, 12, 13, 15, 17]. A braid is obtained by laying down a number of parallel strands and intertwining them so that they run in the same direction. For each integer $n \geq 2$, the $n$-braid group $B_n$ is the group generated $\sigma_1\sigma_2 \dots \dots \dots \sigma_{n-1}$ with the relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ where $|i-j| \geq 2$ and $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ otherwise. The number $n$ is called the braid index and each element of $B_n$ is called $n$ - braid. Two braids $x$ and $y$ are said to be conjugate if there exist a braid $a$ such that $= axa^{-1}$ . For $m < n$, $B_n$

can be considered as a subgroup of $B_n$ generated by $\sigma_1\sigma_2 \ldots\ldots\ldots \sigma_{m-1}$.

In Braid Cryptography, let $G$ be a non-abelian group and $u, a, b, c \in G$. In order to perform the Diffie- Hellman key agreement on $G$, we need to choose $a$, $b$ in $G$ satisfying $ab = ba$ in the DHCP. Hence we introduce two commuting subgroups $G_1$, $G_2 \subset G$ satisfying $ab = ba$ for any $a \in G_1$, $b \in G_2$ .More precisely, the braid cryptography are based on the following decision problems.

- Input:

A non-abelian group , two commuting subgroups $G_1$, $G_2 \subset G$.

- Conjugacy Problem :

Given $(u, aua^{-1})$ with $u, a \in G$ , compute $a$. (Note that if we denote $aua^{-1}$ by $u^a$, it looks like the DLP.)

- Diffie-Hellman Conjugacy Problem:

Given $(u, aua^{-1}, bub^{-1})$ with $u, \in G, a, \in G_1\ b, \in G_2$ , compute $baua^{-1}b^{-1}$.

- Decisional Diffie-Hellman Conjugacy Problem:

Given $(u, aua^{-1}, bub^{-1}, cuc^{-1})$ with $u, c \in G, a, \in G_1\ b, \in G_2$ , decide whether $c = ba$.

In braids, we can easily take two commuting subgroups $G_1$, $G_2 \subset G$ of $B_n$ (For simplicity, we only consider a braid group with an even braid index. But it is easy to extend this to an odd braid index.). For example, $G_1 = LB_n$ (resp. $G_2 = RB_n$ ) is the subgroup of $B_n$ consisting of braids made by braiding left $\frac{n}{2}$ strands (resp. right $\frac{n}{2}$ strands) among $n$ strands. Thus $LB_n$ is generated by $\sigma_1\sigma_2 \ldots\ldots\ldots \sigma_{\frac{n}{2}-1}$ and $RB_n$ is generated by $\sigma_{\frac{n}{2}-1}, \ldots\ldots \sigma_{n-1}$. Then we have the commutative property that for any $a, \in G_1\ b, \in G_2$ , $ab = ba$.

We choose a sufficiently complicated $(l + r) -$ braid $\alpha \in B_{l+r}$.Then following is a one-way function.

$$(f: G_1 \times G_n \rightarrow G_n \times G_n , f(a, x) = (axa^{-1}, x)$$

There is an efficient time algorithm [16] for a given pair $(a, x)$ to compute $axa^{-1}$, but all the known attacks need exponential time to compute $a$ from $(axa^{-1}, x)$ . This one-way function is based on the difficulty of conjugacy problem.

## III. REVIEW OF VERMA'S SCHEME

This section reviews a proxy blind signature scheme over braid group [15]. In this scheme, to sign a message $\in [0,1]^*$ , Alice (original signer) transfers/delegates his signing capability to Bob( proxy signer). The steps are given below:

### A. *key generation*

Each user $u$ does the following steps.

- ✓ Selects a braid $x_u \in_R B_n$ such that $x_u \in SSS(x_u)$.
- ✓ Choose $x'_u$, $a_u \in_R RSSBG(x_u, d)$.
- ✓ Return public key as $pk = (x_u, x'_u)$ and secret key $sk = a_u$ .

### B. *proxy key generation*

Bob gets the proxy key pair as follows.

- ✓ The original signer Alice selects a braid $\alpha_o \in_R B_n$
- ✓ Alice computes $t_o = a_0 x a_o^{-1}$. Then, she sends the pair $(\alpha_o, t_o)$ to Bob through a secure channel.
- ✓ Bob checks whether $t_o x'_o \sim \alpha_o\, x_o$. If it is hold, he accept the key, otherwise reject it.

### C. *proxy blind signature generation*

Whenever Bob ( proxy signer) have to signs a document on behalf of Alice (original signer), Bob computes the following steps.

- ✓ Bob selects $b \in_R B_n$ and computes $\alpha = bx_pb^{-1}$ and reverts $(t_o, \alpha)$ to the user.
- ✓ Blinding: User selects $\delta = \in_R B_n\,(l))$ computes
$$t'_0 = \delta t_0 \delta^{-1} ,$$
$$\alpha' = \delta\alpha\delta^{-1}$$
$$h = H\{H_1(t'_o, x'_o) \parallel m\}$$
and sends $h$ to the proxy signer.
- ✓ Proxy signer computes $= bhb^{-1}$ , $\gamma = ba_p^{-1}ha_pb^{-1}$ and sends $(\beta, \gamma$ ) to the user .
- ✓ Unblinding: User computes
$$\beta' = \delta\beta\delta^{-1} \text{ and } \gamma' = \delta\gamma\delta^{-1}$$
and then $(\alpha', \beta', \gamma', t'_0)$ as a proxy blind signature on message $m$.

### D. *proxy blind signature verification*

The verification process of a proxy blind signature on a message $m$ consists the following steps.

- ✓ Verifier computes $h = H\{H_1(t'_o, x'_o) \parallel m\}$.
- ✓ Verifier checks whether $\alpha' \sim x_p$, $\beta' \sim h, \gamma' \sim h, \alpha'\, \beta' \sim x_p h$, $\alpha'\gamma' \sim x'_p\, h$, if it is hold, accept the signature, otherwise reject it.

## IV. SECURITY PITFALL: CLONING ATTACK

In this section, we introduced a different kind of security attack on Verma's proposed proxy blind signature scheme over braid group[15]. We named our attack as Cloning Attack. Cloning attack means an antagonist can generate a valid proxy blind signature (Cloned Proxy Blind Signature) only with the help of a previously generated proxy blind signature. The interesting fact is that Cloned Proxy Blind Signature can be generated without any knowledge of proxy secret key or other related secret parameters. The Cloned Proxy Blind Signature looks like as original signature and also satisfy all the properties/ requirements of the original signature. The following steps show that how an antagonist can mount a cloning attack on Verma's proxy blind signature over braid group. Suppose the antagonist had a valid blind signature $(\alpha', \beta', \gamma', t'_0)$ on the message $m$ ,which is generated by a valid proxy signer. Now, an antagonist, Charlie can generate a Cloned Proxy Blind Signature $(\alpha'', \beta'', \gamma'', t'_0)$, in the following way.

- ✓ Charlie selects a braid $\xi \in_R B_n$
- ✓ Charlie computes $\alpha'' = \xi\alpha'\xi^{-1}$, $\beta'' = \xi\beta'\xi^{-1}$ and $\gamma'' = \xi\gamma'\xi^{-1}$.

Now, we are in a condition to show that the fabricated proxy blind signature $(\alpha'', \beta'', \gamma'', t_0')$ is a Cloned Proxy Blind Signature on the message *m*.

### *A. cloned proxy blind signature verification*

In order to check the validity of a Cloned Proxy Blind Signature, any verifier runs the following steps.

✓Verifier computes $h = H\{H_1(t_o', x_o') \parallel m\}$.
✓Verifier checks whether $\alpha''\sim x_p$, $\beta''\sim h, \gamma''\sim h, \alpha''\ \beta''\sim x_p h,\ \alpha''\gamma''\sim x_p'\ h$, if it is hold, accept the signature, otherwise reject it.

Since, in the verification phase the first step is same as the original scheme, therefore this always holds truly. Obviously, all the conjugacy relations will hold truly. It can be proved easily as follows.

We have $\alpha'' = \xi\alpha'\xi^{-1},\ \because \alpha' = \delta\alpha\delta^{-1}$,

$\alpha'' = \xi\delta\alpha\delta^{-1}\xi^{-1},\ \because \alpha = bx_p b^{-1}$.

$\alpha''= \xi\delta bx_p b^{-1}\delta^{-1}\xi^{-1}$,

$\alpha'' = \xi\delta bx_p(\xi\delta b)^{-1}$ . $\because (ab)^{-1} = b^{-1}a^{-1}$

$\Rightarrow \alpha''\sim x_p$.

We can show that $\beta'' = \xi\beta'\xi^{-1}\ \because \beta' = \delta\beta\delta^{-1}$,

$\beta'' = \xi\delta\beta\delta^{-1}\xi^{-1},\ \because \alpha = bx_p b^{-1}$.

$\beta''= \xi\delta bhb^{-1}\delta^{-1}\xi^{-1}$,

$\beta'' = \xi\delta bh(\xi\delta b)^{-1}$ . $\because (\xi\delta b)^{-1} = b^{-1}\delta^{-1}\xi^{-1}$

$\Rightarrow \beta''\sim h$.

Similarly, we have $\gamma'' = \xi\gamma'\xi^{-1}\ \because\ \gamma' = \delta\gamma\delta^{-1}$

$\gamma'' = \xi\delta\gamma\delta^{-1}\xi^{-1},\ \because \gamma = ba_p^{-1}ha_p b^{-1}$.

$\gamma'' = \xi\delta ba_p^{-1}ha_p b^{-1}\delta^{-1}\xi^{-1}$,

$\gamma'' = \left(\xi\delta ba_p^{-1}\right)h(a_p b^{-1}\delta^{-1}\xi^{-1})$ . $\because (ab)^{-1} = b^{-1}a^{-1}$

$\gamma'' = \left(\xi\delta ba_p^{-1}\right)h(\xi\delta ba_p^{-1})^{-1}\ \because (\xi\delta ba_p^{-1})^{-1} = a_p b^{-1}\delta^{-1}\xi^{-1}$

$\Rightarrow \gamma''\sim h$ .

Now we have $\alpha'' = \xi\delta bx_p(\xi\delta b)^{-1}$ and $\beta'' = \xi\delta bh(\xi\delta b)^{-1}$, therefore,

$\alpha''\ \beta'' = \xi\delta bx_p(\xi\delta b)^{-1}\ \xi\delta bh(\xi\delta b)^{-1}$,

$= \xi\delta bx_p(b^{-1}\delta^{-1}\xi^{-1})\ \xi\delta bh(\xi\delta b)^{-1}$,

$= \xi\delta bx_p(b^{-1}\delta^{-1})(\xi^{-1}\ \xi)\delta bh(\xi\delta b)^{-1}, \because [(a)^{-1}a = Identity]$

$= \xi\delta bx_p(b^{-1}(\delta^{-1}\delta)bh(\xi\delta b)^{-1}$,

$= \xi\delta bx_p(b^{-1}b)h(\xi\delta b)^{-1}$,

$= \xi\delta bx_p h(\xi\delta b)^{-1}$,

$\Rightarrow \alpha''\ \beta''\sim x_p h$.

Now we have $\alpha'' = \xi\delta bx_p(\xi\delta b)^{-1}$ and $\gamma'' = \left(\xi\delta ba_p^{-1}\right)h(\xi\delta ba_p^{-1})^{-1}$, therefore,

$\alpha''\gamma'' = \xi\delta bx_p(\xi\delta b)^{-1}\left(\xi\delta ba_p^{-1}\right)h(\xi\delta ba_p^{-1})^{-1}$,

$= \xi\delta bx_p(b^{-1}\delta^{-1}\xi^{-1})\left(\xi\delta ba_p^{-1}\right)h(\xi\delta ba_p^{-1})^{-1}, \because [(a)^{-1}a = Identity]$

$= [\xi\delta bx_p(b^{-1}\delta^{-1}\xi^{-1})][\left(\xi\delta ba_p^{-1}\right)h(a_p b^{-1}\delta^{-1}\xi^{-1})]$,

$= \xi\delta bx_p\left(\xi\delta ba_p^{-1}\right)h(a_p b^{-1}\delta^{-1}\xi^{-1})$,

$= \xi\delta ba_p^{-1}a_p x_p\ a_p^{-1}\ h(a_p b^{-1}\delta^{-1}\xi^{-1})$,

$= \xi\delta ba_p^{-1}(a_p x_p\ a_p^{-1})\ h(a_p b^{-1}\delta^{-1}\xi^{-1})$,

$= \xi\delta ba_p^{-1}x_p'\ h(a_p b^{-1}\delta^{-1}\xi^{-1})$,

$= \xi\delta ba_p^{-1}x_p'\ h(\xi\delta ba_p^{-1})^{-1}, \because (\xi\delta ba_p^{-1})^{-1} = a_p b^{-1}\delta^{-1}\xi^{-1}$

$\Rightarrow \alpha''\gamma''\sim x_p'\ h$

Here, we should note that original proxy blind signature and Cloned Proxy Blind Signature are statistically indistinguishable in all the way. It is clear that the Cloned Proxy Blind Signature also satisfies all the verification steps successfully, so we can assume that the verifier accept the Cloned Proxy Blind Signature as a real proxy blind signature.

## V. CONCLUSIONS

This paper proves that the proposed scheme has serious securities vulnerability: cloning attack. It is clear that the original signature and Cloned Signature are identical and statistically indistinguishable in all the way. In this way the Cloned Proxy Blind Signature also satisfies all the verification steps successfully and the server provides the access right to the attacker.

## REFERENCES

[1] Boldyreva, A. Palacio and B. Warinschi, Secure proxy signature schemes for delegation of signing rights, available at *http://eprint.iacr.org/2003/096*.

[2] B. Lee, H. Kim, and K. Kim, Strong proxy signature and its applications, *in the Proceedings of SCIS2001*, pp. 603-608,2001.

[3] Cao. T., Lin. D., and Xue. R., Improved privacy-protecting proxy signature scheme, Proc. of AWCC'04 - *Advanced Workshop on Content Computing*, Chi-Hung Chi, and Kwok- Yan Lam (Eds.), Volume 3309 of *LNCS*, pp.208-213, Spring-Verlag,2004.

[4] D. Chaum, Blind signature systems, Proceedings of Crypto 83, pp. 153- 158, Springer Verlag, 1984.

[5] D. Chaum, A. Fiat, M. Naor, Untraceable electronic cash, Proceedings of Crypto 88, LNCS - 403, pp. 319-327, Springer Verlag, 1988.

[6] D. Hofheinz and R. Steinwandt, A practical attack on some Braid group based cryptographic primitives, in *Public key Cryptography, PKC* 2003 proc., *LNCS* - 2567, pp. 187-198, Springer Verlag 2002.

[7] D. Pointcheval and J. Stern, Probably secure blind signature schemes, Proc. Asiacrypt-96, LNCS - 1163, pp. 252-265, Springer Verlag, 1996.

[8] Dai. J., Yang. X., and Dong. J., A privacy-protecting proxy signature scheme and its application, *Proc. of The 42nd annual Southeast regional conference*, *ACM* Southeast Regional Conference, pp.203-206, 2004.

[9] E. A. Elrifai and H. R. Morton, Algorithms for positive braids, *Quart. J. Math. Oxford* 45 (1994), 479-497.

[10] E. Lee, S. J. Lee and S. G. Hahn, Pseudorandomness from braid groups, *Advances in Cryptology*, Proceedings of Crypto 2001, *LNCS*- 2139, ed. J. Kilian, Springer-Verlag (2001), 486- 502.

[11] Emil Artin, Theory of Braids, *Annals of Math*, 48, pp. 101- 126, 1947.

[12] F. A. Garside, The braid group and other groups, *Quart. J. Math. Oxford* 20 (1969), no. 78, 235-254.

[13] F. Zhang and K. Kim. ID-Based Blind Signature and Ring Signature from Pairings. In Proceedings of ASIACRYPT 2002, LNCS-2501, pp. 533-547, Springer-Verlag, 2002.

[14] F. Zhang and K. Kim. Efficient ID-Based Blind Signature and Proxy Signature. In Proceedings of ACISP 2003, LNCS 2727, pp. 312-323, Springer-Verlag, 2003.

[15] G. K. Verma, A proxy blind signature schemes over Braid groups, International Journal of Network Security, Vol.9, No.3, pp. 214 - 217, Nov. 2009.

[16] Guo. L.,Wang. G., and Bao. F., On the security of a threshold proxy signature scheme using self-certified public keys, Proc. Of CISC'05 - *The SKLOIS conference on information security and cryptology*, Higher Education Press of China. Dec. 15-17, 2005.

[17] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Van and J. S. Cheon, An efficient implementation of Braid groups, Proc. Of Asiacrypt-2001, *LNCS* -2248, pp. 144-156, Springer Verlag, 2001.

[18] J. S. Birman, Braids, links, and mapping class groups,*Annals of Math*, study 82, Princeton University Press (1974).

[19] J. S. Birman, K. H. Ko and S. J. Lee, A new approach to the word and conjugacy problem in the braid groups,*Advances in Mathematics* 139 (1998), 322-353.

[20] J. Zhang, T.Wei, J. Zhang andW. Zou. Linkability of a Blind Signature Scheme and Its Improved Scheme. In Proceedings of ICCSA 2006, LNCS 3983, pp. 262-270, Springer-Verlag, 2006.

[21] J. Zhang and W. Zou. Linkability of a Blind Signature Scheme. In Proceedings of ICICIC 2006, Vol. 1, pp. 468-471, IEEE, 2006.

[22] K. H. Ko, D. H. Choi, M. S. Cho and J. W. Han, New signature scheme using conjugacy problem, 2002, *available at http://eprint.iacr.org/2002/168.*

[23] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. S. Kang and C. S. Park, New public key cryptosystem using Braid groups, Proc. Crypto-2000, *LNCS*-1880, pp. 166- 183, Springer Verlag 2000.

[24] K. Manoj, Security analysis of a proxy signature scheme over Braid groups, *Cryptology eprint archieve report*, http://www.eprint.iacr.org/2009/158, 2009.

[25] K. Manoj, Linkability of Blind Signature Schemes over Braid Groups, *Cryptology eprint archieve report*, http://www.eprint.iacr.org/2009/192, 2009.

[26] K. Zhang, "Threshold proxy signature schemes," in the Proc of *Information Security Workshop*, Japan, pp. 191-197, 1997.

[27] L. Li., S.Tzeng, M. Hwang, : Generalization of proxy signature-based on discrete logarithms, *Computers & Security*, Vol. 22(3),pp.245-255, Elsevier Science, 2003.

[28] M. Abe and T. Okamoto. Provably Secure Partially Blind Signature. In Proceedings of CRYPTO 2000, LNCS 1880, pp.271-286, Springer-Verlag, 2000.

[29] Mambo. M., Usuda. K., and Okamoto. E., Proxy signatures for delegating signing operation, Proc. of 3rd ACM *Conference on Computer and Communications Security*, pp.48-57, *ACM* press, 1996.

[30] S. H. Nagore and M. R. Sekhar, Nonrepudiable threshold proxy signatures with tracebility property, *Far East Journal of Applied Mathematics*, Vol. 6(3), pp. 233-240, 2002.

[31] S. J. Kim, S. J. Park, D. H.Won, Proxy Signatures, revisited, in the *Proceedings of ICICS*'97, *LNCS* - 1334, pp. 223-232, Springer-Verlag.

[32] S. Kim, S. Park and D. Won, Proxy signatures: Revisited, in Y. Han, T. Okamoto, S. Quing, editors, *Proceedings in InternationalConference on Information and CommunicationsSecurity* (ICICS), of *LNCS*- 1334, pp 223-232, Springer Verlag, 1993.

[33] Sun. H., and Hsieh. B., On the security of some proxy signature schemes, *Cryptology ePrint Archive: Report 2003/068, available at http://eprint.iacr.org/2003/068*.

[34] Tan. Z., Liu. Z., andWang. M., On the security of some nonrepudiable threshold proxy signature schemes, Proc. of ISPEC' 05 - *First International Conference on Information SecurityPractice and Experience*, Robert H. Deng, Feng Bao, Hwee- Hwa Pang, and Jianying Zhou (Eds.), Volume 3439 of *LNCS*, pp.374-385. Springer-Verlag, 2005.

[35] Wang. G., Bao. F., Zhou. J., and Deng. R.H., Comments on a Threshold Proxy Signature Scheme Based on the RSA Cryptosystem, *Cryptology ePrint Archive: Report 2004/054, available at http://eprint.iacr.org/2004/054*.

[36] Wang. G., Bao. F., Zhou. J., and Deng. R.H., Security analysis of some proxy signatures, Proc. of ICISC'03 - *6th International Conference on Information Security and Cryptography*, Jong In Lim, and Dong Hoon Lee (Eds.), Volume 2971 of *LNCS*, pp.305-319, Springer-Verlag, 2003.

[37] Tan, Z., Liu, Z. and Tang, C. (2002), Digital proxy blind signature schemes based on DLP and ECDLP, in MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing, pp. 212-217.

[38] Z. Huang, K. Chen, Y. Wang. Efficient Identity-Based Signatures and Blind Signatures. In Proceedings of CANS 2005, LNCS 3574, pp. 120-133, Springer-Verlag, 2005.

## Authors Profile

**Manoj Kumar** is working in Department of Mathematics, R. K. College Shamli, U.P. - INDIA-247776. He is a member of Indian Mathematical Society, Indian Society of Mathematics and Mathematical Science, Ramanujan Mathematical society, and Cryptography Research Society of India. He is working as a reviewer for some International peer review Journals: Journal of System and Software, Journal of Computer Security, International Journal of Network Security, The computer networks, computer and security, The Computer Journal. He is also working as a Technical Editor for some International peer review Journals- Asian Journal of Mathematics & Statistics, Asian Journal of Algebra, Trends in Applied Sciences Research, Journal of Applied Sciences. He has published his research works at National and International level. His current research interests include Cryptography and Applied Mathematics.