Linkability of Blind Signature Schemes over Braid Groups

Manoj Kumar
Department of Mathematics
R. K. College Shamli-Muzaffarnagar, U.P.-India- 247776
E-mail: yamu_balyan@yahoo.co.in

Abstract

Blindness and unforgeability are two essential security requirements of a secure blind signature scheme. Blindness means that after interacting with various users, the signer can never be able to link a valid message pair. Blindness is meaningless if after interacting with various users, the signer is able to link a valid message signature pair. This security vulnerability is known as linkability attack. Recently, Verma proposed two blind signature schemes over braid groups. Verma claimed that the proposed schemes are secure against all possible security vulnerabilities and also satisfy all essential securities properties.This paper reviews Verma's proposed blind signature schemes and found that these scheme do not withstand against the linkability vulnerability.

1. Introduction

The concept of blind digital signatures was first introduced by Chaum [1]in 1983 .Informally, a blind signature scheme is a protocol played by two parties in which a user obtains a signers signature for a desired message and the signer learns nothing about the message except its length. Blind signature is a key idea for constructing various anonymous electronic cash instruments. These are instruments for which the bank can not trace where (and hence for what purpose) a user spends her/his electronic money. The security of blind signature scheme [4, 19, 21]should guarantee that only a valid authority of the bank can generate a valid signature and it is difficult for the user to forge a signature of any additional document, even after getting from the bank a number of blind signatures. Blindness (unlinkability) is also an essential property of blind signature. Blindness (unlinkability) means after interacting with various user, the signer is not abler to link a valid signature pair. With such properties, the blind signature scheme are useful in several applications such as electronic voting and electronic payment.Blindness is meaningless if any how after interacting with various users, the signer is able to link a valid message signature pair. This security vulnerability is known as linkability attack [14, 20, 15].

On the other side,within the last years several attempts have been made to derive cryptographic primitives from braid groups. These finitely presented groups are well-studied [12] and various proposals have been made for deriving cryptographic primitives from the conjugacy problem in these groups. In 2000, Ko et. al. proposed a key agreement protocol and a public key encryption scheme based upon braid groups [17]. The schemes based upon braid groups [3, 16] are analogous to the Diffie-Hellman key agreement scheme and the ElGamal encryption scheme on abelian groups. Their basic mathematical problem is the Conjugacy Problem (CP) on braids: For a braid group B_n, we are asked to find a braid *a* from $u, b \in B_n$satisfying $b = aua^{-1} \in B_n$. The security is based on the *Diffie-Hellman Conjugacy Problem* (**DHCP**) to find $baua^{-1}b^{-1} \in B_n$ for given $u, aua^{-1}, bub^{-1} \in B_n$for *a* and *b* in two commuting subgroups of B_n respectively.

In 2008, Verma [11] proposed two blind signature schemes over braid groups.Verma [11] claimed that the proposed schemes are secure against all possible security attacks and also satisfy all essential properties.This paper reviews Verma's proposed scheme and found that this scheme is vulnerable to linkability attack. This paper is organized as follows.

Section - 2 provides a brief idea of braid groups. In section - 3, we review Verma's blind signature scheme over braid groups. The securities vulnerabilities of Verma's proposed blind signature schemes are discussed in section - 4. Finally, we conclude the work in section - 5.

2 Braid Groups

In this section, we give the basic idea 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, 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 by $\sigma_1\sigma_2, ..., \sigma_{n-1}$ 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 $y = axa^{-1}$. For $m < n$,B_m can be considered as a subgroup of B_n generated by $\sigma_1\sigma_2, ..., \sigma_{m-1}$.

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 $a \in G_1$ and $b_2 \in G_2$. More precisely, the the braid cryptography are based on the following decision problems.

- `Input`:
  A non-abelian group *G*, 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 $u \in G, a \in G_1$ and $b \in G_2$, compute $baua^{-1}b^{-1}$.
- `Decisional Diffie-Hellman Conjugacy Problem`:
  Given$(u, aua^{-1}, bub^{-1}, cuc^{-1})$ with $u, c \in G, a \in G_1$ and $b \in G_2$, decide whether *c* = *ba*.

In braids, we can easily take two commuting subgroups G_1 and G_2 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 $n/2$ strands(resp. right $n/2$ strands) among n strands. Thus LB_n is generated by$\sigma_1\sigma_2, ..., \sigma_{n/2-1}$ and RB_n is generated by $\sigma_{n/2-1}, ..., \sigma_{n-1}$. Then we have the commutative property that for any $a \in G_1$and $b \in G_2$, *ab* = *ba*. We choose a sufficiently complicated $(l+r)$-braid $\alpha \in B_{l+r}$.Then following is a one-way function.

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

There is an efficient time algorithm [17] 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.

3 Review of Verma's Blind Signature Schemes

This section reviews blind signature schemes over braid group [11]. The parameters *n, l, d* are fixed as in [17] and the concatenation of two strings in $(0, 1)^*$ is represented by $\|$. Let $m \in (0, 1)^*$ be the message to be signed and $H : (0, 1)^* \longrightarrow B_n(l)$ be a one way hash function. Before involving in the signing processing,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 $sk = a$.

Now we are in a position to review Verma's blind signature schemes over braid group [11].

3.1 Scheme I

- BLINDING: The user selects $\alpha \in_r RB_n$ and computes $t = \alpha y \alpha^{-1}$ where $y = H(m)$ and sends *t* to signer.

- **Signing**: Signer computes $\sigma^{'} = ata^{-1}$ and sends back to the user.

- Unblinding: User computes $\sigma = \alpha^{-1}\sigma^{'}\alpha$ and then (σ, m) be the message signature pair.

- *Verification*: verifier accepts the signature if and only if $\sigma \sim y$ and $\sigma u^{'} \sim yu$.

3.2 Scheme II

- Signer chooses $(\alpha = bxb^{-1}, b) \in_R RSSBG(x, d)$and sends α as a commitment.

- BLINDING: The user selects $\delta \in_r RB_n$ and computes $\alpha^{'} = \delta\alpha\delta^{-1}$and $h = H(m \parallel \alpha^{'})$ and sends *h* to the signer.

- **Signing**: Signer computes $\beta = bhb^{-1}$,$\gamma = ba^{-1}hb^{-1}$ and sends β, γ back to the user.

- Unblinding: User computes $\beta^{'} = \delta\beta\delta^{-1}$ and $\gamma^{'} = \delta\gamma\delta^{-1}$ and then $(\alpha^{'}, \beta^{'}, \gamma^{'})$ is a signature on the message *m*.

- *Verification*: verifier accepts the signature $(\alpha^{'}, \beta^{'}, \gamma^{'}, m)$ if and only if $\alpha^{'} \sim x, \beta^{'} \sim h, \gamma^{'} \sim h, \alpha^{'}\beta^{'} \sim xh$ and $\alpha^{'}\gamma^{'} \sim x^{'}h$.

4 Security Analysis of Verma's Proxy Blind Signature Schemes over braid groups

This section analyzes the security of blind signature schemes over braid group[11]. This section proves that both the proposed schemes do not satisfy the unlinkability property, which one of the essential security requirement of a secure blind signature scheme. In both the proposed scheme, after interacting with various users the signer is able to link a valid message signature pair. This attack is known as linkability attack.

4.1 Linkability Attack of Scheme-I

In the scheme-I, during the interactive protocol execution between the signer and user, the signature (σ, m) is generated. For the signer, in order to establish a link between revealed message and blind information, the signer records owned all the generated information, such as $\sigma_i^{'}, t_i$. After the signature (σ_i, m_i) is revealed , the signer executes the following steps:

1. Set the value t_i.
2. Select a valid signature pair (σ_i, m_i).
3. Computes $y_i = H(m_i)$.
4. Check the conjugacy relation $t_i \sim y_i$, if it is hold go to next step, otherwise go to step-I and set a different value of t_i.
5. Check the conjugacy relation $t_i \sim \sigma_i$, if it is holds it means the singer has managed to link a valid signature $(\sigma_i, m_i)$with the blind information t_i.

In the Scheme-I, since $t_i = \alpha_i y_i \alpha_i^{-1}$,$\sigma_i^{'} = a_i t a_i^{-1}$ and $\sigma_i = \alpha_i^{-1}\sigma_i^{'}\alpha_i$, therefore every selected t_i will only be mapped on its corresponding y_i and σ_i. In this way, the Verma's I blind signature over braid group [11]is vulnerable to linkability attack and the signer is able to link a valid signature $(\sigma_i, m_i)$with the blind information t_i.

4.2 Linkability Attack of Scheme-II

In the scheme-II, during the interactive protocol execution between the signer and user,$(\alpha^{'}, \beta^{'}, \gamma^{'})$ is a signature on the message *m*. For the signer, in order to establish a link between revealed message and blind information, the signer records owned all the generated information, such as $\alpha_i, \beta_i, \gamma_i$. After the signature $(\alpha_i^{'}, \beta_i^{'}, \gamma_i^{'}, m_i)$ is revealed , the signer executes the following steps:

1. Set the value α_i
2. Select a valid signature pair $(\alpha_i^{'}, \beta_i^{'}, \gamma_i^{'}, m_i)$.
3. Computes $y_i = H(m_i)$.

4. Check the conjugacy relation $\alpha_i \sim \alpha_i^{'}$, if it is hold go to next step, otherwise go to step-1 and set a different value of α_i.

5. Set the value β_i.

6. Check the conjugacy relation $\beta_i \sim \beta_i^{'}$,if it is hold go to next step, otherwise go back to step-4 and set a different value of β_i.

7. Set the value γ_i.

8. Check the conjugacy relation $\gamma_i \sim \gamma_i^{'}$,if it holds it means the singer has managed to link a valid signature pair, otherwise go back to step-5 and set a different value of γ_i.

In the Scheme-II, $\alpha_i = b_i x b_i^{-1}$, $\beta_i = b_i h_i b_i^{-1}$ and $\gamma_i = b_i a^{-1} h_i b_i^{-1}$. On the otherside,$\alpha_i^{'} = \delta_i \alpha_i \delta_i^{-1}$,$\beta_i^{'} = \delta_i \beta_i \delta_i^{-1}$ and $\gamma_i^{'} = \delta_i \gamma_i \delta_i^{-1}$. It can be observed easily that every selected transcription $\alpha_i, \beta_i, \gamma_i$ will only be mapped on its corresponding transcription $(\alpha_i^{'}, \beta_i^{'}, \gamma_i^{'}, m_i)$. In this way, the Verma's II blind signature over braid group [11]is vulnerable to linkability attack and the signer is able to link a valid message signature $(\alpha_i^{'}, \beta_i^{'}, \gamma_i^{'}, m_i)$ with the blind information $\alpha_i, \beta_i, \gamma_i$.

5 Conclusions

This paper has reviewed the security of Verma's blind signature schemes over braid groups. In Verma's scheme the signer is able to link the blind information to a valid revealed signature pair. The discussion has proved that the proposed scheme does not satisfy the unlinkability/blindness property, which one of the essential security requirement of a blind signature scheme.

References

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

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

[3] 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.

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

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] G. K. Verma, Blind signature schemes over Braid groups, *Cryptology eprint archieve report* http://www.eprint.iacr.org/2008/027, 2008.

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

[13] 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.

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

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

[16] 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.*

[17] 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.

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

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

[20] S. H. Heng, W. S. Yap and K. Khoo, Linkability of Some Blind Signature Schemesn, Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems, LNCS - 4462, Springer Berlin / Heidelberg, pp. 80 - 89,2007

[21] Z. Tan, Z. Liu, and C.Tang, Digital proxy blind signature schemes based on DLP and ECDLP, in MM Research Preprints, No. 21, MMRC, AMSS, Academia, Sinica, Beijing, pp. 212217,2002.

Manoj Kumar received the B.Sc. degree in mathematics from Meerut University Meerut, in 1993; the M. Sc. in Mathematics (Gold medalist) from C.C.S.University Meerut, in 1995; the M. Phil. (Gold medalist) in Cryptography, from Dr. B. R. A. University Agra, in 1996; the Ph.D. in Cryptography, in 2003. He also qualified the National Eligibility Test (NET), conducted by Council of Scientific and Industrial Research (CSIR), New Delhi- India, in 2000. He also taught applied Mathematics at D. A. V. College, Muzaffarnagar, India from Sep 1999 to March 2001; at S.D. College of Engineering & Technology, Muzaffarnagar- U.P. - INDIA from March 2001 to Nov 2001; at Hindustan College of Science & Technology, Farah, Mathura- U.P. - INDIA, from Nov 2001 to March 2005. In 2005, the Higher Education Commission of U.P. has selected him. Presently, he is working in Department of Mathematics, R. K. College Shamli- Muzaffarnagar- 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.