Probable Security Proof of a Blind Signature Scheme over Braid Groups

Girraj Kumar Verma

Department of Mathematics, Hindustan College of Science and Technology
Agra-Delhi Highway (NH-2), Farah, Mathura 281122, India (Email: girrajv@gmail.com)
(Received June 19, 2009; revised and accepted Nov. 2, 2009)

Abstract

In this paper, we reinvestigate the security analysis of blind signature scheme over braid groups proposed by Verma in 2008. A blind signature scheme is a cryptographic primitive used for e-commerce for getting a signature from the signer without revealing any information about its contents. These schemes are especially used in e-transactions, e-votings, DRM systems, etc. The security of blind signature is basically defined by two properties blindness and unforgeability. Here we prove a special form of unforgeability called one more forgery defined by Pointcheval et al. Although, Verma has defined the same and discussed the security analysis using a stronger assumption called chosen target conjugator search problem. In this paper, we also discuss the analysis using a simple problem, which is much closer to conjugate search problem.

Keywords: Blind signature, unforgeability, braid groups, conjugality problem, probable security

1 Introduction

The concept of blind signatures was introduced by Chaum [3]. A blind signature scheme is a cryptographic primitive in which two entities a user and a signer are involved. It allows a user to obtain a signature from the signer without revealing any information about the message or message signature pair after signature generation [4, 12]. The security arguments given by Pointcheval et al. [8] are much concrete to analyze the security of a blind signature scheme.

The braid groups were first introduced to construct a key agreement protocol and a public key encryption scheme [5] and a digital signature scheme [6] was introduced by Ko et al. Later some other signature schemes [9, 10, 11] were proposed using conjugality problem over braid groups. In 2009, Kumar [7] has discussed the security flaws in blind signature scheme [9]. He has discussed the unlinkability of the proposed scheme, but has given no comment about the unforgeability of the scheme. In this paper, we will analyze the security of blind signature scheme over braid groups proposed in the random oracle model [9]. Although, Verma has defined the same and discussed the security analysis using a stronger assumption called chosen target conjugator search problem. In this paper, we discuss the analysis using a simple problem, which is much closer to Conjugality search problem considered in [6]. In braid groups, the decision version of conjugality problem is easy and searching of conjugator is hard. This gap between two versions has been used for proving the security.

The rest of the paper is organized as follows: In Section 2, we define security properties of a blind signature scheme and some problems over braid groups. In Section 3, we discuss Verma's scheme [9] and then provide the security analysis. In Section 4, we conclude our discussion.

2 Preliminaries

2.1 Security Properties of Blind Signature

A blind signature scheme is a cryptographic primitive involving two entities: an user and a signer. So, we consider the user as an adversary for providing the security proof. In this subsection, we describe the required security properties of a blind signature scheme [8].

Unforgeability. The standard notion of unforgeability under chosen message attack of digital signatures cannot be used as a notion of unforgeability for blind signatures since their construction a user has to be able to produce a valid signature of a previously signed message. Here we consider a special form of *unforgeability*, namely, the user that has been engaged in l runs of the blind signing protocol, should not be able to obtain more than l signatures. This formalization of security for blind signature is called security against *one more forgery* [8].

Unlinkability. When the signature is verified, the signer knows nothing about the message or its signature.

2.2 Braid Groups and Conjugality Problem

In this section, we give a brief description of the braid groups and discuss some hard problem related to conjugality search problem. For more information on braid groups, word problem and conjugality problem please refer to [1, 2, 5, 6].

Definition 1. *For each integer n, the n-Braid group B_n is defined to be the group generated by $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ with the relation:*

1) $\sigma_i\sigma_j = \sigma_j\sigma_i$, Where $\mid i-j \mid \geq 2$.

2) $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$, Otherwise.

The integer n is called braid index and each element of B_n is called an n-braid.

In this section, we describe some mathematically hard problems over braid groups. We say that two braids x and y are conjugate (written as $x \approx y$) 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 $\sigma_1, \sigma_2, \cdots, \sigma_{m-1}$.

Definition 2. *Conjugality Decision Problem (CDP):*
Instance: $(x, y) \in B_n \times B_n$ such that $y = axa^{-1}$ for some $a \in B_n$.
Objective: Determine whether x and y are conjugate or not.

Definition 3. *Conjugality Search Problem (CSP):*
Instance: $(x, y) \in B_n \times B_n$ such that $y = axa^{-1}$ for some $a \in B_n$.
Objective: To find $b \in B_n$ such that $y = bxb^{-1}$.

Definition 4. *Matching Triplet Search Problem (MTSP) [6]:*
Instance: A CSP hard pair $(x, x' = axa^{-1}) \in B_n \times B_n$ and $y \in B_n$.
Objective: Find a triplet $(\alpha, \beta, \gamma) \in B_n \times B_n \times B_n$ such that $\alpha \approx x$, $\beta \approx \gamma \approx y$, $\alpha\beta \approx xy$ and $\alpha\gamma \approx x'y$.

In [6], Ko et al. have considered that CSP and MTSP have approximately the same complexity.

Since braid group B_n is an infinite group, so it is impractical to use B_n for cryptographic purposes. As in [6, 9] for a positive integer l, we take $B_n(l)$ as the set of all braids from B_n having canonical length at most l. So for each braid b in $B_n(l)$, we can write $b = \Delta^u\pi_1\pi_2\cdots\pi_l$, where Δ is called the fundamental braid and π's are permutations from Z_n to Z_n. Hence $\mid B_n(l) \mid \leq (n!)^l$.

Now there is an efficient polynomial time algorithm in [6] for solving CDP in $B_n(l)$ but CSP is still exponential time to solve. So, this gap between two problems has been used by cryptographers to develop cryptographic protocols [5, 6, 9, 10, 11].

3 Proposed Security Analysis

3.1 Signature Scheme by Verma

In this section, we are giving blind signature scheme by Verma [9]. The parameters n, l, d are fixed as in [6, 9] and the concatenation of two strings in $\{0,1\}^*$ is represented by $\|$. Let $m \in \{0,1\}^*$ be the message to be signed and $H : \{0,1\}^* \rightarrow B_n(l)$ and $H_1 : B_n(l) \rightarrow \{0,1\}^*$ be two one-way hash functions.

Key Generation. Each user does the following steps:

1) Selects a braid $x \in B_n(l)$ such that $x \in SSS(x)$;
2) Chooses $(x' = axa^{-1}, a) \in_R RSSBG(x, d)$;
3) Return $pk = (x' = axa^{-1}, x)$ and $sk = a$.

Blind Signing. There are four steps as follows:

1) signer chooses $(\alpha = bxb^{-1}, b) \in RSSBG(x, d)$ and sends α as a commitment to the user.
2) Blinding: User chooses $\delta \in_R B_n(l)$ and computes $\alpha' = \delta\alpha\delta^{-1}$ and $h = H(m\|H_1(\alpha'))$ and then sends h to the signer.
3) signer computes $\beta = bhb^{-1}, \gamma = ba^{-1}hab^{-1}$ and sends (β, γ) to user.
4) Unblinding: User computes $\beta' = \delta\beta\delta^{-1}, \gamma' = \delta\gamma\delta^{-1}$ and display $(\alpha', \beta', \gamma')$ as a blind signature on message m.

Verification. Verifier computes $h = H(m\|H_1(\alpha'))$ and accepts the signature if and only if $\alpha' \approx x, \beta' \approx h, \gamma' \approx h, \alpha'\beta' \approx xh$, and $\alpha'\gamma' \approx x'h$.

3.2 Analysis of Scheme

In this section, we analyze the security of the above scheme in the random oracle model under chosen message attack.

Definition 5. *Let $S = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ be a signature scheme and let $BS = (\mathcal{BK}, \mathcal{BS}, \mathcal{BV})$ be the corresponding blind signature scheme. An adversary $\mathcal{A}$ learns the public key* pk *randomly generated by $\mathcal{BK}$. $\mathcal{A}$ is allowed to play the role of a user in the runs of the blind signing protocol, After interaction with the signer $\mathcal{A}$ outputs some number of message signature pairs. The advantage of the adversary $Adv^{blind}_{B_n}(\mathcal{A})$ is defined as the probability of $\mathcal{A}$ to output a set L of valid message signature pairs, such that the number of invoked blind signing protocols with the signer is strictly less than the size of L.*

We say that the blind signature scheme BS is secure against *one more forgery* under chosen message attack or just secure blind signature scheme if there does not exist a polynomial time adversary(PPT) $\mathcal{A}$ with non-negligible advantage $Adv^{blind}_{B_n}(\mathcal{A})$.

Theorem 1. *If MTSP is infeasible in braid group B_n then the blind signature scheme in Section 3.1 is unforgeable under one more forgery as defined in Section 2.1.*

Proof. Let in braid group B_n, Conjugality Decision Problem (CDP) is easy and conjugality Search Problem (CSP) is hard. Let $\mathcal{A}$ be any polynomial time adversary attacking the blind signature scheme over braid group against one more forgery under chosen message attack. Now we will use $\mathcal{A}$ to construct another Probabilistic Polynomial Time (PPT) adversary $\mathcal{B}$ that will solve the MTSP with advantage $Adv_{B_n}^{MTSP}(\mathcal{B}) = \frac{Adv_{B_n}^{blind}(\mathcal{A})}{q_h}$.

Suppose the adversary $\mathcal{B}$ is given $(x, axa^{-1} = x') \in B_n \times B_n$ and $y \in B_n$ as challenge and $\mathcal{B}$ has to simulate the random hash oracle $H : \{0,1\}^* \rightarrow B_n$ and blind signing oracle BS for adversary $\mathcal{A}$. Suppose the number of hash oracle queries by $\mathcal{A}$ be q_h and q_s the number of queries to blind signing oracle. Each time $\mathcal{A}$ makes a new hash oracle query $m_i \mid\mid H_1(\alpha_i')$ for $1 \leq i \leq q_h$, that is distinct from the previous hash oracle query. If $\mathcal{A}$ makes a hash oracle query that it already made before, $\mathcal{B}$ searches in H_{list} and replies with old one. Otherwise it replies in the following way.

If $i = i_0$ (for some $1 \leq i_0 \leq q_h$), then $\mathcal{B}$ returns $H(m_i \mid\mid H_1(\alpha_i')) = y$. Otherwise $\mathcal{B}$ chooses a random braid $k_i \in_R B_n$ and returns $H(m_i \mid\mid H_1(\alpha_i')) = k_i$ and adds the answer to its H_{list}.

When $\mathcal{A}$ makes a blind signing oracle queries on h, then $\mathcal{B}$ resends it to blind signing oracle $\mathcal{BS}$ and forwards the answers to $\mathcal{A}$. Eventually $\mathcal{A}$ halts and output a list of message signature pairs $(m_1, \sigma_1), (m_2, \sigma_2), \cdots, (m_{q_s+1}, \sigma_{q_s+1})$ where each $\sigma_i = (\alpha_i', \beta_i', \gamma_i')$ for $1 \leq i \leq q_s + 1$. Now $\mathcal{A}$ selects a message signature pair $(m, (\alpha', \beta', \gamma'))$ and outputs it as forgery on message m.

If $m = m_{i_0}$, then $\alpha' \approx x, \beta' \approx y, \gamma' \approx y, \alpha'\beta' \approx xy$, and $\alpha'\gamma' \approx x'y$ where $H(m \| H_1(\alpha')) = y$.

Therefore $(\alpha', \beta', \gamma')$ is a solution of MTSP of instance $(x, axa^{-1} = x') \in B_n \times B_n$ and $y \in B_n$ and $Adv_{B_n}^{MTSP}(\mathcal{B}) = \frac{Adv_{B_n}^{blind}(\mathcal{A})}{q_h}$. Hence the theorem follows.

Otherwise, $\mathcal{B}$ reports failure and halt. □

4 Conclusion

In this paper, we have analyzed a blind signature scheme over braid groups given in [9]. Our security analysis is defined for a new hard problem considered in [6], which is approximately the same complexity as CSP.

Acknowledgement

The author would like to thanks the review committee of the journal and all the persons whose references have been made this work possible.

References

[1] E. Artin, "Theory of Braids," *Annals of Math*, vol. 48, pp. 101-126, 1947.

[2] J. S. Birman, "Braids, links, and mapping class groups," *Annals of Math Study*, vol. 82, Princeton University Press, 1974.

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

[4] F. P. Chiang, Y. M. Lin, and Y. F. Chang, "Comments on the security flaw of Hwang et al.' blind signature scheme," *International Journal of Network Security*, vol. 6, no. 2, pp. 185-189, 2008.

[5] 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," *Proceedings of Crypto'00*, LNCS 1880, pp. 166-183, 2000.

[6] K. H. Ko, D. H. Choi, M. S. Cho and J. W. Han, "New signature scheme using Conjugality problem," *Cryptology eprint Archieve Report*, 2002. (http://eprint.iacr.org/2002/168)

[7] M. Kumar, "Linkability of blind signature schemes over braid groups," *Cryptology eprint Archieve Report*, 2009. (http://eprint.iacr.org/2009/192)

[8] D. Pointcheval and J. Stern, "Probably secure blind signature schemes," *Proceedings of Asiacrypt'96*, LNCS 1163, pp. 252-265, 1996.

[9] G. K. Verma, "Blind signature schemes over braid groups," *Cryptology eprint Archieve Report*, 2008. (http://www.eprint.iacr.org/2008/027)

[10] G. K. verma, "A proxy signature scheme over braid groups," *Cryptology eprint Archive Report*, 2008. (http://www.eprint.iacr.org/2008/160)

[11] G. K. verma, "A proxy blind signature scheme over braid groups," *International Journal of Network Security*, vol 9, no. 3, pp. 214-217, 2009.

[12] Z. M. Zhao, "ID-based weak blind signature from bilinear pairings," *International Journal of Network Security*, vol. 7, no. 2, pp. 265-268, 2008.

Girraj Kumar Verma received his Int. M.Sc. in Mathematics and Computer Science from Institute of Basic Science, Dr. B. R. Ambedkar University, Agra, India in 2003. He has been working as a lecturer at Hindustan College of Science and technology, Mathura, India. He has published four technical papers in the area of Cryptography and Network security.