A Proxy Blind Signature Scheme over Braid Groups

Girraj Kumar Verma
Department of Mathematics, Hindustan College of Science and Technology
Farah, Mathura, Uttar Pradesh, India (Email: girrajv@gmail.com)
(Received May 11, 2008; revised and accepted Oct. 2, 2008)

Abstract

A proxy signature scheme, introduced by Mambo, Usuda and Okamoto, allows a designated person to sign on behalf of an original signer. Blind signatures, introduced by D. Chaum allow a user to get a signature from a signer without revealing any information about message or its signature. A proxy blind signatures, first time introduced by Tan et al in 2002, combines all the security properties of both proxy signatures and of blind signatures. In this paper we have proposed a proxy blind signature scheme using conjugacy search problem over braid groups. Our proxy blind signature scheme is partial protected proxy signature.

Keywords: Blind signature, braid groups, conjugacy problem, proxy signature, proxy blind signature

1 Introduction

Proxy signatures, Introduced by Mambo, Usuda and Okamoto [17], allow a designated person called proxy signer, to sign on behalf of an original signer. According to the delegation type, the proxy signatures are classifieds as full delegation, partial delegation and delegation by warrant [5, 15, 17]. The proxy signature plays an important role in many applications [12, 13, 14] and has been received great attention since it was proposed. Later many specific types i.e. multy proxy, threshold proxy, proxy blind signatures have been proposed. Proxy blind signature was proposed by Tan et al [19] in 2002. These signatures ensure the security properties of both the proxy signatures and blind signatures [18]. Many proxy blind signature schemes have been given since inception using number theoretic setting. But, no proxy blind signature has been proposed using a non commutative group like braid group.

The braid groups were first introduced to construct a key agreement protocol and a public key encryption scheme [15] in CRYPTO-2000 by Ko et al and in 2002 a digital signature scheme [16] was introduced by Ko et al. Later some other signature schemes [20, 21] were proposed using conjugacy problem over braid groups. But, no proxy blind signature scheme has been proposed using braid groups as a setting.

In this paper, we are introducing a proxy blind signature scheme over braid groups. In braid groups, the decision version of conjugacy problem is easy and searching of conjugator is hard. This gap between two versions has been used for constructing this protocol.

The rest of the paper is organized as follows: In Section 2, we have defined security properties of proxy blind signature scheme and some problems over braid groups. In Section 3 we have discussed the scheme by Ko et al and have introduced our proxy blind signature scheme. In Section 4 we have analyzed our proposed scheme and Section 5 we have concluded our discussion.

2 Preliminaries

2.1 Security Properties of Proxy Blind Signature

Our scheme is a cryptographic primitive involving four entities an original signer, a proxy signer, a user and a verifier. In this subsection we describe the required security properties of a proxy blind signature [13, 14, 17, 19].

1) Unforgeability: Only a designated signer can create a valid proxy blind signature for the original signer (even the original signer cannot do it).

2) Verifiability: After verification, the verifier can be convinced of the original signer's agreement on the signed message.

3) Secrete Key Dependencies: Proxy key or delegation pair can be computed only by the original signer's secret key.

4) Distinguishability: Verifier can distinguish the original signature and proxy signature efficiently.

5) Identifiability: Verifier can identify both the proxy and the original signers.

6) Undeniability: Due to fact that the delegation information is signed by the original signer and the proxy

signatures are generated by the proxy signer's secret key both the signers cannot deny their behavior.

7) Non Repudiation: The proxy signer cannot claim that the proxy signature in dispute is illegally signed by the original signer.

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

2.2 Braid Groups and Congugacy Problem

In this section, we give a brief description of the braid groups and discuss some hard problem related to conjugacy search problem. For more information on braid groups, word problem and conjugacy problem please refer to [2, 3].

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

$$\begin{cases} \sigma_i\sigma_j = \sigma_j\sigma_i, & where \mid i-j \mid \geq 2 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, & Otherwise. \end{cases}$$

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

Some Hard Problems: 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 $\sigma_1, \sigma_2, \cdots, \sigma_{m-1}$.

Conjugacy 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.

Conjugacy 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 $y = bxb^{-1}$.

Since braid group B_n is an infinite group, so it is impractical to use B_n for cryptographic purposes. As in [16] for a positive integer l, we take $B_n(l)$ as the set of all braids from B_n having canonical length almost 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 [16] 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 [9, 10, 12, 15, 16, 20, 21].

3 Proposed Scheme

3.1 Signature Scheme by Ko et al. [16]

In this section we are giving digital signature scheme by Ko et al. The parameters n, l, d are fixed as in [16] and the concatenation of two strings in $\{0,1\}^*$ is represented by $||$. Let $m \in \{0,1\}^*$ be the message to be signed and $H : \{0,1\}^* \rightarrow B_n(l)$ be a one way hash function.

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 $sk = a$.

Signing: The signer does the following steps:

1) Signer chooses $(\alpha = b^{-1}xb, b) \in_R RSSBG(x, d)$;

2) Computes $h = H(m \mid\mid \alpha)$ for a message m and $\beta = b^{-1}hb$ and $\gamma = b^{-1}aha^{-1}b$;

3) Return a signature $\sigma = (\alpha, \beta, \gamma) \in B_n(l) \times B_n(l + 2d) \times B_n(l + 4d)$.

Verification:

1) Verifier computes $h = H(m \mid\mid \alpha)$.

2) Return accept 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 Proposed Proxy Blind Signature Scheme

Let the message to be signed be $m \in \{0,1\}^*$ and let $H : \{0,1\}^* \rightarrow B_n(l)$ and $H_1 : B_n(l) \rightarrow \{0,1\}^*$ be one way hash functions and other parameters are same as in Section 3.1. The key generation is also same as in Section 3.1.

1) Proxy Generation: Original signer chooses $\alpha_0 \in_R B_n(l)$ and computes $t_0 = a_0\alpha_0 a_0^{-1}$ and sends (α_0, t_0) to proxy signer in a secure way.

2) Proxy Verification: Proxy signer checks $t_0 x_0' \approx \alpha_0 x_0$.

3) Proxy Blind Signing by Proxy Signer:

- Proxy signer chooses $b \in_R B_n(l)$ and computes $\alpha = bx_p b^{-1}$ and sends (t_0, α) to user.
- Blinding: User chooses $\delta \in_R B_n(l)$ and computes $t_0' = \delta t_0 \delta^{-1}, \alpha' = \delta\alpha\delta^{-1}$ and $h = H(H_1(t_0'x_0') \mid\mid m)$ and sends h to the proxy signer.
- Proxy signer computes $\beta = bhb^{-1}, \gamma = ba_p^{-1}ha_pb^{-1}$ and sends (β, γ) to user.
- Unblinding: User computes $\beta' = \delta\beta\delta^{-1}, \gamma' = \delta\gamma\delta^{-1}$ and display $(\alpha', \beta', \gamma', t_0')$ as a proxy blind signature on message m.

4) Verification: Verifier computes $h = H(H_1(t_0'x_0') \parallel m)$ and accepts the signature if and only if $\alpha' \approx x_p, \beta' \approx h, \gamma' \approx h, \alpha'\beta' \approx x_p h$, and $\alpha'\gamma' \approx x_p' h$.

Proof of Verification: Verification works because

$$\begin{aligned}
\alpha' &= \delta b x_p b^{-1}\delta^{-1} = (\delta b) x_p (\delta b)^{-1} \\
\beta' &= \delta b h b^{-1}\delta^{-1} = (\delta b) h (\delta b)^{-1} \\
\gamma' &= \delta\gamma\delta^{-1} = (a_p b^{-1}\delta^{-1})^{-1} h (a_p b^{-1}\delta^{-1}) \\
\alpha'\beta' &= (\delta b x_p b^{-1}\delta^{-1})(\delta b h b^{-1}\delta^{-1}) \\
&= \delta b x_p h b^{-1}\delta^{-1} \\
&= (\delta b) x_p h (\delta b)^{-1} \\
\alpha'\gamma' &= (\delta b x_p b^{-1}\delta^{-1})(\delta (b a_p^{-1} h a_p b^{-1})\delta^{-1}) \\
&= (\delta b x_p a_p^{-1} h a_p b^{-1}\delta^{-1}) \\
&= \delta b (a_p^{-1} a_p) x_p a_p^{-1} h a_p b^{-1}\delta^{-1} \\
&= (a_p b^{-1}\delta^{-1})^{-1} (a_p x_p a_p^{-1}) h (a_p b^{-1}\delta^{-1}) \\
&= (a_p b^{-1}\delta^{-1})^{-1} x_p' h (a_p b^{-1}\delta^{-1}).
\end{aligned}$$

4 Analysis of Proposed Scheme

In this section, we are analyzing the security parameters satisfied by our proposed scheme.

4.1 Unforgeability

Let an adversary(may be an user or an original signer) wants to impersonate the proposed proxy blind signature scheme. For creating a valid proxy blind signature, adversary needs to compute $h = H(H_1(t_0'x_0') \parallel m)$ and $\alpha = b x_p b^{-1}$, $\beta = b h b^{-1}$, $\gamma = b a_p^{-1} h a_p b^{-1}$. He can intercept the delegation pair $(\alpha_0, a_0\alpha_0 a_0^{-1})$, but he cannot obtain the proxy signer's secret key a_p. As $a_p \in_R B_n(l)$, the adversary can obtain the proxy signer's secret key a_p by guessing it with almost probability $1/(n!)^l$. That is the adversary can impersonate the proxy blind signature successfully with a probability $1/(n!)^l$.

Now, let proxy signer wants to impersonate the signature for illegal use. As he gets $(\alpha_0, a_0\alpha_0 a_0^{-1})$ from original signer and it is conjugacy search problem to extract a_0 from this pair. So, the proxy signer can succeed to solve conjugacy search problem with almost a probability $1/(n!)^l$. That is the proxy signer can impersonate the proxy blind signature successfully with a probability $1/(n!)^l$.

4.2 Scret Keys Dependencies

Since for creating a valid proxy blind signature, the user computes $h = H(H_1(t_0'x_0')\|m)$, where it is impossible to compute $t_0 = a_0\alpha_0 a_0^{-1}$ without the secret key of the original signer. Hence the signing by proxy signer depends on the secret key of the original signer.

4.3 Verifiability

Since in braid groups conjugacy decision problem is easy, so any one can verify the validity of the signature by using the public keys of original as well as of proxy signer. The correctness of verification has been proved.

4.4 Distinguishability

Since the verification of normal signature scheme is valid iff $\alpha \approx x$, $\beta \approx h$, $\gamma \approx h$, $\alpha\beta \approx xh$, and $\alpha\gamma \approx x'h$ holds where $h = H(m \parallel \alpha)$. The verification of proxy blind signature scheme is valid iff $\alpha' \approx x_p$, $\beta' \approx h$, $\gamma' \approx h$, $\alpha'\beta' \approx x_p h$, and $\alpha'\gamma' \approx x_p' h$ holds where $h = H(H_1(t_0'x_0') \parallel m)$. From the verification of two schemes, the verifier can distinguish the normal signature and the proxy blind signatures efficiently.

4.5 Identifiability

Since for verification purpose, $h = H(H_1(t_0'x_0') \parallel m)$ is computed from original signer's public key and the verification is valid iff $\alpha' \approx x_p, \beta' \approx h, \gamma' \approx h, \alpha'\beta' \approx x_p h$, and $\alpha'\gamma' \approx x_p' h$ holds. So, the verifier can easily identify both the original signer as well as the proxy signer efficiently.

4.6 Undeniability

Since the proxy blind signatures are computed by using $(\alpha_0, t_0 = a_0\alpha_0 a_0^{-1})$, as a proxy by original signer, and $\alpha = b x_p b^{-1}, \beta = b h b^{-1}, \gamma = b a_p^{-1} h a_p b^{-1}$ by proxy signer. So, both of the signers cannot deny for their behavior.

4.7 Non Repudiation

Since for construction of proxy blind signature, the proxy signer obtains the delegation pair $(\alpha_0, t_0 = a_0\alpha_0 a_0^{-1})$, from original signer and to obtain a_0, the original signer's secret key, from this pair is conjugacy search problem. Now, since the original signer does not obtain a_p, the proxy signer's secret key. Thus neither the original signer nor the proxy signer can claim the proxy signature in dispute is illegally signed by the other.

4.8 Unlinkability

In signing phase, the user selects $\delta \in_R B_n(l)$ randomly for blinding function exercise. So, the signer receives only medial values and the signature $(\alpha', \beta', \gamma', t_0')$ at last. For verification purpose the relation $\alpha' \approx x_p, \beta' \approx h, \gamma' \approx h, \alpha'\beta' \approx x_p h$, and $\alpha'\gamma' \approx x_p' h$ must hold. Since the decision version of conjugacy problem is easy, so verification is done efficiently. If the signer tries to link his view, he has to find the blinding factor δ from available information i.e. he has to solve conjugacy search problem taking any one of the pair from $(\alpha, \alpha'), (\beta, \beta'), (\gamma, \gamma')$ and (t_0, t_0') as a instance. Since in braid groups, we are considering conjugacy search problem computationally hard, so our proposed proxy blind signature scheme achieves perfect

unlinkability between the proxy signer's view of the protocol and the message signature pair.

5 Conclusion

In this paper, we have proposed the proxy blind signature scheme over braid groups. We have also discussed the security parameters satisfied by our scheme. Although, we have not discussed the efficiency of our scheme non the less our scheme proposed a new setting for constructing protocols for delegating signing rights.

Acknowledgement

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

References

[1] I. Anshel, M. Anshel, and D. Goldfeld, "An algebraic method for public key cryptography," *Mathematical Research Letters*, vol. 6, pp. 287-291, 1999.

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

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

[4] A. Boldyreva, "Efficient threshold signature, multi Signature and blind signature schemes based on the Gap-Diffey Hellman groups," *Cryptology eprint archive Report.* http://eprint.iacr.org/2002/118.pdf

[5] A. Boldyreva, A. Palacio, and B. Warinschi, "Secure proxy signature schemes for delegation of signing rights," *Cryptology eprint archive Report.* http://eprint.iacr.org/2003/096.

[6] J. C. Cha, K. H. Ko, S. J. Lee, J. W. Van, and J. S. Cheon, "An efficient implementation of braid groups," *Asiacryp' 01*, LNCS 2248, pp. 144-156, Springer-Verlag, 2001.

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

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

[9] W. Diffey, and M. E. Hellman, "New directions in cryptography," *IEEE transaction on Information Theory*, vol. 22, no. 6, pp. 74-84, June 1977.

[10] D. Hofheinz, and R. Steinwandt, "A practical attack on some Braid group based cryptographic primitives," *Proceedings of Public key Cryptography*, LNCS 2567, pp. 187-198, Springer-Verlag 2002.

[11] S. Kim, S. Park, and D. Won, "Proxy signatures: Revisited, in Y. Han, T. Okamoto, S. Quing, editors," *Proceedings of International Conference on Information and Communications Security(ICICS' 93)*, LNCS 1334, pp. 223-232, Springer-Verlag, 1993.

[12] H. kim, J. Baek, B Lee, and K. Kim, "Computing with secret for mobile agent using one time proxy signature," *Proceedings of SCIS' 01*, pp. 845-850, 2001.

[13] H. Kim, B. Lee, and K. Kim, "Strong proxy signature and its application," *Proceedings of SCIS' 01*, pp. 603- 608, 2001.

[14] H. Kim, B. Lee, and K. Kim, "Secure mobole agent using strong non designated proxy signature," *Proceedings of ACISP' 01*, LNCS 2119, pp. 474-486, Springer- Veralg, 2001.

[15] 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, Springer-Verlag 2000.

[16] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Han, "New signature scheme using conjugacy problem," *Cryptology eprint archieve report*, 2002. http://eprint.iacr.org/2002/168

[17] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures for deligating signing operation," *Proceedings of the 3rd ACM conference on Computer and Communication Security (CCS)*, pp. 48-57, 1996.

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

[19] Z. Tan, Z. Liu, and C. Tang, "Digital proxy blind signature schemes based on dlp and ecdlp," *MM Research Preprint MMRC*, no. 21, pp. 212-217, AMSS, Academica Sinica, Beijing, 2002.

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

[21] G. K. Verma, "A Proxy signature scheme over braid groups," *Cryptology eprint archieve report*, 2008. http://www.eprint.iacr.org/2008/160

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, Farah, Mathura, India. His research interest includes Cryptography and Network security. He has published 3 technical papers.