Security Analysis of a Proxy Signature Scheme 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

Delegation of powers is a common practice in the real world. To realized the delegation of powers electronically,Mambo,Usuda and Okamoto proposed the first proxy signature scheme in 1996. Since then a number of new schemes and their improvements have been proposed. In 2008, Verma proposed a proxy signature scheme over braid groups. This paper analyzes Verma's scheme and found that this scheme suffers with the serious security flaws. In this scheme,the proxy signer is able to misuse his delegated signing capabilities and the original signer can not restrict the proxy signer for misuse her delegation power. As a result, the proposed scheme does not satisfy some essential security requirements. Verma's proposed scheme is also not secure against the original signer and proxy singer changing attacks. Thus, the proposed scheme is not only insecure against the attacks by original signer and proxy signer but also has pitfalls against the forgery attacks mounted by any antagonist.

1. Introduction

In 1996, Mambo Usuda and Okamoto [19] introduced the concept of proxy signature scheme. The proxy signature scheme allowed an entity called original signer to delegate its signing capabilities to another entity called proxy signer and the proxy signer signs message on behalf of the original signer. Once the signature verifier receives the proxy signature, it can check the validity of the signature and identify the proxy signer, and also the originals agreement on the signed message. Based on delegation type, Mambo et al. [19] classified proxy signatures as full delegation, partial delegation and delegation by warrant. In the full delegation, the original signer gives his secret key to the proxy signer. In the partial delegation, the original signer generates a proxy signature key by using his secret key and gives it to the proxy signer who uses the proxy key to sign the message on behalf of original signer. In the delegation by warrant, the proxy signer first obtains the warrant, which is a certificate composed of a message part and a public signature key from the original signer, and then uses the corresponding secret key to sign. The resulting signature consists of the created signature and the warrant. A number of schemes [1, 2, 17, 18, 19] and their improvements [3, 11, 21, 22, 23, 24, 25, 26] have been proposed since the introduction of the concept of proxy signatures. However, most of them do not meet the below listed security requirements. A Proxy signature scheme should satisfy the following basic security requirements

1.1 Security Requirements

The security requirements for a secure proxy signature schemes are specified in [2]. which are explained below.

- **SR**$_1$. VERIFIABILITY: From the proxy signature, any verifier can be convinced of the original signer's agreement on the signed message.
- **SR**$_2$.STRONG UNFORGEABILITY:PROXY PROTECTION: A valid proxy signature can only be generated by proxy signer. This means that valid proxy signature cannot be created by the original signer or any third party who is not designated as proxy signer. In other words, we can say that only

the delegated proxy signer can generate valid partial proxy signature. Even the original signer cannot masquerade as a proxy signer.

- **SR**$_3$.STRONG IDENTIFIABILITY: Anyone can determine the identity of the corresponding proxy signer form a proxy signature.

- **SR**$_4$.STRONG UNDENIABILITY (NONREPUDIATION): Any valid proxy signature must be generated by proxy signer. Therefore, proxy signer can not deny that he/she has signed the message. In addition, the original signer cannot deny having delegated the power of signing messages to the proxy signer.

- **SR**$_5$.DISTINGUISHABILITY: The verifier can distinguish the original and proxy signature efficiently.

- **SR**$_6$.SECRET KEY DEPENDENCIES: Proxy signature key or the delegation information can be computed only with the help of original signer's secret key.

- **SR**$_6$.TIME CONSTRAINT: The proxy signing key can be used only during the delegated period. Once the proxy key expire, the proxy signature generated by using this key become invalid.

- **SR**$_7$.PREVENTION OF MISUSE : The proxy signer is restricted to transfer the proxy key to someone else. The proxy signer also can not use proxy key for purposes other than generating a valid proxy signature. In case of misuse, the responsibility of the proxy signer should be determined from the warrant.

In 2000, Ko et. al. proposed a key agreement protocol and a public key encryption scheme based upon braid groups [16]. The schemes based upon braid groups [6, 7, 8, 9] 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 introduced a proxy signature scheme over braid groups [10].This paper analyzes Verma's scheme and found that this scheme suffers with the security flaws. This paper is organized as follows Section 2 provides a brief idea of braid group and explain the difficulty of the computational version. In section 3, we review Verma's proxy signature scheme over braid group. The securities flaws of Verma's scheme are discussed in section 4. Finally, we conclude the work in section 5.

2 Braid Group and Conjugacy problem

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 [4, 6, 7, 8, 9, 12, 13, 14, 15, 16]. 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 [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.

3 Review of Verma's Scheme

This section reviews a proxy signature scheme over braid group [10]. In this scheme, to sign a message $m \in [0, 1]^*$, the original signer Alice delegates his signing capability to a proxy signer Bob.

3.1 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 $sk = a$.

3.2 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 $t_o = a_o x a_o^{-1}$. 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.

3.3 Proxy Signature Generation

When the proxy signer Bob signs a document on behalf of original signer Alice, he computes the following steps.

- Bob computes $h = H(H_1(t_o x_o^{'})\|m)$.
- Bob selects $b \in_R B_n$ and computes $\alpha = bxpb^{-1}, \beta = bhb^{-1}, \gamma = ba_p^{-1}ha_pb^{-1}$.
- Bob displays $(\alpha, \beta, \gamma, t_o)$ as a proxy signature on the message *m*

3.4 Proxy Signature verification

To verify the proxy signature, a verifier computes the following steps.

- Verifier computes $h = H(H_1(t_o x_o^{'})\|m)$.
- 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.

4 Security Analysis of Verma's Scheme

This section analyzes the security of a proxy signature scheme over braid group. According to Verma, the proposed scheme satisfies all the security requirements strongly. Moreover, Verma claimed that there is no effect of the revelation of the delegation pair on the security of the proposed scheme. we feel that these claims are not true. In Verma's scheme,the original signer sends the signing key in the form of a pair $(\alpha_o, t_o)$to Bob through a secure channel. The proxy singer verify the validity of this pair by checking the congruence $t_o x_o^{'} \sim \alpha_o x_o$. If it is hold, he displays $(\alpha, \beta, \gamma, t_o)$ as a proxy signature on the message *m*. In the proxy key generation, the value t_o is kept secret, while the same value is displayed in the proxy signature $(\alpha, \beta, \gamma, t_o)$.This is a contradiction in Verma's scheme. On the basis of this contradiction, we successfully identifying several interesting forgery attacks on Verma's scheme. The following section presents a security analysis of the Verma's proposed proxy signature scheme over braid group in detail.

4.1 Misuse of delegation Power

In this scheme, the delegation pair includes neither the identity information of the proxy signer nor the limit on delegated messages. The proxy signer can further delegate the proxy key to someone else who can also perform the signing operation on behalf of original signer.In this way,a third party has same signing capability as a designated proxy signer. Furthermore,the delegation pair does not contain any information about the duration period of delegated power. It means the proxy signer has been selected permanently. Once a proxy signer selected,then he will remain the proxy signer forever. The original signer's delegation power does not contain any information about the qualification of the messages on which the proxy signer can sign. The proxy signer can select any message of his choice and then sign it. In these ways,the proxy signer is able to misuse his delegated signing capabilities and the original signer can not restrict the proxy signer for misuse her delegation power. Consequently, in Verma's scheme, the security requirements $SR_1, SR_2, SR_5, SR_6, SR_7$ are not satisfied.

4.2 Original signer changing attack

In Verma's proposed scheme there is a need of secure channel to deliver the delegation information. Verma claimed that his scheme is still secure even if an attacker intercept the delegation pair. We observe that his claim is not true. The following steps prove that how an antagonist can mount an original signer attack on Verma' s scheme by the interception of the delegation pair.

4.2.1 Generation of Fabricated Proxy Key

- The antagonist intercept the delegation pair(α_o, t_o).
- The antagonist selects a braid $\alpha_c \in_R B_n$ and computes $t_c = a_c x a_c^{-1}$. Then, she replaces the pair$(\alpha_o, t_o)$with (α_c, t_c) and sends this pair to the proxy singer Bob.
- Bob checks whether $t_c x_c^{'} \sim \alpha_c x_c$. If it is hold, he accept the key, otherwise reject it. Obviously, This conjugacy relation will hold truly. It can be seen easily that the delegation pairs (α_o, t_o) and (α_c, t_c) are statistically indistinguishable. Since,there is also no information about the original signer in the delegation pair(α_o, t_o) strictly, therefore the Bob can not determine the identity of the original signer explicitly.

Now in place of delegation pair (α_o, t_o),the proxy signer uses the fabricated delegation pair (α_c, t_c). It can be seen easily that this replacement does not effect the proxy signature generation and verification phases.

4.3 Proxy Signer Changing Attack

In Verma's scheme the delegation pair does not include the identity of the proxy signer. In this situation, an interesting attack can be mounted on Verma's proposed scheme. In this attack, an antagonist can become the proxy signer in place of a valid proxy signer Bob. we call this attack proxy signer changing attack. in this attack, any antagonist Charlie can generate a valid proxy signature on a message m_c of her choice. Verma claimed that his scheme is still secure even if an attacker intercept the delegation pair. Again, We prove that his claim is not true.The following steps prove that how an antagonist can mount proxy signer attack on Verma' s scheme by the interception of the delegation pair.

4.3.1 Generation of Fabricated Proxy signature

- The antagonist intercept the delegation pair(α_o, t_o).
- The antagonist Charlie select a message $m_c$of her choice.

- Charlie computes $h_c = H(H_1(t_o x_o^{'})\|m_c)$ and selects $b_c \in_R B_n$ computes $\alpha_c = b_c x_c b_c^{-1}, \beta_c = b_c h b_c^{-1}, \gamma_c = b_c a_p^{-1} h a_p b_c^{-1}$ and displays $(\alpha_c, \beta_c, \gamma_c, t_o)$ as a fabricated proxy signature on the message m_c.

4.3.2 verification of Fabricated Proxy Signature

To verify the Fabricated proxy signature, a verifier computes the following steps.

- Verifier computes $h_c = H(H_1(t_o x_o^{'})\|m_c)$.

- Verifier checks whether $\alpha_c \sim x_c, \beta_c \sim h, \gamma \sim h, \alpha_c\beta_c \sim x_c h, \alpha_c\gamma_c \sim x_c^{'} h$, if it is hold,accept the signature,otherwise reject it.

Obviously, all the conjugacy relations will hold truly. It can be seen easily that the proxy signature $(\alpha, \beta, \gamma, t_o)$ and fabricated proxy signature $(\alpha_c, \beta_c, \gamma_c, t_o)$ are statistically indistinguishable. Since,neither the delegation pair(α_o, t_o) nor the proxy signature provide any information about the proxy signer strictly, therefore the third party can not determine the identity of the proxy signer explicitly. Thus , the verifier accept the fabricated proxy signature as proxy signature.

5 Conclusions

This paper presents the security analysis of a proxy signature scheme over braid groups.The discussion proves that the proposed scheme does not satisfy the necessary security requirements:Verifiability, Strong unforgeability, Proxy Protection, Distinguishability, Time Constraint, Prevention of misuse. Since, the delegation pair does not provide sufficient information about the original and proxy signer, therefore the proposed scheme has serious securities vulnerabilities. The author claimed that the proposed scheme is still secure even if the attacker intercept the delegation pair. This paper proved that this claim is not true and the proposed scheme is also vulnerable to the misuse of delegation pair, original signer attack and proxy signer attack.

References

[1] A. 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. 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.

[5] 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.

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

[7] 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.

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

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

[10] G. K. Verma, A proxy signature scheme over Braid groups, 2008, *available at http://eprint.iacr.org/2008/160*.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.*

[16] 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.

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

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

[19] 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.

[20] 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.

[21] 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.

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

[23] 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.*

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

[25] 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.*

[26] 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.

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.