Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-3, June 2017
Research Paper

www.ijsrnsc.org

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

Braid Group Based Nominative Proxy Signature Scheme

Vandani Verma

Amity Institute of Applied Sciences, Amity University, Noida, INDIA

[*]Corresponding Author: vandaniverma@yahoo.com

Received 15th Mar 2017, Revised 24th Apr 2017, Accepted 18th May 2017, Online 30th Jun 2017

***Abstract*—** Braid groups are highly non-commutative groups, they can be found in our daily life in jewellery, in hair braid and in many more. Nominative proxy signatures is a special type of proxy signatures in which the original signer delegates his signing rights to proxy signer and proxy signer on behalf of the original signer generates the signatures intended for nominee in such a way that only the nominee can verify the signatures and if required he is the only one to prove the validity of the signatures to third party. These signatures are different from designated verifier signatures as the validity of the signatures can be proved to third party when asked. In this paper, we combine the two concepts nominative proxy and braid groups and present the maiden nominative proxy signatures based on braid groups. We also analyse the security aspects of the proposed scheme and showed that the conjugacy decomposition problem, conjugacy search problem and base problem 1 in braids are not solvable for the proposed scheme.

***Keywords*—** nominative proxy signatures, braid group, conjugacy search problem

I. INTRODUCTION

Mambo et al [5] proposed the concept of proxy signatures in 1996, in which the original signer delegates his signing rights to the other entity called the proxy signer and he signs the message on behalf of the original signer. These proxy signatures holds the property of self-authentication i.e. on access anyone can verify the signatures. Sometimes a situation arises where the self authentication property is not suitable; to solve this problem, Kim et al. [6] proposed the concept of nominative signatures (NS) in 1996. Zuo-Wen Tan et al [9] combined the concept of proxy signatures with nominative signatures to form nominative proxy signatures. In a nominative proxy signature scheme, an original signer can delegate his signing power to a proxy signer who generates a nominative signature on behalf of original signer. In a nominative proxy signature scheme, the proxy signer generates the signatures in such a way that only the nominee can verify the signatures and if necessary he only can prove the validity of the signatures to the third party.

Nominative proxy signature (NPS) schemes are classified as:

- Original Nominative Proxy signature if the original signer is the nominator. It satisfies the following properties:

a. Only the original signer can nominate the verifier
b. Non-repudiation
c. Only the nominee/verifier can verify the NPS
d. If necessary, only the nominee can prove the validity of signatures to a third party.

- Proxy nominative proxy signature if the verifier is only nominated by the proxy signer and requirement (b-d) of original NPS.

Moreover, NPS satisfies all the basic properties of proxy signatures like verifiability, strong identifiability, strong unforgeability and proxy protected. Nominative proxy signature schemes are suitable for mobile communication environment in which the receiver is chosen by the mobile user (original signer, as it provides the user anonymity) and he can nominate a proxy agent as the proxy signer to decrease the computational cost through the proxy signature.

Highly non-abelian groups proposed by Artin [1] called Braid groups are being used to generate the cryptographic primitives in recent times i.e. they have emerged as an alternative to public key cryptosystems. They have attracted the cryptographer's as the operations in braid groups are simpler, more efficient and easy to implement on computer's with low computational cost. Wang et al [10] discussed the conjugate adjoining problem and then proposed the signature scheme based on the same. In literature, many proxy signatures based on braid [2, 3, 7] have been proposed and many signatures [4, 8, 11] based on bilinear pairing have also been proposed. Nominative proxy has applications in mobile communication and Braids are easy to implement on computers at low cost. But no efforts were made to combine the two thoughts; this is the first attempt in literature to bring down the concept of nominative proxy signatures to braid group based cryptography so that nominative signatures can be implemented at a low cost. No such braid group based signature scheme exists in literature. The aim of this paper is to introduce a new nominative proxy signature scheme over braid groups. The paper presents the preliminaries of braid groups in section 2, propose the first braid group based nominative proxy signature scheme in section 3, analyze the security aspects in section 4 and finally conclude in section 5.

II. PRELIMINARIES

Braids are found everywhere in this world: in hairdressing, in jewellery, in ropes, in bread and in many more. In mathematics 'n' braid is obtained by laying down a number of parallel strands and interlacing them so that they run in the same direction. Braids always start from top and end at the bottom. A pair of strands can be interlaced if we pass left string either over / under the right string. Braid index is defined as the number of strands in a braid group and the set of all possible n-braids form a group called the n-braid group Bn.

- The identity element of the braid group is formed by allowing the entire strand go parallel (without intertwining)
- The inverse of any braid is the mirror image or its reflection with respect to a horizontal line.
- Two braids are said to be equivalent if one braid can be distorted to the other braid by sliding the crossings and canceling inverses without adding or removing any other crossings.

Group Bn of n-braid (n≥2) is generated by σ_1, σ_2… σ_{n-1} which satisfies the conditions

(i) $\sigma_i\sigma_j = \sigma_j\sigma_i, where\left|i-j\right| \geq 2$
(ii) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$

Here σ_i is a braid formed by crossing strings ith and (i+1)th braids.

Braids are very simple to store on computers due to their unique representation and decomposition. The security of number theoretic cryptosystem is based on the problems like factorization problem, discrete log problem and many more. Similarly, the security of braid group based cryptosystems depends on the following difficult problems:

- Conjugacy Decision Problem:
  For the given pair $(x, y) \in B_n \times B_n$ the problem is to find whether x and y are conjugate of each other.
- Conjugacy Search Problem:
  Given a pair $(x, y) \in B_n \times B_n$, the problem is to find $a \in B_n$ such that $y = axa^{-1}$
- Conjugacy Decomposition Problem: *Given a* pair $(x, y) \in B_n \times B_n$ s.t. $y = axa^{-1}$ for $a \in B_n$, the problem is to find $b_1, b_2 \in B_n$ such that $y = b_1\, x\, b_2$
- Base Problem 1:
  Given the triple x_c, α, x'_c € B_{l+r} where $\alpha = bx_cb^{-1}$ and $x'_c = a_cx_ca_c^{-1}$ for hidden $a_c \in RB_n$ and $b \in LB_l$, where RB_n and LB_l are right braid and left braid formed from *'n'* and *'l'* braids from *(l+r)*, find
  $a_c\alpha a_c^{-1} (=a_cb\, x_c\, a_c^{-1} b^{-1})$

III. PROPOSED SCHEME

In this section we present the first nominative proxy signatures based on the concept of braid groups as follows: let B_{l+r} is divided into two subgroups for a pair of integers *(l, r)* such that $LB_l = \{\sigma_1, \sigma_2 \ldots \sigma_{l-1}\}$and $RB_r = \{\sigma_{l+1}, \ldots \sigma_{l+r-1}\}$ and for some $a \in LB_l$ and some $b \in RB_r$, $ab = ba$. Consider H_1: $\{0, 1\}^* \rightarrow B_{l+r}$ and H_2: $B_{l+r} \rightarrow \{0, 1\}^*$ as one way hash functions.

A. *Secret and public key generation:* User '*u*' chooses a braids $x_u \in_R B_{l+r}$ such that $x_u \in_R LB_l$ and computes $x'_u = a_ux_ua_u^{-1}$ where a_u is the secret key and (x'_u, x_u) is the public key.

B. *Original signer's*: Alice (Original signer) chooses a random braid $\alpha_A \in RB_l$ to compute
$z_1 = a_A\alpha_Ax_A\alpha_A^{-1}a_A^{-1}$, $h = H_1[H_2(z_1)||m_w]$
$z_2 = \alpha_Ah\alpha_A^{-1}$.
Sends $\sigma_1 = (m_w, z_1, z_2)$ as the delegation signatures to Bob (proxy signer).

C. *Verification of delegation by the proxy signer*:
Bob on receiving $\sigma_1 = (m_w, z_1, z_2)$ computes $h = H_1[H_2(z_1)||m_w]$ and accepts the delegation by Alice if conjugacy of $z_2z_1 \sim hx'_A$ holds.

D. *Proxy signature generation*: To generate the proxy signatures for the nominee Cindy Bob computes the proxy key as $Sp = a_B\alpha_B$ where $\alpha_B \in_R RB_l$ and then computes the nominative proxy signatures as follows:
$t_1 = bx_cb^{-1}$, $t_2 = bx'_cb^{-1}$, $H = H_1[H_2(t_2)||m_w]$,
$t_3 = t_1x_Bt_1^{-1}$, $t_4 = z_2bS_pt_1^{-1}H\,t_1S_p^{-1}b^{-1}z_2^{-1}$,
$t_5 = z_2b\,x'_cb^{-1}z_2^{-1}$, $t_6 = S_pt_1^{-1}H\,t_1S_p^{-1}$, $t_7 = t_1z_1t_1^{-1}$
$\sigma_2 = (m_w, t_1, t_3, t_4, t_5, t_6, t_7)$ is considered as the nominative proxy signatures on message 'm'.

E. *Nominative proxy signature verification*: On receiving σ_2 nominee Cindy computes $t_2 = a_ct_1a_c^{-1}$ and checks the conjugacy of $t_2 \sim x'_c$. If it holds she then computes $H = H_1[H_2(t_2)||m_w]$ and check the conjugacy of $t_3 \sim x_B$, $t_4t_5 \sim t_6t_2$ and $t_3t_7 \sim x_Bx'_A$

IV. Security Analysis

The security of the proposed scheme depends on conjugacy decomposition problem, as finding b from $t_2 \sim x'_c$ is a conjugacy decomposition problem. Also, finding b from $t_1 = bx_c b^{-1}$ is a base problem 1.

A. *Correctness*:

i. $t_3 = t_1 x_B t_1^{-1} \Rightarrow t_3 \sim x_B$

ii. $t_4 t_5 \sim t_6 t_2$

$$\begin{aligned} & t_4 t_5 \\ & = z_2 b S_p t_1^{-1} H\, t_1 S_p^{-1} b^{-1} z_2^{-1} z_2 b\, x'_c b^{-1} z_2^{-1} \\ & = z_2 b (S_p t_1^{-1} H\, t_1 S_p^{-1}) b^{-1} b\, x'_c b^{-1} z_2^{-1} \\ & = z_2 b (S_p t_1^{-1} H\, t_1 S_p^{-1})(b\, x'_c b^{-1}) b^{-1} z_2^{-1} \\ & = z_2 b (t_6 t_2) b^{-1} z_2^{-1} \\ & \Rightarrow t_4 t_5 \sim t_6 t_2 \end{aligned}$$

iii. $t_3 t_7 \sim x_B x'_A$

$$\begin{aligned} & t_3 t_7 \\ & = t_1 x_B t_1^{-1} t_1 z_1 t_1^{-1} \\ & = t_1 x_B z_1 t_1^{-1} \\ & = t_1 x_B (a_A \alpha_A x_A \alpha_A^{-1} a_A^{-1}) t_1^{-1} \\ & = t_1 x_B (a_A \alpha_A) x_A (\alpha_A^{-1} a_A^{-1}) t_1^{-1} \\ & = t_1 x_B (\alpha_A a_A) x_A (a_A^{-1} \alpha_A^{-1}) t_1^{-1} \\ & \qquad \because a_A \alpha_A = \alpha_A a_A \ \& \ \alpha_A^{-1} a_A^{-1} = a_A^{-1} \alpha_A^{-1} \\ & = t_1 x_B \alpha_A (a_A x_A a_A^{-1}) \alpha_A^{-1} t_1^{-1} \\ & = t_1 (x_B \alpha_A) x'_A \alpha_A^{-1} t_1^{-1} \\ & = t_1 (\alpha_A x_B) x'_A \alpha_A^{-1} t_1^{-1} \\ & \quad \because x_B \alpha_A = \alpha_A x_B \ as \ \alpha_A \in RBl, x_B \in LBl \\ & = t_1 \alpha_A (x_B x'_A) \alpha_A^{-1} t_1^{-1} \\ & \Rightarrow t_3 t_7 \sim x_B x'_A \end{aligned}$$

B. *Verifiability*: Signature σ_2 does not contain $t_2 = bx'_c b^{-1}$, in order verify the signatures Cindy requires t_2 , she uses her secret key to calculate $t_2 = a_c t_1 a_c^{-1}$. Due the need of calculating t_2 , it is impossible for anyother to verify the signature as the verification phase requires a valid t_2.

C. *Strong Identifiability*: Warrant m_w used in the verification of the signatures includes original signer and proxy signer's identity and moreover, their public keys are used in the signature verification ($t_3 \sim x_B, t_3 t_7 \sim x_B x'_A$). So, it is easy to identify the both signer.

D. *Strong unforgeability*: In $\sigma_2 = (m_w, t_1, t_3, t_4, t_5, t_6, t_7)$, t_4 is dependent on z_2, the random braid α_B chosen by Bob and the secret key of Bob. Also, z_2 is shared between Bob and Alice so they only know this information and nobody except Bob has the information of secret key and the random number chosen by him. So, the proposed scheme provides the property of Strong unforgeability.

E. *Proxy protected*: Alice cannot create the same proxy signatures as Bob does for the nominee Cindy as creating the valid proxy signatures requires the valid proxy key Sp and random braids.

V. Conclusion

Nominative proxy signatures are a special type of proxy signatures that generates the signatures indeed for the nominee only and he is the only person that can check the validity of the signatures. The paper proposes the first attempt of transferring the concept of nominative proxy signatures from elliptical curves to braid groups and analyzed the security aspects. Conjugacy decomposition problem conjugacy search problem and base problem 1 forms the building blocks for the security; in addition to that the proposed scheme also satisfies all the properties of proxy signature. The proposed scheme will open the new gates of implementing nominative proxy for mobile communication at a low cost.

References

[1]. E. Artin, "The theory of braids", American Scientist, Vol.38, Issue.1, pp.112-119, 1950.

[2]. GK Verma, "*A Proxy Signature Scheme over Braid Groups",* Cryptology ePrint Archive Report, India, pp.1-47, 2008.

[3]. GK. Verma, "*A Proxy Blind Signature Scheme over Braid Groups*", International Journal of Network Security, Vol.9, No.3, pp.214-217, 2009.

[4]. I.A. Ismail, S.F. El-Zoghdy, A.A. Abdo, "*A Secure Nominative Proxy Signature Scheme for Distributed Shared Object Systems*", International Journal of Advanced Networking and applications, vol.2, Issue.1, pp.411-418, 2010.

[5]. M. Mambo, K. Usuda, E. Okamoto, "*Proxy Signatures- Revisited*", In Proc. Of ICICS (LNCS 1334), Berlin, pp.223-232, 1997.

[6]. SJ Kim, SJ Park, DH Won, "*Won Zero knowledge Nominative Signatures*", International Conference on the Theory and Applications of cryptography, Vol.95, Issue.7, pp.380-392, 1996.

[7]. A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[8]. Xiang-jun XIN, Mei-zhi WANG, Guo-zhen XIAO., *"A (k, n) Threshold Nominative Proxy Signature Scheme for Electronic Commerce*", Journal of China University of Mining and Technology, Vol.16, Issue.4, pp.470-474 2006.

[9]. Zuo-Wen Tan, Tan Liu, Zhuo-Jun Liu, "*Nominative proxy signature schemes*", Cryptography eprint Archive Report, US, pp.1-128, 2004.

[10]. LiCheng Wang, LiHua Wang, ZhenFu Cao, YiXian Yang, XinXin Niu, "*Conjugate adjoining problem in braid groups and new design of braid-based signatures*", Science China information sciences, Vol. 53, Issue.3, pp.524-536, 2010.

[11]. V. Kapoor, "*A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.39-46, 2013.

Authors Profile

Dr. Vandani Verma received the M.Phil. and Ph.D. degrees in Applied Mathematics from Institute of Basic Sciences. Khandari, Agra under the supervision of Prof. Sunder Lal in 2006 and 2010, respectively. She is at present working as an Assistant Professor in Department of Mathematics, Amity Institute of Applied Sciences, Amity University, Noida, India since 2008. She is a member of EAI and IAENG. She has published more than 10 research papers in reputed international journals and conferences including IEEE and it's also available online. Her area of interest includes cryptography algorithms, digital signatures, designated verifier signatures and coding theory. She has 11+ years of teaching experience and 4 years of Research Experience.