A Proxy Signature Scheme over Braid Groups

Girraj Kumar Verma
Department of Mathematics,
Hidustan College of Science and Technology, Farah, Mathura
girraj_ibs@rediffmail.com, girrajv@gmail.com

Abstract: Proxy signatures, introduced by Mambo, Usuda and Okamoto, allow a designated person to sign on behalf of an original signer. Braid groups has been playing an important role in the theory of cryptography as these are non commutative groups used in cryptography. Some digital signature schemes have been given but no proxy signature has been introduced over braid groups. In this paper we have proposed proxy signature scheme using conjugacy search problem over braid groups. Our proxy signature scheme is partial delegated protected proxy signature.

Key Words: Proxy Signature, Conjugacy Decision Problem, Braid groups, Conjugacy problem.

1. Introduction:

1.1 Background and Previous Results: Proxy signatures as mentioned in [11] allow a designated person called proxy signer, to sign a message on behalf of an original signer. According to the delegation type, the proxy signatures are classified as full delegation, partial delegation and delegation by warrant. For more please refer [4, 8, 11].These signatures should satisfies the following security parameters:

(i) Unforgeability: Besides an original signer, a designated signer can create a valid proxy signature for the original signer. But the third party who is not designated as proxy signer cannot create a valid proxy signature of the proxy signer.

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

(iii) Secret Key Dependencies: Proxy key or delegation pair can be computed only by the original signer's private key.

(iv)Distinguishability: Verifier can distinguish the original and proxy signatures efficiently.

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

(vi) Undeniability: Due to fact that the delegation information is signed by the original signer and the proxy signatures are generated by proxy signer's secret key both the signers can not deny their behavior.

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

These signatures are used in those situations, where original signer is unable to sign the message. He instructs some person (as secretary) as a proxy so that he can create a valid proxy signature. For example, an employee in a company needs to go on a business trip to some place which has no computer network access. During the trip he will receive e-mail, and expect to responds to some message quickly. Before going on a trip, he forwards his e-mail to his secretary, and instructs his secretary to respond to the e-mail in place of the employee according to prearranged plan. Then the secretary responds to the e-mail using the proxy signature for the employee.

The braid groups were first introduced to construct a key agreement protocol and a public key encryption scheme [9] presented at CRYPTO2000. In 2002 a signature scheme [10] was given by Ko et al using conjugacy problem. In 2008 [12], a blind signature scheme over braid group has been proposed by G. K. Verma. Several other digital signature schemes have also been proposed but no proxy signature scheme has been introduced.

In this paper we are introducing a proxy signature scheme over Braid groups. The base for our construction is conjugacy search problem in a non commutative group. In braid groups conjugacy decision problem is easy to compute and conjugacy search problem is computationally hard. Our Proxy signatures scheme is proxy version of the signature scheme given by Ko et al [10]. Our signature schemes have the following features and implications:

- This is a first proxy signature scheme over a non commutative group.

-This demonstrates the usefulness of braid groups in cryptography as implementation of braid groups is simple over a computer system.

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

Definition: For each integer $n \geq 2$, the *n*-Braid group B_n is defined to the group generated by $\sigma_1, \sigma_2, ...\sigma_{n-1}$ with the relation

(i) $\sigma_i \sigma_j = \sigma_j \sigma_i$ where $|i-j| \geq 2$

(ii) $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$ otherwise.

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

Some Hard Problem: In this section we describe some mathematically hard problems over braid groups.

We say that two braids *x* and *y* are 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 $\sigma_1, \sigma_2, ...\sigma_{m-1}$.

Cojugacy 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: 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 [10], 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 $b = \Delta^u \pi_1 \pi_2 ....\pi_l$, where Δ is called a fundamental braid and π_i's are permutations from Z_n to Z_n. Hence $|B_n(l)| \le (n!)^l$.

Now there is an efficient polynomial time algorithm in [10] for solving CDP in $B_n(l)$ but CSP is still exponential time to compute. So, this gap between two problems has been used by cryptographers to develop cryptographic protocols [9, 10, 12].

The rest of the paper is organized as follows:

In section 2 we have discussed the signature schemes by Ko et al. In section 3 we have discussed our proposed scheme. In section 4 we have discussed the security parameters satisfied by our scheme and in section 5 we have concluded our discussion.

2 Signature Scheme by Ko et al [10]:

In this section we are giving digital signature scheme by Ko et al. The parameter *n*, *l*, *d* are same as in [10]. Let $m \in \{0,1\}^*$ be the message to be signed and $H : \{0,1\}^* \to B_n(l)$ be a one way hash function.

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

Signing:
1. Signer chooses $(\alpha = b^{-1}xb, b) \in_R RSSBG(x, d)$;
2. Compute $h = H(m \,||\, \alpha)$ for a message *m* and let $\beta = b^{-1}hb$ 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 $h = H(m \,||\, \alpha)$.
2. Return accept if and only if $\alpha \sim x, \beta \sim h, \gamma \sim h, \alpha\beta \sim xh$ and $\alpha\gamma \sim x'h$.

3. Proposed Proxy Signature Scheme:

In this section we are giving our proposed scheme. Let the message to be signed be $m \in \{0,1\}^*$, and $H : \{0,1\}^* \to B_n(l)$ and $H_1 : B_n(l) \to \{0,1\}^*$ be one way hash functions and let *n ,l,* d are same as in [10].

1. Key Generation: Each user *u* does the following steps

***** Selects a braid $x_u \in_R B_n(l)$ such that $x_u \in SSS(x_u)$.

***** Choose $(x'_u = a_u x_u a_u^{-1}, a_u) \in RSSBG(x_u, d)$.

***** Return public key as $(x_u, a_u x_u a_u^{-1})$ and secret key a_u .

2. Proxy Generation: Original signer chooses $\alpha_o \in_R B_n(l)$ and computes $t_o = a_o \alpha_o a_o^{-1}$ and sends (α_o, t_o) to proxy signer in a secure way.

3. Proxy Verification: Proxy signer checks $t_o x'_o \sim \alpha_o x_o$.

4. **Signing by the Proxy signer:** Proxy signer computes $h = H(H_1(t_o x'_o) \| m)$ and chooses $b \in_R B_n(l)$ and computes $\alpha = b x_p b^{-1}, \beta = bhb^{-1}, \gamma = b a_p^{-1} h a_p b^{-1}$ and display $(\alpha, \beta, \gamma, t_o)$ as a signature on message *m.*

5. Verification: Verifier computes $h = H(H_1(t_o x'_o) \| m)$ and accepts the signature if and only if $\alpha \sim x_p,\ \beta \sim h,\ \gamma \sim h,\ \alpha\beta \sim x_p h,\ \alpha\gamma \sim x'_p h$.

Proof of Verification: Verification works because

$$\alpha = b x_p b^{-1},\ \beta = bhb^{-1},\ \gamma = (a_p b^{-1})^{-1} h (a_p b^{-1})$$

$$\alpha\beta = (b x_p b^{-1})(bhb^{-1}) = b(x_p h) b^{-1}$$

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

4. Analysis of Proposed Schemes:

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

4.1 Unforgeability: Let an adversary want to impersonate the proxy signatures. For creating a valid proxy signature, adversary needs to compute $h = H(H_1(t_o x'_o) \| m)$ and $\alpha = b x_p b^{-1}, \beta = bhb^{-1}, \gamma = b a_p^{-1} h a_p b^{-1}$. 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 proper proxy signer's secret key a_p by guessing it with at most a probability $1/(n!)^l$. That is the adversary can impersonate the proxy signature successfully with a probability $1/(n!)^l$.

Now, let proxy signer wants to impersonate the signature for illegal use. As he get $(\alpha_0, a_0\alpha_0 a_0^{-1})$ 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 atmost a probability$1/(n!)^l$. That is proxy signer can impersonate the proxy signature successfully with a probability$1/(n!)^l$.

4.2 Secret Keys Dependencies: Since the proxy signer computes$h = H(H_1(t_o x'_o) \| m)$, 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 verification of normal signature scheme is valid iff $\alpha \sim x, \beta \sim h, \gamma \sim h, \alpha\beta \sim xh, \alpha\gamma \sim x'h$ holds where$h = H(m \| \alpha)$. The verification of proxy signature scheme is valid iff $\alpha \sim x_p,\ \beta \sim h,\ \gamma \sim h,\ \alpha\beta \sim x_p h,\ \alpha\gamma \sim x'_p h$ holds, where$h = H(H_1(t_o x'_o) \| m)$. From the verification of two schemes, the verifier can distinguish the normal signatures and the proxy signatures efficiently.

4.5 Identifiability: Since for verification purpose, $h = H(H_1(t_o x'_o) \| m)$ is computed from original signer's public key and the verification is valid iff $\alpha \sim x_p,\ \beta \sim h,\ \gamma \sim h,\ \alpha\beta \sim x_p h,$ and $\alpha\gamma \sim x'_p h$ holds. So, the verifier can easily identify both the original signer as well as the proxy signer efficiently.

4.6 Undeniability: Since the proxy signatures are computed by using$(t_o = a_o\alpha_o a_o^{-1}, \alpha_o)$, as a proxy by original signer, and $\alpha = bx_p b^{-1}, \beta = bhb^{-1}, \gamma = ba_p^{-1}ha_p b^{-1}$ by proxy signer. So, both of the signers cannot deny for their behavior.

4.7 Non Repudiation: Since for construction of proxy signature, the proxy signer obtains the delegation pair $(t_o = a_o\alpha_o a_o^{-1}, \alpha_o)$ from original signer and to obtaina_o, the original signer's secret key, from this pair is conjugacy search problem. Now, since the original signer does not obtaina_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.

5. Conclusion: In this paper we have proposed a proxy signature scheme using conjugacy search problem over braid groups. We have also discussed the security parameters satisfied by our schemes. Although we have not discussed the efficiency of our schemes none the less our schemes proposed a new setting for constructing protocols for delegating signing rights.

6. References:

[1]: I. Anshel, M. Anshel, and D. Goldfeld, *An algebraic method for public key cryptography*, Math. Research Letter (6), pp. 287-291, 1999.

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

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

[4]: A. Boldyreva, A. Palacio and B. Warinschi, *Secure proxy signature schemes for delegation of signing rights*, available at http://eprint.iacr.org/2003/096.

[5]: 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.

[6]: W. Diffey and M. E. Hellman. *New directions in cryptography*, IEEE transaction on Information Theory, 22(6),pp. 74-84, June 1977.

[7]: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.

[8] 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.

[9]: 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.

[10]: 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

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

[12] G. K. Verma, *Blind signature schemes over Braid groups*, 2008, available at http://eprint.iacr.org/2008/027.