Blind signature scheme over Braid groups

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

Abstract: A blind signature scheme is a cryptographic protocol for obtaining a signature from a signer such that the signer's view of the protocol cannot be linked to the resulting message signature pair. In this paper we have proposed two blind signature schemes using braid groups. The security of given schemes depends upon conjugacy search problem in Braid groups.

Key Words: Blind signature, Braid groups, Conjugcy search problem.

1. Introduction: The concept of blind signatures was introduced by D. Chaum [6]. A blind signature scheme is a cryptographic primitive in which two entities a user and a signer are involved. It allows the user to have a given message signed by the signer, without revealing any information about the message or its signature. Blind signatures are the basic tools of digital cash payment systems, electronic voting systems etc.

In this paper we have proposed two blind signature schemes over Braid groups. The foundation of construction is conjugacy search problem in braid groups. In 2000 Ko et al [10] proposed a new public key cryptosystem on braid groups based on the difficulty of solving conjugacy search problem. The foundation of this system is quite different from widely used cryptosystems on number theoretic aspects as RSA .

The paper is organized as follows:

In section 2 we give a brief description of braid groups and computationally hard problems regarding conjugacy. In section 3 we have given the blind signature scheme by Boldyreva [4] in 2003. In section 4 we have given our proposed schemes and in section 5 we have discussed the security analysis of our schemes.

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].

2.1. 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.

Two braids are equivalent if one can be deformed to the other continuously in the set of braids.

B_n is the set of all equivalence classes of geometric *n*-braids with a natural group structure. The multiplication *ab* of two braids *a* and *b* is the braid obtained by positioning *a* on the top of *b*. The identity *e* is the braid consisting of *n* straight vertical strands and the inverse of *a* is the reflection of *a* with respect to a horizontal line. So a^{-1}can be found by switching the over strand and under strand.

2.2. Conjugacy Search Problem (CSP): In this section we describe some mathematically hard problems related to conjugacy.

We say that two braids *x* and *y* are conjugate if there exist an *a* such that $y = axa^{-1}$.

For $m<n$, B_m can be considered as a subgroup of B_n generated by $\sigma_1, \sigma_2, ...\sigma_{m-1}$.

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.

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

3. Generalized Conjugacy Search Problem:

Instance: $(x, y) \in B_n \times B_n$ such that $y = axa^{-1}$ for some $a \in B_m$, $m<n$.

Objective: Find $b \in B_m$ such that $y = bxb^{-1}$.

4. Conjugacy Decomposition Problem:

Instance: $(x, y) \in B_n \times B_n$ such that $y = axa^{-1}$ for some $a \in B_m$, $m<n$.

Objective: Find $b_1, b_2 \in B_m$ such that $y = b_1 x b_2$.

We consider two subgroups LB_n and RB_n of B_{2n} for some integer *n*, where LB_n (respectively RB_n) consisting of braids made by braiding left *n* (respectively right *n*) strands among *2n* strands. LB_n is generated by $\sigma_1, \sigma_2, ...\sigma_{n-1}$ and RB_n is generated by $\sigma_{n+1}, \sigma_{n+2}, ...\sigma_{2n-1}$. For any $a \in LB_n$ and $b \in RB_n$ $ab = ba$.

$f : LB_n \times B_{2n} \to B_{2n} \times B_{2n}$ such that $f(a, x) = (axa^{-1}, x)$

This function is a one way function, because it is easy to compute axa^{-1} from *a* and *x* but it is exponential time to compute *a* from axa^{-1} and *x*.

3. Blind Signature by Boldyreva [4]: For more detail please refer [4].

* **Key generation**: Let $H : \{0,1\}^* \to G_1$ be a map to point hash function. The secret key of signer is $x \in_R \mathbb{Z}_q$ and the public key is $P_{pub} = xP$.

Signing Protocol: Given secret key *x* and a message $m \in \{0,1\}^*$ to be signed.

* Blinding: The user chooses $r \in_R \mathbb{Z}_q$ and computes $M' = rH(m)$ and sends to signer.

* Signing: The signer computes $\sigma' = xM'$ and sends back to user.

* Unblinding: User computes $r^{-1}\sigma' = \sigma$ and (m, σ) is a signature.

Verification: The verifier accepts the signature iff $e(P_{pub}, H(m)) = e(P, \sigma)$.

4. Proposed Schemes: In this section we are giving two blind signature schemes both are based on conjugacy search problem on braid groups.

4.1 Simple Conjugacy Blind signature scheme: In this section we are giving the simple conjugacy signature scheme and then we are giving our proposed blind version of the scheme.

Simple Conjugacy signature scheme[11]: Let G be a non commutative group where CSP is hard and CDP is feasible. Let $H:\{0,1\}^* \to G$ be a hash function.

Key Generation: A public key is a CSP hard pair (x, x') in G and a secret key is a for $x' = axa^{-1}$.

Signing: Given a message m, a signature σ is given by $\sigma = a^{-1}ya$ where $y = H(m)$.

Verifying: A signature σ is valid if and only if $\sigma \sim y$ and $x'\sigma \sim xy$.

Our Scheme:

Let the message to be signed be $m \in \{0,1\}^*$ and let $H:\{0,1\}^* \to B_n$ be a one way hash function.

* **Key Generation:** Signer chooses $u \in B_{2n}$ and $a \in LB_n$. Then computes $u' = aua^{-1}$ and then makes public (u, u') and a secret.
* **Blinding:** The user selects $\alpha \in_r RB_n$ and computes $t = \alpha y\alpha^{-1}$ where $y = H(m)$ and sends t to signer.
* **Signing:** Signer computes $\sigma' = ata^{-1}$ and sends back to user.
* **Unblinding:** User computes $\sigma = \alpha^{-1}\sigma'\alpha$ and then (σ, m) be the message signature pair.
* **Verification:** verifier accepts the signature iff $\sigma \sim y$ and $\sigma u' \sim yu$.
* **Proof of verification:** Verification works because

$$\begin{aligned}\sigma = \alpha^{-1}\sigma'\alpha &= \alpha^{-1}(ata^{-1})\alpha \\ &= \alpha^{-1}(a(\alpha y\alpha^{-1})a^{-1})\alpha \\ &= \alpha^{-1}(\alpha(aya^{-1})\alpha^{-1})\alpha \\ &= aya^{-1}\end{aligned}$$

4.2: Blind signature scheme:

In this section we are giving blind signature scheme based on the signature scheme given by Ko et al [11]. The parameter *n, l, d* are same as in [11].

Scheme by Ko et al [11]**:**

Let $m \in \{0,1\}^*$ be the message to be signed and $H:\{0,1\}^* \to B_n(l)$ be is an 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 $\alpha\gamma \sim x'h$.

Our Scheme: Let $m \in \{0,1\}^*$ be the message to be signed and $H : \{0,1\}^* \to B_n(l)$ be is an one way hash function as in [11].

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:

* Signer chooses $(\alpha = bxb^{-1}, b) \in_R RSSBG(x, d)$ and sends α as a commitment.

***Blinding:** User chooses $\delta \in B_n(l)$ and computes $\alpha' = \delta\alpha\delta^{-1}$ and $h = (m \,||\, \alpha')$, then sends h to signer.

* Signer computes $\beta = bhb^{-1}$ and $\gamma = ba^{-1}hab^{-1}$, sends β and γ to user.

* **Unblinding:** User computes $\beta' = \delta\beta\delta^{-1}$ and $\gamma' = \delta\gamma\delta^{-1}$ then $(\alpha', \beta', \gamma')$ is a signature on m.

Verification: Verifier accepts signature iff $\alpha' \sim x, \beta' \sim h, \gamma' \sim h, \alpha'\beta' \sim xh$ and $\alpha'\gamma' \sim x'h$.

Proof of Verification: Verification works because

$$\alpha' = \delta bxb^{-1}\delta^{-1} = (\delta b)x(\delta b)^{-1},\ \beta' = \delta bhb^{-1}\delta^{-1} = (\delta b)h(\delta b)^{-1}$$

$$\gamma' = \delta ba^{-1}hab^{-1}\delta^{-1} = (\delta ba^{-1})h(\delta ba^{-1})^{-1}$$

$$\alpha'\beta' = ((\delta b)x(\delta b)^{-1})((\delta b)h(\delta b)^{-1}) = (\delta b)xh(\delta b)^{-1} \text{ and}$$

$$\alpha'\gamma' = ((\delta b)x(\delta b)^{-1})((\delta ba^{-1})h(\delta ba^{-1})^{-1})$$

$$= (\delta b)xa^{-1}h(\delta ba^{-1})^{-1}$$

$$= (\delta ba^{-1})axa^{-1}h(\delta ba^{-1})^{-1}$$

$$= (\delta ba^{-1})x'h(\delta ba^{-1})^{-1}$$

5. Security Analysis: The notion of security of blind signatures captures two properties. The first is "*blindness"* meaning the signer in the blind signing protocol should not learn any information about the messages, the user obtained signatures on. The second property is 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. The standard notion of unforgeability under chosen message attack of digital signatures cannot be used as a notion of unforgeability for blind signatures since by their construction a user has to be able to produce a valid signature of a previously signed message. The accepted formalization of security for blind signature is security against *one more forgery* [12].

Definition 5.1: Let *S = (K, S, V)* be a signature scheme and let *BS = (BK, BS, BV)* be the corresponding blind signature scheme. An adversary *A* learns the public key *pk* randomly generated by *BK*. *A* is allowed to play the role of a user in the runs of the blind signing protocol. After interactions with the signer *A* outputs some number of message signature pairs. The advantage of the adversary $Adv_{BS,I}^{blind}(A)$ is defined as the probability of *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 *A* with a non-negligible advantage $Adv_{BS,I}^{blind}(A)$.

Known target Conjugator search problem (CSP) and assumption: Let B_n be a braid group of index *n*. Let *a* be a random braid from B_n and let $y = axa^{-1}$ for some braid *x* and *y*. Let H be a random instance of a hash function family $\{\{0,1\}^* \to B_n\}$. The adversary *A* is given (*x, y, H)* and has access to the target oracle T_{B_n} that returns random braid z_i in B_n and the helper oracle $a(.)a^{-1}$. Let q_t, (respectively q_h) be the number of queries *A* made to the target oracle (respectively helper oracle). The advantage of the adversary attacking the chosen target CSP $Adv_{B_n}^{ct-csp}(A)$ is defined as the probability of *A* to output a set V of, say *l* pairs $((v_1, j_1),.....(v_l, j_l))$ Where all $1 \le i \le l, \exists 1 \le j_l \le q_t$ such that $v_i = a(z_i)a^{-1}$, all v_i's are distinct and $q_t < q_h$.
The chosen target CSP assumption states that there is no polynomial time adversary *A* with non negligible $Adv_{B_n}^{ct-csp}(A)$.

Theorem: If the chosen target CSP assumption is true in group B_n then our proposed blind signature scheme is secure against one more forgery under chosen message attack.
Proof: Let B_n be a braid group where Conjugacy Decision Problem is easy and Conjugacy Search Problem is hard and let $I = (x, H)$ be the global info. Let *A* be any polynomial time adversary attacking the conjugacy search blind signature scheme against one more forgery under chosen message attack. We will present a polynomial time adversary *B* for the chosen target CSP such that $Adv_{BCS(B_n),I}^{blind}(A) = Adv_{B_n}^{ct-csp}(B)$.
The statement of the theorem follows:
We note that since the signer in blind signing protocol of given scheme has only one move, it is enough in the definition of security of definition of 5.1 to give *A* access to a blind signing oracle $a(.)a^{-1}$ where *a* is a secret input by the signer. Since we analyze the security of given blind signature scheme in the random oracle model, the adversary *A* is also given access to the random hash oracle *H (.)*.
We now describe the algorithm of *B* which will simulate *A* in order to solve chosen target CSP. The adversary *B* is given (B_n, x, y, H) *B* has to simulate the random hash oracle and the blind signing oracle for *A*. Each time *A* makes a new hash oracle query, that is distinct from the previous hash queries, *B* forward it to its target oracle, returns the reply to *A* and add this query and the reply to the stored list of such pairs. If *A* makes a hash query that it already made before, *B* replies consistently with an old reply. When *A* makes a query to the blind signing oracle, *B* resends it to its helper oracle $a(.)a^{-1}$ and forwards the answer to *A*.

At some point A outputs a list of message signature pairs $((M_1,\sigma_1),.....(M_l,\sigma_l))$. For each $1 \le i \le l$ B finds M_i in the list of stored hash oracle queries and replies. Let j_i be the index of found pair B returns the list $((j_1,\sigma_1),.....(j_l,\sigma_l))$ as its own output.

It is easy to see that the view of A in the simulated experiment is in distinguishable form its view in the real experiment and that B is successful only if A is successful. Then $Adv^{blind}_{BCS(B_n),l}(A) = Adv^{ct-csp}_{B_n}(B)$.

6. Conclusion: In the proposed paper we have introduced a blind signature scheme using conjugacy search problem on braid groups. We have also discussed the security of our blind signature scheme.

7. 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 grous,* Annals of Math, study 82, Princeton University Press (1974).

[4]: A. Boldyreva, *Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffey Hellman group signature schemes,* available at http://eprint.iacr.org/2002/118.pdf

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

[7]: D. Chaum, A. Fiat, M. Naor, *Untraceable electronic cash*, Proceedings of Crypto 88, LNCS#403, pp. 319-327, Springer Verlag, 1988.

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

[9]: 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.

[10]: 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.

[11]: 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

[12]: D. Pointcheval and J. Stern, *Probably secure blind signature schemes,* Proc. Asiacrypt-96, LNCS#1163, pp. 252-265, Springer Verlag, 1996.