A Strong Blind Signature Scheme over Braid Groups

WEI Yun, XIONG Guo-Hua, BAO Wan-Su, ZHANG Xing-Kai

E-mail: weiyun456@sohu.com

Abstract: The rapid development of quantum computing makes public key cryptosystems not based on commutative algebraic systems hot topic. Because of the non-commutativity property, the braid group with braid index more than two becomes a new candidate for constructing cryptographic protocols. A strong blind signature scheme is proposed based on the difficulty of the one-more matching conjugacy problem in the braid groups, in which the signer can not relate the signature of the blinded message to that of the original message. The usage of random factor ensures that the blind signatures of the same message are different and avoids the weakness of simultaneous conjugating. The scheme can resist the adaptively chosen-message attack under the random oracle model.

Key words: Braid Group; Blind Signature; One-more Matching Conjugacy; Random Oracle Model

1 Introduction

The braid groups were first introduced by Artin[1]. Because of the non-commutativity property, the braid groups have become a new candidate to construct cryptosystem and attracted many cryptographers' attention. In 2000, they were first used to construct a key agreement protocol and a public key encryption scheme[2]. Since then there have been many attempts to design cryptographic primitives using braid groups. Positive proposals are key agreement protocols[3], an implementation of braid computations[4], the first digital signature scheme[5], entity authentication schemes[6, 7], public key encryption algorithm[8] and several digital signature schemes with additional properties[9-15].

The concept of blind signature was introduced by Chaum to allow a receiver to get a signature without giving the signer any information about the actual message or the resulting signature[16]. The blindness property plays a important role in electronic voting and electronic schemes[17, 18]. Since Chaum's first scheme was published many blind signature schemes have been proposed[19, 20, 21]. But using braid groups in the constructions of blind signature schemes is still a new subject[11, 15]. And Kumar claimed that all of them are not secure against the linkability vulnerability[22]. Hence, new constructions are desirable.

This paper proposes a new blind signature scheme over braid groups and security analysis is present. The rest of this paper is organized as follows. The second section introduces the basics of braid groups, security model and some notations. The signature scheme is proposed in section 3 and security analysis is given in section 4. Section 5 is the conclusion.

2 Preliminaries

2.1 Braid Group[2]

In this section, the basics of braid groups and hard problems in braid groups are introduced.

Definition 1 For each integer $n \geq 2$, the *n*-braid group B_n is an infinite non-commutative group which is defined as the group generated by $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ with the relation:

(1) $\sigma_i \sigma_j = \sigma_j \sigma_i \quad (|i-j| \geq 2)$;

(2) $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad (1 \le i \le n-2)$.

The integer n is called the braid index and each element of B_n is called an n-braid. A braid is said to be positive if and only if it can be written as a product of generators $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$, i.e., no negative powers of $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ are involved. The identity $\varepsilon \in B_n$ is also regarded as positive. The positive braids in B_n form a semi-group B_n^+ which embeds into B_n. The fundamental braid $\Delta \in B_n$ is defined as: $\Delta = (\sigma_1\sigma_2\cdots\sigma_{n-1})(\sigma_1\sigma_2\cdots\sigma_{n-2})\cdots(\sigma_1\sigma_2)\sigma_1$.

A partial ordering "$\le$" on the elements of B_n is defined by setting $v \le w$ if and only if there are positive braids $\alpha, \beta \in B_n^+$ satisfying $w = \alpha v \beta$. Any braid $\alpha \in B_n$ satisfying $\varepsilon \le \alpha \le \Delta$ is called a canonical factor. A factorization $\gamma = \alpha\beta$ of a positive braid γ into a canonical factor α and a positive braid β is said to be left-weighted if α has the maximal word length among all such factorizations. Every braid $w \in B_n$ can be written uniquely as $w = \Delta^r \alpha_1 \cdots \alpha_q$ such that $\alpha_1, \cdots, \alpha_q$ are canonical factors and $\alpha_i\alpha_{i+1}(1 \le i < q)$ is left-weighted. And r, denoted by $\inf(w)$, is the greatest integer j satisfying $\Delta^j \le w$. $r+q$, denoted by $\sup(w)$, is the smallest integer j satisfying $w \le \Delta^j$. q is called the canonical length of w.

Two braids $\alpha, \beta \in B_n$ are said to be conjugate if there exist a braid s such that $\beta = s^{-1}\alpha s$. And by $\alpha \sim \beta$ we mean α and β are conjugate. There are some mathematically hard problems related to conjugation over braid groups which can be used to design cryptographic protocols.

Definition 2 Conjugacy Decision Problem (CDP)

Instance: $(\alpha, \beta) \in B_n \times B_n$ such that $\beta = s^{-1}\alpha s$ for some $s \in B_n$.

Objective: Determine whether α and β are conjugate or not.

Definition 3 Conjugacy Search Problem (CSP)

Instance: $(\alpha, \beta) \in B_n \times B_n$ such that $\beta = s^{-1}\alpha s$ for some $s \in B_n$.

Objective: Find $t \in B_n$ such that $\beta = t^{-1}\alpha t$.

Definition 4 Simultaneous Conjugacy Search Problem (SCSP)

Instance: $(\alpha_1, s^{-1}\alpha_1 s), \cdots, (\alpha_N, s^{-1}\alpha_N s) \in B_n \times B_n$ for some $s \in B_n$.

Objective: Find $t \in B_n$ such that $t^{-1}\alpha_1 t = s^{-1}\alpha_1 s, \cdots, t^{-1}\alpha_N t = s^{-1}\alpha_N s$.

A cryptographic scheme is said to have the weakness of simultaneous conjugating if its security depends on the simultaneous conjugacy search problem.

Definition 5 Matching Conjugacy Search Problem (MCSP)

Instance: $(\alpha, \beta, \gamma) \in B_n \times B_n \times B_n$ such that $\alpha \sim \beta$.

Objective: Find $\delta \in B_n$ such that $\gamma \sim \delta$, $\alpha\gamma \sim \beta\delta$.

Obviously, if CSP can be solved easily, so does MCSP. MCSP is not harder than CSP.

There is an efficient polynomial time algorithm for solving CDP[5]. And many algorithms have been proposed to solve CSP, its variants and other problems in braid groups[24-29]. But none of them was proved to be polynomial in solving CSP or MCSP. So these hard problems are still used to develop cryptosystems.

2.2 Security Model

The existential forgery under adaptively chosen-message attack[31] is considered, in which the attack algorithm $\mathcal{F}$ is allowed to:

(1) make q_h queries to the random oracle;

(2) make q_s queries to the signing oracle for valid blind signatures of messages of its choice.

q_h and q_s are polynomial in the security parameter k . $\mathcal{F}$ is successful if it outputs, in polynomial time and with non-negligible probability $Adv_{\mathcal{F}}^{EFU-CMA}(k)$, a valid blind signature for some message m such that he has not asked for a valid blind signature of message m .

The attack algorithm $\mathcal{F}$ is said to be $(t, q_h, q_s, \varepsilon)$ -successful if the numbers of queries it makes to the random oracle and the signing oracle are not more than q_h and q_s , respectively, and it can successfully outputs the forgery with the probability $Adv_{\mathcal{F}}^{EFU-CMA}(k) \geq \varepsilon$ within polynomial time t . A signature scheme is said to be $(t, q_h, q_s, \varepsilon)$ -secure if there is no $(t, q_h, q_s, \varepsilon)$ -successful attack algorithm.

The definition of one-more matching conjugacy problem(OM-MCP) [32] is proposed in order to analyze the security of signature schemes based on braid groups.

Definition 6[27] (u, u') is given such that $u' \sim u$. $\mathcal{A}$ is a polynomial time algorithm, which can ask the matching conjugacy oracle $\mathcal{O}_{mc}(\cdot)$ and the challenge oracle $\mathcal{O}_{ch}(\cdot)$ for the following services:

(1) send a request $y \in B_n$ to $\mathcal{O}_{mc}(\cdot)$ and an element $\sigma \in B_n$ is returned by $\mathcal{O}_{mc}(\cdot)$, which satisfies $\sigma \sim y$, $\sigma u' \sim yu$;

(2) send a request to $\mathcal{O}_{ch}(\cdot)$ and a random element from B_n is returned by $\mathcal{O}_{ch}(\cdot)$.

OM-MCP means $\mathcal{A}$ has to output N pairs $(y_1, \sigma_1), \cdots, (y_N, \sigma_N)$ satisfying $\sigma_i \sim y_i$ and $\sigma_i u' \sim y_i u (i = 1, \cdots, N)$ after obtaining $y_1, \cdots, y_N$ from $\mathcal{O}_{ch}(\cdot)$ on the condition that the requests sent to $\mathcal{O}_{mc}(\cdot)$ are not more than $N - 1$.

OM-MCP is said to be hard if the success probability $Adv_{\mathcal{A}}^{OM-MCP}(k)$ is negligible for any polynomial time algorithm $\mathcal{A}$. Obviously, if One-more matching conjugacy problem can be solved efficiently, so does MCSP.

2.3 Notations

In this paper, $a \in_R A$ denotes a random choice of an element a from the set A . And $P_1 \Rightarrow P_2$ means P_2 holds if P_1 holds.

3 The Blind Signature Scheme over Braid Groups

Verma proposed two blind signature schemes[11] and one proxy blind signature scheme[15], which are claimed to be secure. But analysis shows that none of them withstands against the linkability vulnerability[22, 23]. In this section we are giving the new blind signature scheme over braid groups.

3.1 The Scheme

Let $B1_n, B2_n, B3_n, B4_n$ be the subgroups of B_n generated by $\{\sigma_1, \sigma_2, \cdots, \sigma_{\lfloor 2n/3 \rfloor - 1}\}$, $\{\sigma_{\lfloor n/3 \rfloor + 1}, \sigma_{\lfloor n/3 \rfloor + 2}, \cdots, \sigma_n\}$, $\{\sigma_1, \sigma_2, \cdots, \sigma_{\lfloor n/3 \rfloor - 1}\}$ and $\{\sigma_{\lfloor 2n/3 \rfloor + 1}, \sigma_{\lfloor n/3 \rfloor + 2}, \cdots, \sigma_n\}$, respectively. The system parameters n and l are positive integers large enough. Let

$$B_n(l) = \{b \in B_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\}$$

$$Bi_n(l) = \{b \in Bi_n \mid 0 \leq \inf(b) \leq \sup(b) \leq l\} (i = 1, 2, 3, 4)$$

$| B_n(l) | \leq l(n!)^l$ and $B_n(l)$ is finite set[12]. Then $B1_n(l), B2_n(l), B3_n(l), B4_n(l)$ are finite set, too.

$H : \{0,1\}^* \to B_n(l)$ is a collision resistant one way hash function. $m \in \{0,1\}^*$ is the message to be signed.

Key Generation: The signer chooses $u \in_R B1_n(l)$, $a \in_R B2_n(l)$ and computes $u' = aua^{-1}$.

Then a is the secret key and (u,u') is the public key.

Blinding: The user chooses $\alpha,\beta \in_R B3_n(l)$, $b \in_R B4_n(l)$ satisfying $\beta \neq \alpha^{-1}$ and computes $t = \alpha byb^{-1}\beta$ and sends t to the signer, where $y = H(m)$.

Signing: The signer computes $\sigma' = ata^{-1}$ and sends it back to the user.

Unblinding: The user computes $\sigma = \alpha^{-1}\sigma'\beta^{-1}$ and displays (σ, m) as the blind signature.

Verification: The verifier computes $y = H(m)$ and accepts the signature if and only if $\sigma \sim y$ and $\sigma u' \sim yu$.

3.2 Security Analysis

(1)Completeness

If the user and the signer perform honestly in the signature scheme, the generated blind signature can pass the verification. The completeness can be proved by the following equations.

$$a \in_R B2_n(l), \alpha,\beta \in_R B3_n(l) \Rightarrow a\alpha = \alpha a, \beta a^{-1} = a^{-1}\beta$$

$$\Rightarrow \sigma = a^{-1}\sigma' a = \alpha^{-1}a\alpha byb^{-1}\beta a^{-1}\beta^{-1} = abyb^{-1}a^{-1}$$

$$\Rightarrow \sigma \sim y$$

$$u \in_R B1_n(l), b \in_R B4_n(l) \Rightarrow b^{-1}u = ub^{-1}$$

$$\Rightarrow \sigma u' = abyb^{-1}a^{-1}aua^{-1} = abyb^{-1}ua^{-1} = abyub^{-1}a^{-1}$$

$$\Rightarrow \sigma u' \sim yu$$

(2)Blindness

In the scheme, $\sigma' \sim t$ and $\sigma \sim y$ hold. But σ' is not conjugate to σ . And t is not conjugate to y . So the signer can not link (σ', t) with (σ, y) without the knowledge of blinding factors. Hence, the signature scheme is a strong blind scheme.

(3)Unforgeability

Theorem. In the random oracle model, the proposed blind signature scheme is $(t, q_h, q_s, \varepsilon)$ -secure against the existential forgery under adaptively chosen-message attack.

Proof. Assume that an algorithm $\mathcal{F}$ is $(t, q_h, q_s, \varepsilon)$ -successful in attacking the proposed blind signature scheme, i.e., $\mathcal{F}$ produces, within polynomial time t and with non-negligible success probability not less than ε , a valid blind signature σ^* of the message m^* , such that he has asked q_h queries to the random oracle and q_s queries $m_i(i=1,\cdots,q_s)$ to the signing oracle and $m^* \notin \{m_i(i=1,\cdots,q_s)\}$. We design a solver algorithm $\mathcal{A}$ that uses $\mathcal{F}$ as a subroutine and solves OM-MCP within time t' with success probability not less than ε' ,where $\varepsilon' = \varepsilon$, $t' = t + t_s q_s + t_h q_h + t_{mc}(N-1-q_s)$, t_h , t_s and t_{mc} are the time consumed in one query to the random oracle, the signing oracle and the matching conjugacy oracle, respectively.

Let (u,u') be an input of the OM-MCP, in which $u' \sim u$. $\mathcal{A}$ sends $N(N > q_s)$ requests to the challenge oracle $\mathcal{O}_{ch}(\cdot)$ and obtains $y_1,\cdots,y_N$. $\mathcal{A}$ has to output $\sigma_1,\cdots,\sigma_N$ satisfying $\sigma_i \sim y_i$ and $\sigma_i u' \sim y_i u$ on the condition that the requests he sends to the matching conjugacy oracle $\mathcal{O}_{mc}(\cdot)$ are not more than $N-1$. $\mathcal{A}$ must simulate the environment of $\mathcal{F}$; that is, it must provide consistent answers to all the queries that $\mathcal{F}$ is allowed to make to the random oracle and the signing oracle. In order to maintain the consistency and to avoid collision, $\mathcal{A}$ keeps lists L_h and L_s to store the answers used.

When $\mathcal{F}$ makes the $j'th$ $(1 \leq j \leq q_h)$ query to the random oracle, $\mathcal{A}$ checks the corresponding list L_h . If an entry for the query is found, the same answer will be retuned; otherwise, $\mathcal{A}$ answers with y_j and stores the query and the answer in the list L_h .

$\mathcal{A}$ simulates the signing oracle to any query m in the following way. Firstly $\mathcal{A}$ checks the list L_h . If m is found in L_h , there exists $i \in \{1, \cdots, N\}$ satisfying $y_i = H(m)$; otherwise, $\mathcal{A}$ chooses y_i which has not appeared in L_h as the corresponding answer and stores them in L_h . Then $\mathcal{A}$ checks the list L_s . If y_i is found in L_s , the corresponding answer is returned to $\mathcal{F}$; otherwise, $\mathcal{A}$ sends the request y_i to the matching conjugacy oracle $\mathcal{O}_{mc}(\cdot)$ and returns the obtained answer σ_i to $\mathcal{F}$. Then y_i and σ_i will be stored in the list L_s .

If $\mathcal{F}$ successfully forge a blind signature σ^* of message m^* , m^* and the corresponding hash value y^* must satisfy that m^* exists in L_h but y^* can not be found in L_s and $y^* \in \{y_1, \cdots, y_N\}$. Assume that $y^* = y_\tau (1 \le \tau \le N)$. For $i = 1, \cdots, \tau - 1, \tau + 1, \cdots, N$, if y_i does not exist in L_s , $\mathcal{A}$ sends the request y_i to the oracle $\mathcal{O}_{mc}(\cdot)$ and stores y_i and the answer σ_i in L_s .

Finally, $\mathcal{A}$ outputs $(\sigma_1, \cdots, \sigma_N)$ as the solution of OM-MCP. For $i = 1, \cdots, N$, $\sigma_i \sim y_i$ and $\sigma_i u' \sim y_i u$ hold. And the requests send by $\mathcal{A}$ to $\mathcal{O}_{mc}(\cdot)$ are not more than $N - 1$. That is, $\mathcal{A}$ successfully solve the OM-MCP. The success probability equals to the success probability of $\mathcal{F}$, which means $\varepsilon' = \varepsilon$. The time $\mathcal{A}$ needs is the sum of the time $\mathcal{F}$ needs in the forgery and the time consumed in the interactions with all oracles. The queries $\mathcal{A}$ can ask to the hash and the signing oracles are not more than q_h and q_s respectively. Then the requests $\mathcal{A}$ sends to the matching conjugacy oracle are not more $N - 1 - q_s$. Hence, $t' = t + t_s q_s + t_h q_h + t_{mc}(N - 1 - q_s)$.

（4）**Non-determinability and free of simultaneous conjugacy weakness**

In the signature $\sigma = abyb^{-1}a^{-1}$, the introduction of the random factor b ensures that signatures of the same message are different. That is to say the signature is not determinable. In addition, b avoids the existences of conjugate pairs with the same conjugate a . Hence, the scheme does not have the weakness of simultaneous conjugating.

4 Conclusion

In this paper, a new blind signature scheme is proposed based on the difficulty of the conjugacy search problem and the multiple conjugacy search problem. Security analysis shows that the proposed scheme satisfies the security requirements of blind signature.

References:

[1] Artin E. Theory of braids, Annals of Math , 1947, 101-126.

[2] Ko K H, Lee S J, Cheon J H, et al. New public key cryptosystem using Braid groups. In: Proceedings of Crypto-2000, Lecture Notes in Computer Science, Springer-Verlag, 2000, 1880: 166-183.

[3] Anshel I, Anshel M, Fisher B, et al. New key agreement protocol in braid group cryptography. Topics in Cryptology- CT- RSA 2001, Lectures in Computer Science, Benlin: Springer Verlag, 2001, 2020: 1-15.

[4] Cha J C, Ko K H, Lee S J, et al. An efficient implementation of braid groups. In: Advances in Cryptology: Proceedings of ASIACRYPT 2001, Lecture Notes in Computer Science, Springer-Verlag, 2001, 2248: 144-156.

[5] Ko K H, Choi D H, Cho M S, et al. New signature scheme using conjugacy problem. http://eprint.iacr.org/2002/168.

[6] Sibert H, Dehornoy P, Girault M, Entity authentication schemes using braid word reduction. http://eprint.iacr.org/2002/187.

[7] Lal S and Chaturvedi A. Authentication schemes using braid groups. http://arXiv.org/cs.CR/0507066.

[8] Tang X M, Hong F and Cui G H. A public key encryption algorithm on braid groups. Journal of Software, 2007, 18(3): 722-729.

[9] Thomas T, Lal A K. Group Signature Scheme Using Braid Groups. http://arXiv.org/cs.CR/0602063.

[10] Zou S H, Zeng J W and Quan J J. Designated verifier signature scheme based on braid groups. http://eprint.iacr.org/2006/329.

[11] Verma G K. Blind signature schemes over Braid groups. http://eprint.iacr.org/2008/027.

[12] Verma G K. A proxy signature scheme over braid groups. http://eprint.iacr.org/2008/160.

[13] Zhang L L, Zeng J W. Proxy signature based on braid group. Journal of Mathematical Study, 2008, 41(1): 56-64.

[14] Lal S and Verma V. Some Proxy Signature and Designated Verifier Signature Schemes over Braid Groups. http://arXiv.org/cs.CR/09043422.

[15] Verma G K. A proxy blind signature scheme over braid groups. International Journal of Network Security, 2009, 9(3): 214-217.

[16] Chaum D. Blind signatures for untraceable payments. In: Advances in Cryptology: Proceedings of Crypto 82, 1982, 199-204.

[17] Rodrguez-Henrquez F, Ortiz-Arroyo D and Garca-Zamora C. Yet another improvement over the Mu-Varadharajan e-voting protocol. Computer Standards and Interfaces, 2007, 29: 471-480.

[18] Asaar M, Mohajeri J and Salmasizadeh M. Security modification for the Hwang-Wen-Hwang’s e-voting scheme. In Proceedings of International Conference on Security and Management, 2008, 486-490.

[19] Verma G K. New ID-based fair blind signatures. http://eprint.iacr.org/2008/093..

[20] Markus R. Lattice-based blind signature. http://eprint.iacr.org/2008/322.

[21] Overbeck R. A step towards QC blind signatures. http://eprint.iacr.org/2009/102.

[22] Kumar M. Linkability of blind signature schemes over braid groups. http://eprint.iacr.org/2009/192.

[23] Kumar M. On the security of a proxy blind signature schemes over braid groups. http://eprint.iacr.org/2009/361.

[24] Garber D, Kaplan S, et al. Length-based conjugacy search in the braid group. http://arXiv.org/math.GR/0209267.

[25] Hofheinz D, Steinwandt R. A Practical Attack on Some Braid Group Based Cryptographic primitives. In: Proceedings of PKC2003, Lectures in Computer Science, Benlin: Springer-Verlag, 2003, 2567: 187-198.

[26] Garber D, Kaplan S. Probabilistic solutions of equations in the braid group. http://arXiv.org/math.GR/0404076.

[27] Myasnikov A, Shpilrain V and Ushakov A. A practical attack on a braid group based cryptographic protocol. In: Proceedings of Crypto 2005, Lectures in Computer Science, Benlin: Springer-Verlag, 2005, 3621: 86-96.

[28] Tsaban B. On an authentication scheme based on the root problem in the braid group. http://eprint.iacr.org/2005/264.

[29] Myasnikov A, Shpilrain V and Ushakov A. Random subgroups of braid groups: an approach to cryptanalysis of a braid group based cryptographic protocol. In: Proceedings of PKC 2006, Lectures in Computer Science, Benlin: Springer-Verlag, 2006, 3958: 302-314.

[30] Myasnikov A and Ushakov A. Length based attack and braid groups: cryptanalysis of Anshel-Anshel-Goldfeld Key （AAGK）exchange protocol. In: Proceedings of PKC 2007, Lectures in Computer Science, Benlin: Springer-Verlag, 2007, 4450: 76-88.

[31] Pointcheval D and Stern J. Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 2000, 13(3): 361-396.

[32] Wang L C. Design and Analysis of Cryptographic Schemes Based on Braid Groups. Doctor Thesis, Shanghai Jiao Tong University, 2007.