SCIS 2004 The 2004 Symposium on
Cryptography and Information Security
Sendai, Japan, Jan.27-30, 2004
The Institute of Electronics,
Information and Communication Engineers

Provably-Secure Identification Scheme based on Braid Group

Zeen Kim * Kwangjo Kim *

Abstract— In this paper we construct a new interactive identification scheme based on the conjugacy problem. We prove that this scheme is secure against passive attacks if the matching triple search problem (MTSP) is intractable. Our proof is based on the fact that the conjugacy search problem (CSP) is hard in braid group, on the other hand, the conjugacy decision problem (CDP) is easy in braid group by Ko *et al.*'s algorithm.

Keywords: Identification Scheme, Braid Group, Conjugacy Search Problem, Provable Security

1 Introduction

Braid Cryptography. The braid group were first introduced to construct a key agreement protocol and a public-key encryption scheme at CRYPTO 2000 by Ko *et al.* [1]. Within the last years various attempts have been made to derive cryptographic primitives from problems originating in combinatorial group theory. As positive results are the discovery of a hard-core predicate for the conjugacy search problem in the braid group, and implementation of braid computation, and a conversion of the public-key encryption schemes into a provable one. But to the best of our knowledge, there is no identification scheme based on conjugacy problem over a braid group in the open literature.

Identification Scheme. It is well known that an *identification scheme* is a very important and useful cryptographic tool. The identification scheme is an interactive protocol where a prover, $\mathcal{P}$, tries to convince a verifier, $\mathcal{V}$, of his identity. Only $\mathcal{P}$ knows the secret value corresponding to his public one, and the secret value allows to convince $\mathcal{V}$ of his identity. If we replace "identity" by "authenticity" of messages, identification schemes are nearly equivalent to *signature schemes*. As mentioned by Fiat and Shamir [4] and Shoup [13], the distinction between identification and signature schemes is very subtle. Therefore, two types of schemes can be used interchangeably [4, 9, 10, 8].

Our Contribution. In this paper we construct an interactive identification scheme based on the conjugacy problem. We prove that this scheme is secure against passive attacks if the matching triple search problem (MTSP) is intractable. Our proof is based on the fact that the conjugacy search problem (CSP) is hard in braid group, on the other hand, the conjugacy decision problem (CDP) is easy in braid group by Ko *et al.*'s algorithm.

Outline of Paper. The rest of this paper is organized as follows: After describing the history of braid cryptography in this section, we state some preliminaries in Section 2. In Section 3 we present our identification scheme. In Section 4 we formally state our definition of security and give a proof of security and zero-knowledge for our scheme. Finally, we end with concluding remarks.

2 Preliminaries

2.1 Braid Groups

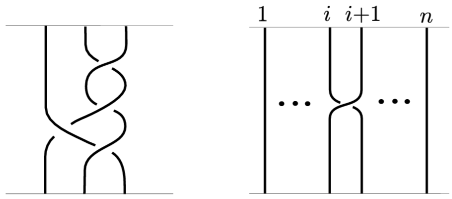
A *braid* is obtained by laying down a number of parallel strands and intertwining them so that they run in the same direction. The number of strands is called the braid *index*. The set B_n of isotopy classes of braids of index n is naturally equipped with a group structure, called the *n-braid group*, where the product of two braids x and y is nothing more than laying down the two braids in a row and then matching the end of x to the beginning of y.

Any braid can be decomposed as a product of simple braids. One type of simple braids is the *Artin generator* σ_i that has a single crossing between i-th and $(i+1)$-th strand. B_n is presented with the Artin generators $\sigma_1, \ldots, \sigma_{n-1}$ and relations $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $\mid i-j \mid > 1$ and $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ for $\mid i-j \mid = 1$. When a braid a is expressed as a product of Artin generators, the minimum number of terms in the product is called the word length of a. An example of braid and the generator is given in Figure 1.

We have still other presentations. Let S_n be the symmetric group of an n-element set $I_n = \{1, 2, \ldots, n\}$. Let $Ref = \{(i,j) \mid 1 \le i < j \le n\}$ be the set of reflections (that interchange two elements and fix the other elements of I_n) in S_n and S the subset $\{(i, i+1) \mid 1 \le i < n\}$ of Ref. We define $\ell(x)$ the *length of a permutation* x in S_n as

$$\ell(x) = min\{k \mid x_1 \cdots x_k \text{ for } x_i \in S\}$$

* Intetnational Research center for Information Security (IRIS), Information and Communications University (ICU), 119 Munji-ro, Yusong-ku, Daejeon, 305-714, Korea, Tel: +82-42-866-6236, Fax: +82-42-866-6273, ({zeenkim,kkj}@icu.ac.kr)



(a) the 3-braid $\sigma_2^2\sigma_1^{-1}\sigma_2$ (b) the generator σ_i

Figure 1: An example of braid and the generator

B_n admits another presentation with generators $\{rx \mid x \in S_n\}$ and relations $r(xy) = (rx)(ry)$ if $\ell(xy) = \ell(x) + \ell(y)$. In this presentation, the longest permutation w_0 with $w_0(i) = n+1-i$ yields a braid Δ, which is called the *fundamental braid* or the *half-twist* depending on authors. Let B_n^+ denote the submonoid of B_n generated by S_n. A braid in B_n^+ is said to be positive. A braid x is written uniquely, $x = \Delta^k x'$ where x' is in $B_n^+ - \Delta B_n^+$. This is called the normal form of x.

There is a partial order on $B_n^+ : x \le y \Leftrightarrow y \in xB_n^+$. The ordering is inherited to S_n (We identify a permutation σ with the corresponding braid $r\sigma$ in B_n^+. We denote rS_n by Ω for the sake of simplicity. For a braid $x \in B_n^+$, the greatest element of the set $\{y \in \Omega \mid y \le x\}$ is called the *left most factor* of x and denoted by $LF(x)$. A sequence of braids $(x_1, \ldots, x_k)$ in $\Omega - \{1\}$ is called the *greedy form* of x if $x_1 \cdots x_k = x$, $LF(x_i x_{i+1}) = x_i$ for all i. The above k in the greedy form is called the *Charney length* of x. This length function is easily extended to general braids using Thurston normal form.

2.2 Cryptographic Assumptions

Conjugacy Problems. In a non-commutative group G, two elements x, y in G are *conjugate* each other, written $x \sim y$ if $y = a^{-1}xa$ for some $a \in G$. Here a or a^{-1} is called a *conjugator* and the pair (x, y) is said to be *conjugate.* Clearly $\sim$ is an equivalence relation. A simple and natural question to ask in a noncommutative group G is the conjugacy problem that can be described as a decision version and a computational version. The conjugacy decision problem(CDP) asks to determine whether $x \sim y$ for a given instance $(x, y) \in G \times G$. The conjugator search problem(CSP) asks to find $a \in G$ satisfying $y = a^{-1}xa$ for a given instance $(x, y) \in G \times G$ such that $x \sim y$. We have to be careful when we mention instances in an infinite group G. In the current information theory, it is hard to discuss a uniform distribution in G of elements described by randomly chosen information. To avoid any potential controversy, we always assume that instances to a problem are randomly chosen in a finite subset of an infinite group G restricted by system parameters

We say a problem is *solvable* (*feasible*) if there is a deterministic finite (probabilistic polynomial-time) algorithm that outputs a solution that is accurate (accurate with non-negligible probability). The solvability is a mathematical notion and the complexity of an algorithm is not an issue as long as it is finite. A solvable problem is not necessarily feasible and vice versa.

The representation theory tells us that for any group G there are homomorphisms from G to rings that are invariant under conjugacy relation. Therefore CDP is always feasible although CDP may not be solvable. But the remaining question concerning CDP is how to construct an efficient algorithm to solve CDP with overwhelming probability.

On the other hand, there are many candidates for non-commutative groups where CSP is infeasible. However there is a normal form (such as Jordan form) of a conjugacy class in many matrix groups and so it is difficult to find a non-commutative group given as a subgroup of a matrix group that has an infeasible CSP. Therefore non-commutative groups with infeasible CSP are usually given by presentations.

We believe that CSP is infeasible in the braid groups B_n even though it is solvable. We will construct an efficient algorithm to give a solution to CDP with overwhelming accuracy. Unfortunately we do not know whether there is a polynomial-time algorithm that decides CDP.

- k-Simultaneous Conjugator Search Problem (k-SCSP)
  Instance : k pairs $(x_1, x'_1), \ldots, (x_k, x'_k) \in G \times G$ such that $x'_i = a^{-1}x_i a$ for all i.
  Objective : Find $b \in G$ such that $x'_i = b^{-1}x_i b$ for all i

It is reasonable to believe that k-SCSP becomes easier as k increases. In particular a solution to CSP is almost unique for the braid groups and so k-SCSP is easier than CSP.

Matching Conjugacy Problems. For a noncommutative group G, a pair $(x, x') \in G \times G$ is said to be CSP-hard if $x \sim x'$ and CSP is infeasible for the instance (x, x'). If (x, x') is CSP-hard, so is clearly (x', x). We now define two matching conjugacy problems in G that are equivalent and provide a foundation of our signature scheme.

- Matching Conjugate Search Problem (MCSP)
  Instance : A CSP-hard pair $(x, x') \in G$ and $y \in G$.
  Objective : Find $y' \in G$ such that $y \sim y'$ and $xy \sim x'y'$

- Matching Triple Search Problem (MTSP)
  Instance : A CSP-hard pair $(x, x') \in G$ and $y \in G$.
  Objective : Find a triple $(\alpha, \beta, \gamma) \in G \times G \times G$ such that $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$, and $\alpha\gamma \sim x'y$

If CSP in G is infeasible, instances of MCSP or MTSP can be given as $x, x', y \in G$ such that $x \sim x'$. In the description of the two matching problems, we do not want to exclude a group where CSP is partially infeasible, that is, the probability that a random conjugate pair (x, x') is CSP-hard is non-negligible. If a conjugate pair (x, x') is not CSP-hard, that is, an element $a \in G$ with $x' = a^{-1}xa$ can be known, then $y' = a^{-1}ya$ is a solution to MCSP and $(\alpha, \beta, \gamma) = (b^{-1}xb, b^{-1}yb, b^{-1}aya^{-1}b)$ is a solution to MTSP for any $b \in G$ and so the two matching conjugacy problems are feasible. These solutions are said to be *obvious*.

Fact 1 *In a non-commutative group G,* MCSP *is feasible if and only if* MTSP *is feasible.*

Proof. See the proof of '**Theorem 1**' in [2] ■

2.3 Ko *et al.*'s Conjugacy Signature

A braid-based signature scheme [BSS(braid signature scheme) for shortly] is introduced by Ko *et al.* in [2]. Now we describe the BSS.

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

Signing: Given a message m, choose $b \in G$ at random and let $\alpha = b^{-1}xb$ and $y = h(m\|\alpha)$, then a signature σ is given by a triple $\sigma = (\alpha, \beta, \gamma)$ where $\beta = b^{-1}yb$ and $\gamma = b^{-1}aya^{-1}b$.

Verifying: A signature σ is valid if and only if $\alpha \sim x$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim xy$, and $\alpha\gamma \sim x'y$.

2.4 Identification Schemes

Interactive Identification Scheme. An identification protocol or entity authentication protocol, which allows one party to gain assurances that the identity of another is as declared, thereby preventing impersonation.

An identification protocol is considered to be as an interactive protocol and the general setting for the protocol involves a *prover* or claimant $\mathcal{P}$ and a *verifier* $\mathcal{V}$. In general, $\mathcal{P}$ tries to convince the verifier $\mathcal{V}$ of his identity. The verifier is presented with, or presumes beforehand, the purported identity of the prover. The goal is to corroborate that the identity of the prover is indeed $\mathcal{P}$, *i.e.*, to provide entity authentication. Only $\mathcal{P}$ knows the secret value corresponding to his public one, and the secret value allows to convince $\mathcal{V}$ of his identity.

A primary purpose of identification is to facilitate access control to a resource, when an access privilege is linked to a particular identity. Examples of these cases are local or remote access to computer accounts, withdrawals from automated cash dispensers, or physical entry to restricted area or border crossings. In many applications such as cellular telephony the motivation for identification is to allow resource usage to be tracked to identified entities, to facilitate appropriate billing. Identification is also typically an inherent requirement in authenticated key establishment protocols.

Objectives of Identification Schemes. From the point of view of the verifier, the outcome of an identification protocol is either *acceptance* of the prover's identity as authentic, or *rejection.* More specifically, the objectives of an identification protocol include the following.

1. In the case of honest parties $\mathcal{P}$ and $\mathcal{V}$, $\mathcal{P}$ is able to successfully authenticate himself to $\mathcal{V}$, i.e., $\mathcal{V}$ will complete the protocol having accepted $\mathcal{P}$'s identity.
2. (*Transferability*) $\mathcal{V}$ cannot reuse an identification exchange with $\mathcal{P}$ so as to successfully impersonate $\mathcal{P}$ to a third party $\mathcal{A}$.
3. (*Impersonation*) The probability is *negligible* that any party $\mathcal{A}$ distinct from $\mathcal{P}$, carrying out the protocol and playing the role of $\mathcal{P}$, can cause $\mathcal{V}$ to complete and accept $\mathcal{P}$'s identity.
4. The previous points hold even if: a polynomially large number of previous authentication between $\mathcal{P}$ and $\mathcal{V}$ have been observed; the adversary $\mathcal{A}$ has participated in previous protocol executions with either or both $\mathcal{P}$ and $\mathcal{V}$; and multiple instances of the protocol, possibly initiated by $\mathcal{A}$, may be run simultaneously.

The precise definition of goals for an identification protocol is given with respect to provable security against the attacks in later. Informally speaking, the objectives derive the idea of zero-knowledge-based protocols whose executions do not reveal any partial information which makes $\mathcal{A}$'s task any easier whatsoever.

2.5 Attack Model

Types of attack. What an identification scheme is broken means that an adversary succeeds in an impersonation attempt (making the verifier accept with non-negligible probability). We can classify the type of attacks according to the interaction allowed to the adversary before an impersonation attempt [13].

The weakest form of attack is a *passive attack*, where the adversary is not allowed to interact with the system at all before attempting an impersonation; the only information the adversary has is the public key of the prover. Other attacks of intermediate level such as *eavesdropping attack* or *honest-verifier attack* are essentially equivalent to a passive attack.

The strongest form of attack is an *active attack*, in which the adversary is allowed to interact with $\mathcal{P}$ several times, posing as $\mathcal{V}$. We may consider active attacks as adaptive chosen-cipher text attacks. we should note that active attacks are quite feasible in practice.

3 Our Proposed Scheme

In this section, we present our identification scheme. Let B_n be a braid group where CSP is infeasible and CDP is feasible. Let $h : \{0,1\}^* \longrightarrow B_n$ be a hash function, that is, h is a collision-free one-way function that outputs an element of B_n expressed by a fixed amount of information. For example h can be given by a composition of a usual hash function of bit strings with a conversion from bit strings of a fixed length to elements of B_n.

Key generation. On input k, the key generation algorithm $\mathcal{G}$ works as follows:

1. Generate a braid group B_n.

2. Generate a CSP-hard pair $(x, x') \in B_n \times B_n$ such that $x' = a^{-1}xa$.

3. The public parameter is $\mathsf{Pub} = \langle B_n, (x, x')\rangle$, and the secret parameter is $\mathsf{Sec} = \langle a \rangle$. And then publish them.

Protocol actions between $\mathcal{P}$ and $\mathcal{V}$.
As is the case for other identification schemes, our protocol consists of *Δ*-times challenge-response protocol where Δ is a security parameter as usual identification protocol. The 1 round challenge-response protocol is described as follows:

1. $\mathcal{P}$ chooses $s \in B_n$ at random, computes $X = s^{-1}xs$, $X' = a^{-1}Xa$, and sends $\langle X, X'\rangle$ to $\mathcal{V}$.

2. $\mathcal{V}$ picks $r \in B_n$ at random, and sends r to $\mathcal{P}$.

3. On receiving r, $\mathcal{P}$ computes α, y, β, and γ such that

$$\begin{aligned} \alpha &= r^{-1}Xr \\ y &= h(X\|\alpha) \\ \beta &= r^{-1}yr \\ \gamma &= r^{-1}aya^{-1}r \end{aligned}$$

   and sends it to $\mathcal{V}$; $\mathcal{V}$ accepts $\mathcal{P}$'s proof of identity if all of $\alpha = r^{-1}Xr$, $Xx \sim X'x'$, $\alpha \sim X$, $\beta \sim \gamma \sim y$, $\alpha\beta \sim Xy$, and $\alpha\gamma \sim X'y$ are satisfied and rejects otherwise.

Our proposed scheme repeats Δ-times of the Protocol actions between $\mathcal{P}$ and $\mathcal{V}$. This identification scheme is represented graphically in Figure 2. Once after this scheme can be proved to be secure against passive adversaries.

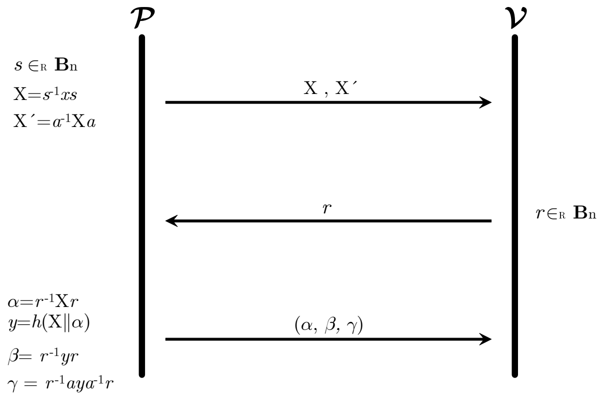


Figure 2: Proposed Scheme

4 Security Analysis

In this section, we analyze our proposed scheme. First we recall the definition of secure identification scheme by Feige *et al.* and then we prove the scheme is secure against the impersonation attack under the definition given by Feige *et al.* [3].

4.1 Secure Identification

Let us remind a secure identification scheme based on the definition given by Feige *et al.* [3]

Definition 1 *An identification scheme $(\mathcal{P}, \mathcal{V})$ is secure if*

SI-1 $(\overline{\mathcal{P}}, \overline{\mathcal{V}})$ *succeeds with overwhelming probability.*

SI-2 *There is no coalition of $\widetilde{\mathcal{P}}$ and $\widetilde{\mathcal{V}}$ with the property that, after a polynomial number of executions of $(\overline{\mathcal{P}}, \widetilde{\mathcal{V}})$ and relaying a transcript of the communication to $\widetilde{\mathcal{P}}$, it is possible to execute $(\widetilde{\mathcal{P}}, \overline{\mathcal{V}})$ with non-negligible probability of success. The probability is taken over the distribution of the public key and the secret key as well as the coin tosses of $\overline{\mathcal{P}}$, $\widetilde{\mathcal{V}}$, $\widetilde{\mathcal{P}}$, and $\overline{\mathcal{V}}$, up to the time of the attempted impersonation.*

4.2 Security Proof

Theorem 1 *The proposed scheme satisfies the properties of secure identification scheme [3].*

Proof.
SI-1. $\overline{\mathcal{P}}$ can convince the $\overline{\mathcal{V}}$ of his identity with probability 1. Honest prover can compute the values, X, X', α, y, β, and γ for any random challenge value r from $\overline{\mathcal{V}}$. After receiving (α, β, γ), $\overline{\mathcal{V}}$ outputs the 'accept' with probability 1. Because the $\overline{\mathcal{V}}$ always check the verifying equation easily by using the conjugacy decision algorithm.

$$\alpha = r^{-1}Xr \ ; \quad \text{so, } \alpha \sim X$$

$$X'x' = a^{-1}Xaa^{-1}xa = a^{-1}Xxa, \quad Xx \sim X'x'$$

$$\beta = r^{-1}yr \ ; \quad \text{so, } \beta \sim y$$

$$\gamma = r^{-1}aya^{-1}r = (a^{-1}r)^{-1}y(a^{-1}r) \ ; \quad \text{so, } \gamma \sim y$$

$$\alpha\beta = r^{-1}Xrr^{-1}yr = r^{-1}Xyr \ ; \quad \text{so, } \alpha\beta \sim Xy$$

$$\begin{aligned} \alpha\gamma &= r^{-1}Xrr^{-1}aya^{-1}r \\ &= r^{-1}Xaya^{-1}r \\ &= r^{-1}aX'ya^{-1}r \\ &= (a^{-1}r)^{-1}X'y(a^{-1}r) \end{aligned}$$

So, $\alpha\gamma \sim X'y$.
Above equation is always successful. So, this shows that our proposed scheme satisfies the property SI-1.

SI-2. First, we define the adversary, $\mathcal{A}$ who works as follows:

1. $\mathcal{A}$ runs the protocol for several times as verifier. This means that $(\mathcal{P}, \mathcal{A})$ works. $\mathcal{A}$ takes the data from the $(\mathcal{P}, \mathcal{A})$ in his memory.

2. $\mathcal{A}$ runs the protocol for several times as prover. This means that $(\mathcal{A}, \mathcal{V})$ works. In this stage, $\mathcal{A}$ tries to impersonate the prover.

If the success probability of $\mathcal{A}$ is negligible, we can obtain the property $\mathsf{SI\text{-}2}$ of our proposed scheme.

After the stage 1, $\mathcal{A}$ gets the data $D_1, D_2, \ldots, D_k$.

$$(D_i = \{X_i, X_i', r_i, \alpha_i, y_i, \beta_i, \gamma_i\})$$

On stage 2, $\mathcal{A}$ sends X_t, X_t' ($X_t \in D_t$ $(1 \leq t \leq k)$) to verifier and gets a random challenge r from verifier. For impersonating the prover, $\mathcal{A}$ must compute the value $\gamma = r^{-1}ah(X_t \| r^{-1}X_t r)a^{-1}r$ without knowing the secret value a. Because it is impossible that find other solution which satisfies $\beta \sim \gamma$, $\gamma \sim y$, $\alpha\gamma \sim X'y$. From the infeasibility of k-SCSP, the success probability is negligible. This means that it is infeasible to get a from any number of pairs $(r_i\gamma_i r_i^{-1}, y_i) = (ay_i a^{-1}, y_i)$. Therefore there is no dishonest prover who can impersonate with non-negligible probability.

This completes the proof of **Theorem 1**. ■

5 Comparison

In this section we compare our proposed scheme with previous identification schemes (KK scheme, Schnorr scheme and GQ scheme) in the point of public key size, existence of security proof, 1-round running time, security against active attack and cryptographic problem. Table 1 shows the result of our comparison.

The proof of security is given for all object schemes. But Schnorr scheme and GQ scheme gives only security against passive attacks. KK scheme, Schnorr scheme, GQ scheme and our proposed scheme are based on BDH(bilinear Diffie-Hellman) problem, DLP (discrete logarithm problem), IFP (integer factorization problem), and MTSP, respectively. Their public key size are 512 bit, 512 bit, 1024 bit and 591 bit, respectively.

The modular multiplication speed on Pentium 3 866MHz is 0.115 ms in [?]. The number of modular multiplications and point additions are given in [?, 8] and we can estimate that $\mathsf{A} \leq 2\mathsf{M}$. KK scheme takes $140\mathsf{A}+2\mathsf{M}$ for $\mathcal{P}$'s processing and $141\mathsf{M}$ for $\mathcal{V}$'s. So, estimating times are 32.4 ms ($\mathcal{P}$) and 16.2 ms ($\mathcal{V}$). $\mathcal{P}$'s processing is same as braid signature's signing. So, it takes 25.8 ms. $\mathcal{V}$ have 2 conjugacy decision more than verifying of [2]. Conjugacy decision algorithm takes 5.15ms. $\mathcal{V}$'s processing time takes $36.1(= 25.8 + 10.3)$ ms.

Comparison	KK02	Schnorr96	GQ88	Our scheme
Security proof	Yes	Yes	Yes	Yes
Public Key Size (bits)	512	512	1,024	591
Active attack Security	Yes	No	No	Yes
Cryptographic problem	BDH	DLP	IFP	MTSP
1-Round running time ($\mathcal{P}$)	32.4	24.2	7.0	25.8
estimation(ms) ($\mathcal{V}$)	16.2	24.2	3.9	36.1

Table 1: Comparison with previous schemes

6 Concluding Remarks

In this paper, we design and analysis of secure identification schemes against passive adversaries. We have reviewed previous works. And then we have presented our suggestions to solve the problems.

We have presented a practical construction of a new identification scheme based on the conjugacy problem on the braid group. The identification scheme is typical three-round (canonical) identification. In the open literature, there is no identification scheme based on conjugacy problem over braid groups. We have settles the the our proposed model of our approach. Then we prove that our identification scheme satisfies the property for secure identification schemes.

We hope that our scheme can open the new genre of braid cryptosystem. As a future works, we modify our scheme to be more efficient and implement the our proposed scheme. We will re-evaluate the current security proof more rigorously and try to design another identification scheme based Shoup-like approach [13].

References

[1] K. Ko, S. Lee, J. Cheon, J. Han, J. Kang, C. Park, “New Pulic-key Cryptosystem using Braid Groups,” *Advances in Cryptology – Crypto 2000*, LNCS 1880, Springer-Verlag, pp. 166–183, 2000.

[2] K.H. Ko, D.H. Choi, M.S. Cho, and J.W. Lee, “ New signature scheme using conjugacy problem,” *Preprint; http://eprint.iacr.org/2002/168*, 2002.

[3] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity”, *J. Cryptology*, 1: 77–94, 1988.

[4] A. Fiat and A. Shamir, “How to prove yourself: pratical solutions to identification and signature problems”, *Advances in Cryptology – Crypto '86*, LNCS 263, Springer-Verlag, pp. 186-194, 1987.

[5] K. Kurosawa and S.-H. Heng, “From Digital Signature to ID-Based Identification/Signature,” *To appear in PKC 2004*.

[6] O. Goldreich and H. Krawczyk, “On the composition of zero-knowledge proof systems”, In *Proceedings of the 17th ICALP*, LNCS 443, Springer-Verlag, pp 268–282, 1990.

[7] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems”, *SIAM J. Comput.*, 18: 186–208, 1989.

[8] T. Okamoto, “Provably secure and practical identification schemes and corresponding signature schemes”, *Advances in Cryptology – Crypto '92*, LNCS 740, Springer-Verlag, pp. 31–53, 1993.

[9] L. Guillou and J. Quisquater, “A practical zero-knowledge protocol fitted to security microprocessors minimizing both transmission and memory”, *Advances in Cryptology – Eurocrypt '88*, LNCS 330, Springer-Verlag, pp. 123–128, 1989.

[10] K. Otha and T. Okamoto, “A modification of the Fiat-Shamir scheme”, *Advances in Cryptology – Crypto ’88*, LNCS 403, Springer-Verlag, pp. 232–243, 1990.

[11] A.D. Santis, S. Micali, and G. Persiano, “Non-interactive zero-knowledge proof systems”, *Advances in Cryptology – Crypto ’87*, LNCS 293, pp 52–72, 1988.

[12] C. Schnorr, “Security of 2^t-root identification and signatures”, *Advances in Cryptology – Crypto ’96*, LNCS 1109, Springer-Verlag, pp. 143–156, 1996.

[13] V. Shoup, “On the security of a practical identification scheme”, *J. Cryptology* 12: 247–260, 1999.

[14] M. Bellare and A. Palacio, “GQ and Schnorr identification schemes ; proofs of security against impersonation under active and concurrent attacks,” *Advances in Cryptology – CRYPTO 2002*, LNCS 2442, Springer-Verlag, pp. 162–177, 2002.