Provably Secure Integration Cryptosystem on Non-Commutative Group

Xiaoming Chen[1], Weiqing You[2]

[1,2] Beijing Electronic Science & Technology Institute Beijing 100070, China
[1] University of Science and Technology of China, Hefei 230026, China
chenxmphd@yeah.net, scipaperyou@sina.com

Abstract. Braid group is a very important non-commutative group. It is also an important tool of quantum field theory, and has good topological properties. This paper focuses on the provable security research of cryptosystem over braid group, which consists of two aspects: One, we prove that the Ko's cryptosystem based on braid group is secure against chosen-plaintext-attack(*CPA*) which proposed in CRYPTO 2000, while it dose not resist active attack. The other is to propose a new public key cryptosystem over braid group which is secure against adaptive chosen-ciphertext-attack(*CCA2*). Our proofs are based on random oracle models, under the computational conjugacy search assumption(*the CCS assumption*). This kind of results have never been seen before.

Keywords: Braid group, Public key cryptosystem, IND-CPA, IND-CCA2, Conjugacy, non-commutative group

1 Introduction

1.1 Background and related work

In 1994, Shor[2] proposed a quantum fourier transforma algorithm, which can construct an integer factorization polynomial (quantum) algorithm, which poses a substantial threat to the security of RSA. In 2003, Proos et al. [3] extended the Shor algorithm to the elliptic curve, and obtained the polynomial (quantum) algorithm for solving the discrete logarithm problem over the elliptic curve, which poses a substantial threat to the security of ECC. However, these famous quantum algorithms mainly focus on the exchange structure. For some Cryptosystems based on noncommutative structures[1][4][7][8],that attacks are ineffective. Therefore, the design of cryptographic systems over certain non-commutative groups is one of the most important way to find algorithms which can resist quantum attacks. It is the key research object in the field of post quantum cryptography.

The braid group is a very important infinite non-commutative generation group. Because of its many difficult problems and many commutative subgroups, that make it can be used as the carrier of the design of cryptographic systems. The braid group has good algebraic properties, making it a good platform for

designing quantum attack algorithms. In 2000, Ko et al proposed a public key cryptosystem based on braid group, after that, there are many papers about the design of the braid cryptosystem in [9][11][12], followed by some questions about the hypothesis of the braid base problem [11][13][14][15][16] were proposed. However, as far as the existing technology and theory are concerned, the conjugate problem on the braid group is still difficult[18][19], that is, there is no polynomial algorithm that can solve the conjugate problem on the braid group in polynomial time, and even in quantum computation, there is no effective algorithm for the conjugate problem at present.

After many years of research and development, people have a deeper understanding of braid cryptology, especially the starting point of the braid group, which greatly promotes the research of cryptographic systems on noncommutative group[36][37][38]. On the other hand, there are some fast computation algorithms were proposed[28][32][22][31], and the implementation of this algorithm has been solved by the center of steven research on algebraic[39]. Recently, there are some digital signature algorithms were proposed, such as WalnutDSA[5][6][10], and others schemes was proposed[20][21]. These scheme are very attractive. The performance of computing and storage is approaching the need of application.

But so far, the research on the proof security of braid cryptosystems is very rare or even empty, which greatly hinders the delovepment and application of braid cryptosystem. The security of IND-CPA, IND-CCA and IND-CCA2 is enhanced in turn [23] [24] [25], and the structure of cipher algorithm is becoming more and more complex, and the consumption of computation is also increasing. The early construction of CCA or CCA2 security is realized by the zero knowledge proof method, so the cryptographic algorithm constructed is very practical. In 1993, Bellare and Rogaway[26] proposed a method to prove IND-CCA2 under the random oracle model. The model is concise and is widely recognized and loved by the researchers. Although the security conclusion of the cryptographic algorithm in this model does not fully represent the actual security[26], it is still the most effective index of security. The ROM model and method are still the main technology of the public key cryptographic security argument. The public key cryptography algorithm based on braid group also uses ROM model to prove security.

1.2 Our result

There are more detailed studies on the definition, basic concepts and computational methods of the braid group[27], this article will not be described here. But the main section is focused on the proof of security of the braid group cryptography algorithm. Our main work is as follows:

1. We have finished the research on the indistinguishability of the braid cryptosystem proposed by Ko[1], proved that it is IND-CPA through the random oracle model under the computational conjugacy search assumption(the CCS assumption), and we emphasize that it does not have the ability to resist active attack.

2. According to the original EIGamal scheme design idea, we propose a cryptographic algorithm with IND-CPA security under the standard model and the decisional conjugacy search assumpiton(the DCS assumption).

3. Adopting the design idea of hybrid encryption system, we propose a new public key cryptosystem in braid against adaptive chosen ciphertext attack. Subsequently, its IND-CCA2 security is proved under the random oracle model.

Before this paper, there is no any research on the provable secure encryption algorithm on braid group, Our algorithm and proof fill this gap. Like all the provable security analysis procedures, the proof part of this article has taken a lot of space, but its logical process is not very complicated.

2 Preliminaries

2.1 Braid Group

Compared with the general group, the structure of the braid group is more special and complicated. Although the introduction of braid group theory has been very detailed, we still need to spend some words to introduce the basic theories related to it. If the readers need more about braid theory, please refer to literature[27]

Definition 1 Define B_n as a braid group generated by $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$, and following the relations:

$$\begin{cases} \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{if } |i-j| = 1 \\ \sigma_i\sigma_j = \sigma_j\sigma_i & \text{if } |i-j| \geq 2 \end{cases}$$

The string formed by generators in braid group B_n is called a braid (or a word), and the number of generators in the string is the length of the braid (or word). It can be clearly seen that the braid group is a class of non commutative generating groups, but there are a large number of commutative elements on it. It is easy to see that there are many commutative subgroups on it. Assume $B_{l+r} = \{\sigma_1, \sigma_2, \cdots, \sigma_{l+r-1}\}$, let $LB_l = \{\sigma_1, \sigma_2, \cdots, \sigma_{r-1}\}$ be a left subgroup, and $RB_r = \{\sigma_{r+1}, \sigma_{r+2}, \sigma_{r+l-1}\}$ be a right subgroup. So

$$\forall x \in LB_l, \forall y \in RB_r, xy = yx$$

This is the basis for computing for building an available key exchange protocol and a cryptographic algorithm.

Definition 2 The fundamental braid is represented by the symbol Δ:

$$\begin{cases} \Delta = 1 \\ \Delta_n = \Delta_{n-1}\sigma_{n-1}\sigma_{n-2}\cdots\sigma_1 \end{cases}$$

Theorem 1 [28] Every word w in braid can be represented as a canonical form: $W = \Delta^k A, k \in Z, A \in B_n^+$, or the canonical form for short. Of course, there are many standard forms of it. Please refer to the literature[29][30][32][33]. For the sake of convenience, this paper adopts the left canonical form.

The literature[1] enumerated 7 hard problems in the braid group, we show that problems related to this paper as follow:

1. Conjugacy Decision Problem
   Instance: $(x, y) \in B_n \times B_n$.
   Objuctive: Determine whether x and y are conjugate or not.

2. Conjugacy Search Problem
   Instance: $(x, y) \in B_n \times B_n$ such that x and y are conjugate.
   Objuctive: Find $a \in B_n$ such that $y = axa^{-1}$.

3. Generalized Conjugacy Search Problem
   Instance: $(x, y) \in B_n \times B_n$ such that $y = axa^{-1}$ for some $b \in B_m$, $m \leq n$.
   Objuctive: Find $a \in B_m$ such that $y = axa^{-1}$.

These hard problems are very useful for the analysis of public key cryptosystems,thus, we will use them to construct the security assumption.

2.2 Security Model

The security model is portrayed by Indistinguishability-Game (IND-GAME), mainly divided into three levels: Indistinguishability-Chosen Plaintext Attack (IND-CPA) [23], Indistinguishability - (Non Adaptive) Chosen Ciphertext Attack (IND-CCA) [24], Indistinguishability - (Adaptive) Chosen Ciphertext Attack (IND-CCA2) [25].

Definition 3 Indistinguishability-Chosen Plaintext Attack (IND-CPA) The IND game of public key encryption scheme under chosen plaintext attack (IND-CPA) is as follows[23]:

Step1. Initialization The Challenger B generates the password system, and the Adversary A obtains the system public key pk.

Step2. The Adversary A generates plaintext messages and obtains encrypted ciphertext (polynomial bounded).

Step3. Challenge. The Adversary A outputs two messages of the same length, M_0 and M_1. The Challenger B chooses $\beta \leftarrow_R \{0, 1\}$, cipher M_β, and sends ciphertext C^* (Target ciphertext) to A.

Step4. Guess. A outputs β', if $\beta' = \beta$, return 1, A attack successfully.

The advantage of the adversary A can be defined as a function of the parameter K:

$$Adv_A^{CPA}(K) = \left| Pr[\beta' = \beta] - \frac{1}{2} \right|$$

For a polynomial time adversary A, there is a negligible function $\varepsilon(K)$ that makes $Adv_A^{CPA}(K) \leq \varepsilon(K)$ set up, it is called IND-CPA security.

Definition 4 Indistinguishability - (Non Adaptive) Chosen Ciphertext Attack (IND-CCA) [24] The IND game of public key encryption scheme under chosen ciphertext attack (IND-CCA) is as follows[24]

Step1. Initialization The Challenger B generates the password system, and the Adversary A obtains the system public key pk.

Step2. Training. A sends the ciphertext C to the B, and B sends the decrypted plaintext to A.(Polynomial bounded)

Step3. Challenge. The Adversary A outputs two messages of the same length, M_0 and M_1. The Challenger B chooses $\beta \leftarrow_R \{0,1\}$, cipher M_β, and sends ciphertext C^* (Target ciphertext) to A.

Step4. Guess. A outputs β', if $\beta' = \beta$, return 1, A attack successfully.

The advantage of the adversary A can be defined as a function of the parameter K:

$$Adv_A^{CCA}(K) = \left| Pr[\beta' = \beta] - \frac{1}{2} \right|$$

For a polynomial time adversary A, there is a negligible function $\varepsilon(K)$ that makes $Adv_A^{CCA}(K) \leq \varepsilon(K)$ set up, it is called IND-CCA security.

The above attack is also called 'lunch time attack'. At a 'lunch time', the enemy has a black box that can perform the decryption operation, and the black box can not be used after 'lunch time'.

Definition 5 Indistinguishability - (Adaptive) Chosen Ciphertext Attack (IND-CCA2) [25] The IND game of public key encryption scheme under adaptive chosen ciphertext attack (IND-CCA2) is as follows[25]

Step1. Initialization The Challenger B generates the password system, and the Adversary A obtains the system public key pk.

Step2. Training1. A sends the ciphertext C to the B, and B sends the decrypted plaintext to A.(Polynomial bounded)

Step3. Challenge. The Adversary A outputs two messages of the same length, M_0 and M_1. The Challenger B chooses $\beta \leftarrow_R \{0,1\}$, cipher M_β, and send ciphertext C^* (Target ciphertext) to A.

Step4. Training2. A sends the ciphertext $C(C \neq C^*)$ to the B, and B sends the decrypted plaintext to A.(Polynomial bounded)

Step5. Guess. A outputs β', if $\beta' = \beta$, return 1, A attack successfully.

The advantage of the adversary A can be defined as a function of the parameter K:

$$Adv_A^{CCA2}(K) = \left| Pr[\beta' = \beta] - \frac{1}{2} \right|$$

For a polynomial time adversary A, there is a negligible function $\varepsilon(K)$ that makes $Adv_A^{CCA2}(K) \leq \varepsilon(K)$ set up, it is called IND-CCA2 security.

3 Two Schemes Provably Secure Against Chosen Plaintext Attack

In order to research on the indistinguishable security of public key algorithms over the braid group , we first give the following two assumptions:

The Compution Conjugacy Search Assumption (The CCS Assumption) Given $X, Y \in B_n, X = xgx^{-1}, Y = ygy^{-1}$, it is hard to compute $Z = (xy)g(xy)^{-1}$

The Decisional Conjugacy Search Assumption (The DCS Assumption) Assume that B_{l+r} is a braid group, LB_l and RB_r are left subgroup and right subgroup, respectively. Assume $g, z \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, y \leftarrow_R RB_r$, The following two distributions are computationally non - distinguishable:

$$R = (g, xgx^{-1}, ygy^{-1}, zgz^{-1}) \tag{1}$$
$$D = (g, xgx^{-1}, ygy^{-1}, (xy)g(xy)^{-1}) \tag{2}$$

We can call the distribution R is Random four tuple while the distribution D is DCS four tuple.

3.1 A Scheme Provably Secure Against Chosen Plaintext Attack

Before analyzing Ko. public key cryptosystem[1], we first propose a non hashing braid group public key cryptosystem, which is very similar to the original ELGamal Scheme[34].

Algorithm 1 Assume B_{l+r} is a braid group, left subgroup LB_l and right subgroup RB_r.

KeyGeneration One selects a element $g \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, X = xgx^{-1}$, the public key is (X, g), the private key is (x, g).
Encryption The cipher gets a message $m \in B_{l+r}$, one selects a element $y \leftarrow_R RB_r$, compute $Y = ygy^{-1}, Z = yXy^{-1}, c = Zm$. The ciphertext is (Y, c).
Decryption The decipher gets the target ciphertext (Y, c), computes $Z = xYx^{-1}, m = Z^{-1}c$.

Theorem 2 If the DCS assumption holds, the algorithm 1 is $IND - CPA$.

Proof: Assume a PPT adversary A attack algorithm 1, A outputs M_0, M_1, the challenger B chooses $\beta \leftarrow_R \{0, 1\}$, cipher it and sents the ciphertext to A. A runs an randomization algorithm, outputs the guessing value β. If $\beta' = \beta$, A attack successfully, represented by event *succ*. Note that the advantage of A is

$$Adv_A^1 = \left| \frac{1}{2} - Pr[Succ] \right|$$

The following constructs an adversary B, B uses A to attack the DCS assumption. Assume B output the tuple $T = (g_1, g_2, g_3, g_4)$, the advatage of B is

$$Adv_B^1 = \left| \frac{1}{2} - Pr[\beta' = \beta] \right|$$

The structure of the B is shown as follows:

$$\begin{array}{l} Experiment_B^1(T): \\ \quad pk = (g_1, g_2); \\ \quad (M_0, M_1) \leftarrow A(pk), |M_0| = |M_1| = l(K); \\ \quad \beta \leftarrow_R (0, 1); \\ \quad C^* = (g_3, g_4 M_\beta); \\ \quad \beta' \leftarrow A(pk, C^*); \\ \quad If \quad \beta' = \beta, return \quad 1; \\ \quad else \quad return \quad 0. \end{array}$$

When return 1, B guesses that the input T is four tuples DCS, else B guesses that the input T is random four tuples. Let R represent events 'T is the random four tuples', D represent events 'T is the DCS four tuples'. Two steps of proof:

1. $Pr[Exp_B^1(T) = 1|R] = \frac{1}{2}$.

When the 'event R' happened, g_4 is a random element in B_{l+r}, so it is independent of the ciphertext C^*. Thus, A have no any information of β, he can't guess β with more than $1/2$ probability. When B return 1 if and only if A success, so $Pr[Exp_B^1(T) = 1|R] = \frac{1}{2}$.

2. $Pr[Exp_B^1(T) = 1|D] = Pr[Succ]$.

When the 'event D' happened, $g_2 = xg_1x^{-1}, g_3 = yg_1y^{-1}, g_4 = yg_2y^{-1}$. So B return 1 if and only if A success.

$$\begin{aligned} Pr[Exp_B^1(T) = 1] &= Pr[D]Pr[Exp_B^1(T) = 1|D] + Pr[R]Pr[Exp_B^1(T) = 1|R] \\ &= \frac{1}{2}Pr[Succ] + \frac{1}{2} \times \frac{1}{2} \end{aligned}$$

$$\begin{aligned} Pr[Exp_B^1(T) = 0] &= Pr[D]Pr[Exp_B^1(T) = 0|D] + Pr[R]Pr[Exp_B^1(T) = 0|R] \\ &= \frac{1}{2}(1 - Pr[Succ]) + \frac{1}{2} \times \frac{1}{2} \end{aligned}$$

so, $\left|Pr[Exp_B^1(T) = 1] - Pr[Exp_B^1(T) = 0]\right| = \left|Pr[Succ] - \frac{1}{2}\right|$

If A attacks B with the non negligible advantage of $\varepsilon(K)$, then B attacks the DCS assumption with the same advantage.

3.2 The Security of Ko's cryptosystem

In the provable security theory of public key cryptography, the weaker the security assumption is, the more rigorous the results are. Like the DDH assumption and the CDH assumption[35], The DCS assumption is more stronger than the CCS assumption. So a scheme under the CCS assumption is more security. The following algorithm 2 was proposed by Ko et al. in crypto 2000[1].

Algorithm 2 Assume B_{l+r} is a braid group, left subgroup LB_l and right subgroup RB_r, $H \leftarrow_R \{H : B_{l+r} \rightarrow \{0,1\}^{l(k)}\}$ is a hash function.

KeyGeneration One selects a element $g \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, X = xgx^{-1}$, the public key is (X, g), the private key is (x, g).
Encryption The cipher gets a message $m \in B_{l+r}$, one selects a element $y \leftarrow_R RB_r$, computes $Y = ygy^{-1}, Z = yXy^{-1}, c = H(Z) \oplus m$. The ciphertext is (Y, c).
Decryption The decipher gets the target ciphertext (Y, c), computes $Z = xYx^{-1}, m = H(Z) \oplus c$.

Theorem 3 If H is a random oracle and the CCS assumption holds, then the algorithm 2 is secure against chosen plaintext attack.

Proof: Assume that A is an $IND-CPA$ adversary who attacks algorithm 2, the advantage of A is Adv_A^2, B is a adversary who attacks the CCS assumption, the advantage of B is Adv_B^2. If A attacks algorithm 2 with the non negligible advantage of $\varepsilon(K)$, it must exist B whom attacks the CCS assumption with the advantage of $Adv_B^2 \geq 2\varepsilon(K)$. The $IND-CPA$ game of algorithm 2 is described as follows:

$Exp_A^2(K)$:
$g \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, X = xgx^{-1}$;
$pk = (g, X), sk = x$;
$(M_0, M_1) \leftarrow A^{H(\cdot)}(pk), |M_0| = |M_1| = l(K)$;
$\beta \leftarrow_R (0,1), y \leftarrow_R RB_r, Y = ygy^{-1}, Z = yXy^{-1}, C^* = (Y, H(Z) \oplus M_\beta)$;
$\beta' \leftarrow A^{H(\cdot)}(pk, C^*)$;
$If \quad \beta' = \beta, return \quad 1$;
$else \quad return \quad 0$.

The advantage of A can be define as a function of the security parameter K

$$Adv_A^2(K) = \left| Pr[Exp_A^2(K) = 1] - \frac{1}{2} \right|$$

B gets $(g, X, \hat{c}_1)$, $\hat{c}_1$ is the first component of the target ciphertext. Using the A attacks algorithm 2 as a subprogram, The following steps are taken to calculate $\hat{y}$, $\hat{c}_1 = \hat{y}g\hat{y}^{-1}$.

1. One chooses a random string $\hat{h} \leftarrow_R 0,1^{l(k)}$ as a guessing value for $H(\hat{Z})$, B don't know the $\hat{Z}$, sents $pk = (g, X)$ to A;

2. H queries (Bounded polynomial times): B build the list H^{list} (Initial empty), element type is $(\hat{Z}_i, \hat{h}_i)$, A can query H^{list} any time, B respond as follows:

• If $\hat{Z}$ in H^{list}, respond with $\hat{h}$ in $(\hat{Z}, \hat{h})$.

• If $\hat{c}_1 = \hat{y}X\hat{y}^{-1}$, respond with $\hat{h}$, record $\hat{Z} = \hat{y}X\hat{y}^{-1}$, save the $(\hat{Z}, \hat{h})$ into list.

• Else, choose random string $\hat{h} \leftarrow_R \{0,1\}^{l(k)}$, respond with $\hat{h}$, record $\hat{Z} = \hat{y}X\hat{y}^{-1}$, save the $(\hat{Z}, \hat{h})$ into list.

3. Challenge. A outputs two messages M_0, M_1, B chooses $\beta \leftarrow_R \{0,1\}$, sets $\hat{c}_2 = \hat{h} \oplus M_\beta$, sends $(\hat{c}_1, \hat{c}_2)$ (as ciphertexts) to A;

4. After end of above steps, A outputs β', B outputs $\hat{Z} = \hat{y}X\hat{y}^{-1}$ which recorded in step2.

Assume that the *event* D: In the simulation, $H(\hat{Z})$ appears in the list H^{list}.

Assertion 1 B is complete in above simulation process.

proof: It is easy to know:

• In the H inquiry of A, each value is answered by random string. In the real attacks of A, the value of the function is generated by the random oracle, so the function value obtained by the A is uniformly distributed;

• For A, $\hat{h} \oplus M_\beta$ is a one-time pad system, From the randomness of $\hat{h}$, it is known that $\hat{h} \oplus M_\beta$ is random for A.

So, Both of the view of A and its view in real attacks are not distinguishable in calculation.

Assertion 2 In the simulation attack above, $Pr[D] \geq 2\varepsilon$

proof Obviously $Pr[Exp_A^2(K) = 1|\neg D] = \frac{1}{2}$,

$\because$ $Adv_A^2 \geq \varepsilon(K)$, in the simulation:

$$\begin{aligned} Pr[Exp_A^2(K) = 1] &= Pr[\neg D]Pr[Exp_A^2(K) = 1|\neg D] + Pr[D]Pr[Exp_A^2(K) = 1|D] \\ &\leq Pr[\neg D]Pr[Exp_A^2(K) = 1|\neg D] + Pr[D] \\ &= \frac{1}{2}Pr[\neg D] + Pr[D] \\ &= \frac{1}{2} + \frac{1}{2}Pr[D] \\ Pr[Exp_A^2(K) = 1] &\geq Pr[\neg D]Pr[Exp_A^2(K) = 1|\neg D] \\ &= \frac{1}{2}Pr[\neg D] \end{aligned}$$

$$= \frac{1}{2} - \frac{1}{2}Pr[D]$$

$\therefore\ \frac{1}{2} - \frac{1}{2}Pr[D] \leq Pr[Exp_A^2(K) = 1] \leq \frac{1}{2} + \frac{1}{2}Pr[D]$

$\therefore\ Adv_A^2(K) = \left|Pr[Exp_A^2(K) = 1] - \frac{1}{2}\right| \leq \frac{1}{2}Pr[D]$

$\therefore\ \frac{1}{2}Pr[D] \geq 2Adv_A^2(K) = 2\left|Pr[Exp_A^2(K) = 1] - \frac{1}{2}\right| \geq 2\varepsilon(K)$

In summary, if A can take advantage of a non negligible advantage $\varepsilon(K)$ to attack algorithm 2, it must exist B whom take $Adv_B^2 \geq 2\varepsilon(K)$ to attack the CCS assumption. So the algorithm 2 is secure against $IND - CPA$.

4 A Public Key Cryptosystem on Braid Provably Secure Against Adaptive Chosen Ciphertext Attack

Under the current complex network environment, it is entirely possible for the adversary to achieve active attack. Therefore, it is very important for the study of an algorithm with IND-CCA2 security. Next, we will propose a cryptographic algorithm secure against adaptive chosen ciphertext attack on braid groups.

Algorithm 3 (E, D) is a pair of symmetric key algorithms secure against adaptive chosen ciphertext attack, other conditions are the same as Algorithm 1.

KeyGeneration One selects a element $g \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, X = xgx^{-1}$, the public key is (X, g), the private key is (x, g).
Encryption The cipher gets a message $m \in B_{l+r}$, one selects a element $y \leftarrow_R RB_r$, computes $Y = ygy^{-1}, Z = yXy^{-1}, k = H(Z), c = E_k(m)$. The ciphertext is (Y, c).
Decryption The decipher gets the target ciphertext (Y, c), computes $Z = xYx^{-1}, k = H(Z), m = D_k(m)$.

Theorem 4 If H is a random oracle, and the CCS assumption holds, then the algorithm 3 is secure against chosen ciphertext attack.

Proof: Suppose an IND-CCA2's adversary A breaks the algorithm 3 with a not negligible advantage $\varepsilon(k)$, then there must be an adversary B attacks the CCS assumption with the advantage of $Adv_B^3 \geq 2\varepsilon(k)$.

Assume that A is an IND-CCA2 adversary who attacks algorithm 3, the advantage of A is Adv_A^3, B is a adversary who attacks the CCS assumption, the advantage of B is Adv_B^3. If A can take advantage of a non negligible advantage $\varepsilon(K)$ to attack algorithm 3, it must exist B whom takes $Adv_B^3 \geq \varepsilon(K)$ to attack the CCS assumption. The IND-CCA2 game of algorithm 3 is described as follows:

$Exp_A^3(K)$:
$g \leftarrow_R B_{l+r}, x \leftarrow_R LB_l, X = xgx^{-1}$;
$pk = (g, X), sk = x$;
$(M_0, M_1) \leftarrow A^{H(\cdot), D_{sk}(\cdot)}(pk), |M_0| = |M_1| = l(K)$;
$\beta \leftarrow_R \{0,1\}, y \leftarrow_R RB_r, Y = ygy^{-1}, Z = yXy^{-1}, k = H(Z), C^* = (Y, E_k(M_\beta)$;
$\beta' \leftarrow A^{H(\cdot), D_{sk,\neq C^*}}(pk, C^*)$;
$If \quad \beta' = \beta, return \quad 1$;
$else \quad return \quad 0$.

$D_{sk,\neq C^*}$ means A can not query C^* to the oracle. The advantage of A can be define as a function of the security parameter K

$$Adv_A^3(K) = \left| Pr[Exp_A^3(K) = 1] - \frac{1}{2} \right|$$

B gets $(g, X, \hat{c}_1)$, $\hat{c}_1$ is the first component of the target ciphertext. Using the A attack algorithm 3 as a subprogram, The following steps are taken to calculate $\hat{y}$, $\hat{c}_1 = \hat{y}g\hat{y}^{-1}$.

1. One chooses a random string $\hat{h} \leftarrow_R \{0,1\}^{l(k)}$ as a guessing value for $H(\hat{Z})$, B don't know the $\hat{Z}$, sents $pk = (g, X)$ to A;

2. H queries (Bounded polynomial times): B build the list H^{list} , element type is (y, c_1, h), initial value is $(*, \hat{c}_1, \hat{h})$, $*$ means unknow in this section. A can query H^{list} any time, B respond as follows:(assume A query y, B compute $c_1 = ygy^{-1}$)

• If (y, c_1, h) in H^{list}, respond with h.

• If $(*, c_1, h)$ in H^{list}, respond with h, Replacing $(*, c_1, h)$ with (y, c_1, h) in H^{list}.

• Else, choose random string $h \leftarrow_R \{0,1\}^{l(k)}$, h response, save the (y, c_1, h) into H^{list}.

3. Decryption inquiries. A queries $(\overline{c}_1, \overline{c}_2)$ to B, B responds as follows:

If there is one item $(\overline{y}, \overline{c}_1, \overline{h}$ or $*, \overline{c}_1, \overline{h}$ in the table, $D_{\overline{h}}(\overline{c}_2)$ response, else, choose a random string $h \leftarrow_R \{0,1\}^{l(K)}$, $D_{\overline{h}}(\overline{c}_2)$ response, save $*, \overline{c}_1, \overline{h}$ into H^{list}.

4. Challenge. A outputs two messages M_0, M_1, B chooses $\beta \leftarrow_R \{0,1\}$, sets $\hat{c}_2 = E_{\hat{h}}(M_\beta)$, sends $(\hat{c}_1, \hat{c}_2)$ (as the target ciphertext) to A;

5. A execution step 2, but he can't query $(\hat{c}_1, \hat{c}_2)$.

6. Guess. A outputs β', B check the H^{list}, if exist one item $\hat{y}, \hat{c}_1, \hat{h}$, then output $\hat{y}$.

Assume that the *event* D: In the simulation, $H(\hat{Z})$ appears in the list H^{list}.

Assertion 1 B is complete in above simulation process.

proof: It is easy to know:

• In the H inquiry of A, each value is answered by random string.

In the real attack of A, the value of the function is generated by the random oracle, so the function value obtained by the A is uniformly distributed;

• According to the structure of H^{list}, $\overline{h} = H(\overline{y}), \overline{c}_1 = \overline{y}g\overline{y}^{-1}$, so the decryption response of B is valid.

Thus, both of the view of A and its view in real attacks are not distinguishable in calculation.

Assertion 2 In the simulation attacks above, $Pr[D] \geq 2\varepsilon$

proof If $H(\hat{Z})$ does not appear in H^{list}, then A have no $\hat{h}$, because of $\hat{c}_2 = E_{\hat{h}}(M_\beta)$ and E's security, then $Pr[\beta' = \beta|\neg D] = \frac{1}{2}$. The rest is the same as Theorem 3.

In summary, if A can take advantage of a non negligible advantage $\varepsilon(K)$ win the IND-CCA2 game, then $H(\hat{Z})$ appears at least in the probability of $2\varepsilon(K)$ in the H^{list} in above simulation process, B check the elements in H^{list} one by one in step6. So the probability of the success of the adversary B is equal to the event D, thus, B attacks the CCS assumption with the non negligible advantage of $2\varepsilon(K)$. The algorithm 3 is secure against $IND - CCA2$.

Note that In this algorithm, we assume that the symmetric algorithm is IND-CCA2, because its construction method is already very mature.[17][35][40][41]

5 Conclusion

For the first time, this paper uses a random oracle model to prove that the Ko cryptosystem[1] is IND-CPA security and gives a non-hash public key cryptosystem on braid group, which is very similar to the ElGamal system[34]. Finally, we propose an algorithm on braid group which is secure against chosen of ciphertext attack. This is a mixed encryption algorithm[17]. The keys of the symmetric encryption part is produced by a random oracle. This design gets rid of the bondage of the braid group, and making the algorithm more compatible and more practical.

This paper opens the door of the research on the security of the braid cryptosystem, fills the blank of the research direction of provably security in braid cryptosystem, to effectively promote the algorithm to engineering applications, to a certain extent, this article has a pioneering spirit.

Acknowledgments. We thank any reviewers to comments our paper.

References

1. Ko, K.H., Lee, S.J., Cheon, J.H., Han, J.W., Kang, J., Park, C: New Public-Key Cryptosystem Using Braid Groups. In: Bellare M.(eds) CRYPTO 2000. LNCS, vol 1880. Springer, Heidelberg. (2000) https://doi.org/10.1007/3-540-44598-6_10
2. Shor, P.W.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. Quantum Entanglement and Quantum Information-Ccast. pp. 303-332. (1999)
3. PROOS, J., ZALKA, C.: Shors Discrete Logarithm Quantum Algorithm for Elliptic Curves. Quantum Inf. Comput. **3**(4), 317-344. (2003)
4. Anshel, I., Anshel, M., and Goldfeld, D.: An algebraic method for public-key cryptography. Math. Res. Lett.**6**, 287-291. (1999)
5. Algebraic Eraser Digital Signature System, Provisional Patent, September, 2015.
6. Anshel, I., Atkins, D., Goldfeld, D., Gunnells, P.E.: Walnut DSA^{TM}: A Quantum-Resistant Digital Signature Algorithm. Cryptology ePrint Archive, Report2017/058 (2017). http://eprint.iacr.org/2017/058.
7. Dehornoy, P.: Using shifted conjugacy in braid-based cryptography. arXiv preprint arXiv:cs/0609091 (2006)
8. Gligoroski, D.: Candidate One-Way Functions and One-Way Permutations Based on QuasigroupString Transformations. arXiv preprint arXiv:cs/0510018 (2005)
9. Cha, J.C., Ko, K.H., Lee, S.J. and Han J.W.: An Efficient Implementation of Braid Groups. In: Boyd C.(eds) ASIACRYPT 2001. LNCS, vol. 2248, pp. 144-156. Springer, Heidelberg (2001)
10. Hart D., Kim D., Micheli G., Pascual-Perez G., Petit C., Quek Y.: A Practical Cryptanalysis of WalnutDSA^{TM}. In: Abdalla M., Dahab R. (eds) PKC 2018. LNCS, vol. 10769, pp. 381-406. Springer, Cham (2018)
11. Cheon,J.H., Jun, B.: A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem. In: Boneh D. (eds) CRYPTO 2003. LNCS, vol. 2729, pp. 212C225. Springer, Heidelberg (2003)
12. Myasnikov, A.D., Shpilrain, V., Ushakov, A.: A Practical Attack on a Braid Group Based Cryptographic Protocol. In: Shoup V.(eds) CRYPTO 2005. LNCS, vol. 3621, pp. 86-96. Springer, Heidelberg (2005)
13. Myasnikov, A.D., Ushakov, A.: Length Based Attack and Braid Groups: Cryptanalysis of Anshel-Anshel-Goldfeld Key Exchange Protocol. In: Okamoto T., Wang X. (eds) PKC 2007. LNCS, vol. 4450, pp. 76-88. Springer, Heidelberg (2007)
14. Lee, E., Park, J.H.: Cryptanalysis of the public key encryption based on braid groups. In: Biham E. (eds) EUROCRYPT 2003. LNCS, vol. 2656, pp. 477-490. Springer, Heidelberg (2003)
15. Hughes, J., Tannenbaum, A.: Length-based attacks for certain group based encryption rewritingsystems. arXiv preprint arXiv:cs/0306032 (2003)
16. Gebhardt,V.: Conjugacy search in braid groups: From a braid-based cryptography point of view. In: Marc G. (eds) AAECC 2006. LNCS, Vol. 17, pp. 219-238. Springer, Heidelberg (2006)
17. Fujisaki, E., Okamoto, T.: Secure integration of asymmetric and symmetric encryption schemes. In: Wiener, M.J. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537C554. Springer, Heidelberg (1999)
18. Ko, K.H., Lee, J., Thomas, T.: Towards generating secure keys for braid cryptography. Des. Codes Cryptogr. **45**(3), 317-333, (2007). https://doi.org/10.1007/s10623-007-9123-0

19. Prasolov, M.: Small braids having a big ultra summit set. arXiv preprint arXiv:cs/0306032
20. Clark,S., Hill, D. : Quantum Supergroups V. Braid Group Action. J.Commun. Math. Phys. **344**(1), 25-65. (2016) https://doi.org/10.1007/s0022
21. Dobson, E., Gavlas,H., Morris,J., Witte, D: Automorphism group of the commutator subgroup of the braid group. J.Discrete Math.. **189**(1-3):69-78. (2017)
22. You, W.Q., Chen X.M.,Qi,J.,Rui,S.S.: A Public-key Cryptography Base on Braid Group. In Proceedings of the International Conference on Computer, electronics and communication Engineering. pp: 566-569. (2017)
23. Goldwasser, S., Micali, S.: Probabilistic Encryption. J. Comput. Syst. **28**(2): 270-299. (1984)
24. Naor,M.,Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In Proceedings of the ACM Symposium on the Theory of Computing, pp. 427-437. (1990)
25. Dolev,D., Dwork, C., Naor, M.: Non-Malleable Cryptography. Proceedings of the 23 annual ACM Symposium on Theory of Computing, pp. 542-552. (1991)
26. Bellare, M., Rogaway,P.: Random oracles are practical: a paradigm for designing efficient protocols. In Proceedings of the 1st ACM Conference on Computer and Communication Security, pp. 62-73. ACM (1993)
27. Garside, F.A.: The braid group and other group. Q. J. MATH. **20**(1), 235-254. (1969)
28. Elrifai, E. A. and Morton, H. R.: Algorithms for positive braids. Quart. J. Math.Oxford **45**(180), 479C497. (1994)
29. Birman, J., Ko, K.H., Lee, S.J.: A new approach to the word and conjugacy problems in the braidgroups. Adv. Math. **139**, 322-353. (1998)
30. Birman,J., Ko,K.H., Lee, S.J.: The infimum, supremum, and geodesic length of a braid conjugacyclass. Adv. Math. **164**, 41C56. (2001)
31. You, W.Q., Chen X.M.,Qi,J.: Research on a kind of anti-quantum computing public key cryptosystem. Netinfo Security. **4**, 53-60 (2017)
32. Feder, E.: Algorithmic problems in the braid group. arXiv preprint arXiv:math/0305205 (2003)
33. Han, J.W., Ko,K.H.: Positive presentations of the braid groups and the embedding problem. Math. Z. **240**(1), 211-232. (2002) https://doi.org/10.1007/s002090100369
34. Elgamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. In Blakley G.R., Chaum D. (eds) CRYPTO 1984. LNCS, vol. 196, pp. 10-18. Springer, Heidelberg (1984). https://doi.org/10.1007/3-540-39568-7_2
35. Abdalla, M., Bellare, M., Rogaway, P.: The oracle Diffie-Hellman assumptions and an analysis of DHIES. In: Naccache, D. (ed.) CT-RSA 2001. LNCS, vol. 2020, pp.143-158. Springer, Heidelberg (2005). https://doi.org/10.1007/3-540-45353-9_12
36. Lichen, W.: Design and Analysis of Cryptographic Schemes Based on Braid Groups. PhD thesis, Shanghai Jiao Tong University. (2007)
37. Myasnkov, A., Shpilrain, V., Ushakov, A.: Non-commutative cryptography and complexity of group-theoretic problems. Providence, Rhode Island. (2011)
38. Vasco, M.I.G., Steinwandt, R.: Group Theoretic Cryptography. Chapman & Hall/CRC. (2015)
39. Cryptography And Groups (CRAG) C++ Library[EB/OL]. http://web.stevens.edu/algebraic/downloads.php (2017)

40. Bellare, M., Desai, A., Pointcheval, D., Rogaway, P.: Relations among notions of security for public-key encryption schemes. In: Krawczyk H. (eds) CRYPTO 1998. LNCS, vol. 1462, pp. 26-45. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055718
41. Fujisaki E., Okamoto T.: How to Enhance the Security of Public-Key Encryption at Minimum Cost. In: PKC 1999. LNCS, vol. 1560, pp. 53-68. Springer, Heidelberg. (1999)