The Twin Conjugacy Search Problem and Applications

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. We propose a new computational problem over the noncommutative group, called the twin conjugacy search problem. This problem is related to the conjugacy search problem and can be used for almost all of the same cryptographic constructions that are based on the conjugacy search problem. However, our new problem is at least as hard as the conjugacy search problem. Moreover, the twin conjugacy search problem has many applications. One of the most important applications, we propose a trapdoor test which can replace the function of the decision oracle. We also show other applications of the problem, including: a non-interactive key exchange protocol and a key exchange protocol, a new encryption scheme which is secure against chosen ciphertext attack, with a very simple and tight security proof and short ciphertexts, under a weak assumption, in the random oracle model.

Keywords: Twin conjugacy search problem, trap-door test, assumption, CCA, non-commutative group, crypto, Diffie-Hellman

1 Introduction

1.1 Background and related work

The conjugacy search problem is an important computational problem on noncommutative groups while it is also a widely used cryptographic primitive. In the context of quantum computing, Ko[1] first proposed a public key encryption system based on the conjugacy problem over the braid group, which greatly promoted the development of the group theoretic cryptography. It makes more and more scholars focus on the research of the conjugacy search problem and its public key cryptosystem and gets many excellent results[2,3,4,6,23]. Although the security of many cryptographic schemes on the braid group has been questioned[7,8,14], it is a good ideal that take the braid group as an instantiated object to study the non commutative group. The public key schemes based on non commutative groups have attracted increasing attention[9,10,12].

The rapid development of quantum computing technology has aggravated the threat to the existing public key cryptosystem[11,13]. However, the algorithm of resisting quantum attack is also constantly proposed. It may be an effective method to find the anti quantum attack algorithm on the non commutative group. As one of the difficult problems on the noncommutative group, the conjugacy search problem is very suitable for designing public key cryptosystems. In recent years, many good papers have been put forward[15,16,17].

Recently, inspired by David Cash et al. [18], we found that the conjugacy search problem has very similar with the Diffie-Hellman problem, due to space constraints, we must defer the details of the theory.

1.2 The Diffie-Hellman problem and the Conjugacy Search problem

To illustrate the similarities between Diffie-Hellman problem and conjugacy search problem more intuitively, we show that:

Hashed-ElGamal Encryption Scheme Based on Diffie-Hellman Problem.[20]

This public key encryption scheme makes use of a group G of prime order q with generator $g \in G$, a sysmmetric cipher (E, D), and a hash function H. Assume that K is a security parameter, the $GenKey_{DH}(K)$ is a key generator of this scheme. The secret key x is a random integer in Z_q, then the public key $X = g^x \mod q$ can be computed. For the sake of simplicity, the following procedure omits the operation: $\mod q$.

```
$\underline{KeyGen^{DH-hElG}(K):}$

    $(x, g, X) \leftarrow GenKey_{DH}(K);$
    $pk = (g, X), sk = x,$ where $X = g^x.$

$\underline{E_{pk}(m):}$ (the plaintext is $m$.)

    $y \leftarrow_R Z_q, Y = g^y, Z = X^y, k = H(Y, Z), c = E_k(m);$
    output $(Y, c)$.

$\underline{D_{sk}(Y, c):}$ (the ciphertext is $(Y, c)$)

    $Z = Y^x, k = H(Y, Z), m = D_k(c);$
    output $m$.
```

The ElGamal scheme[19] based on the Diffie-Hellman problem is a great discovery in public key cryptography. The research in this aspect is more mature than the ElGamal scheme based on the conjugacy search problem. For the sake of conciseness, we simplify the Hashed-ElGamal Encryption Scheme[20] to DH-hElG.

Hashed-ElGamal Encryption Scheme Based on Conjugacy Search Problem[5]

This public key encryption scheme makes use of a non commutative group B_{l+r} and two exchangeable subegroup LB_l, RB_r, a sysmmetric cipher (E, D), and a hash function H. Assume that K is a security parameter, the $GenKey_{CSP}(K)$ is a key generator of this scheme. The secret key x is a random element in LB_l, choose a sufficiently complicated element g in B_{l+r}, then the public key $X = xgx^{-1}$ can be computed.

```
$\underline{KeyGen^{CSP-hElG}(K):}$

    $(x, g, X) \leftarrow GenKey_{CSP}(K)$;
    $pk = (g, X), sk = x$, where $X = xgx^{-1}$.

$\underline{E_{pk}(m):}$

    $y \leftarrow_R RB_r, Y = ygy^{-1}, Z = yXy^{-1}, k = H(Y, Z), c = E_k(m)$;
    output $(Y, c)$.

$\underline{D_{sk}(Y, c):}$

    $Z = xYx^{-1}, k = H(Y, Z), m = D_k(c)$;
    output $m$.
```

With the appropriate modification of the algorithm proposed by Ko[1], we get the Hashed-ElGamal Encryption Scheme based on the conjugacy search problem and simplify it to CSP-hElGamal.

Formally, there are many similarities between DH-hElG and CSP-hElG, and the main difference lies in the computational characteristics of groups. David proposed a new computational problem called the twin Diffie-Hellman problem, and its applications[18], it has solved important problems on the security proofs of the Diffie-Hellman problem. Their results are very useful and amazing. Inspired by the work of David Cash et al.[18], we find some new properties of the conjugacy search problem on the noncommutative group.

1.3 Our result

In order to describe our work more succinctly, the braid group is used as the implementation group of this theory, but all of our results can be applied to any non commutative group, as long as two exchangeable subgroups are contained in the group and the conjugacy search problem is difficult over it. In this paper, for the first time, we define several security assumptions related to the conjugacy search problem, and analyze the security of the CSP-hElG scheme under each security assumptions. The main results are as follow:

1. We propose a new computation problem called the twin conjugacy search problem, and prove that it is at least as hard as the ordinary conjugacy search problem. In addition, the twin conjugacy search problem is hard, even given access to a corresponding decision oracle, assuming the ordinary conjugacy search problem (without any oracles) is hard.
2. We show a trapdoor test based on the twin conjugacy search problem, and it can simulate the function of a decision oracle.
3. A non-interactive key exchange protocol and a key exchange protocol based on the new problem are proposed, and we present a new public key encryption scheme which is secure against chosen ciphertext attack.

2 Preliminaries

Braid group is a typical non-commutative group, it is an important way that using braid group as an implementation tool to explore cryptography algorithm on non commutative group. There are many studies on the braid group and the theory of cryptography[21,22]. However, this paper only takes it as a implementation tool, and we no longer spend too much space on the braid group. At the same time, the reader does not have to fall into complex group theory. What we have to explain is:

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

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

Let LB_l be the left subgroup of B_n, and let RB_r be the right subgroup of B_n, the following algebraic operations need to be noted

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

Conjugacy search problem is a very important computational problem in non-commutative group. It is to be known that the problem is hard on the braid group[9,10]. Describe the following

Conjugacy Search Problem (CSP) $(g, X) \in B_n \times B_n,$, find $x \in B_n$ such that $X = xgx^{-1}$

Compared with other groups, braid group has richer connotations and algebraic properties. However, the braid group is not necessary for our theory, and it is just for the conciseness of the narrative. In fact, our theory can be extended to any noncommutative group as long as two exchangeable subgroups are contained in the group and the conjugacy search problem is difficult over it.

3 Security Assumptions

The security of public key cryptography rely on the security assumptions related to a difficult problem. Here are some security assumptions associated with the conjugate problem.

The Computional Conjugacy Search Assumption(The CCS Assumption): We assume that it is hard to compute Z, given the values X and Y in braid group B_{l+r}. Define $z := ccs(X, Y)$, where $X = xgx^{-1}, Y = ygy^{-1}, Z = xyg(xy)^{-1}$

Ko et al proposed a new public-key cryptosystem based on the braid group, we make some improvements to it, and name it as the conjugacy search encryption scheme(the CS encryption schme), that is, the CSP-hElG Scheme in the introduction.

The CS encryption scheme: (Enc,Dec) is a pair of symmetric key encryption algorithms while H is a hash function,$H : B_{l+r} \to \{0, 1\}^{l(k)}$, $l(k)$ is a security parameter. g is an element in B_{l+r}.

1. **KeyGeneration** Choose a random element x in LB_l, compute $X = xgx^{-1}$, then the public key is (X, g), while the private key is (x, g).
2. **Encryption** For cipher message $m \in B_{l+r}$, one chooses a random element y in RB_r, computes $Y = ygy^{-1}, Z = yXy^{-1}, k = H(Y, Z), c = Enc_k(m)$. The ciphertext is (Y, c).
3. **Decryption** Decipher gets the target ciphertext (Y, c), computes $Z = xYx^{-1}, k = H(Y, Z), m = Dec_k(c)$.

It has been proved that the CS encryption scheme is secure against chosen plaintext attack. However, the CCS assumption is not sufficient to establish the security of chosen ciphertext attack, even the H is a random oracle. To illustrate the problem, an adversary selects group elements $\hat{Y}, \hat{Z}$ randomly, to encrypt a message m, compute $\hat{k} = H(\hat{Y}, \hat{Z})$, and $\hat{c} = Enc_{\hat{k}}(\hat{m})$. Futher, assume that the adversary gives the ciphertext $\hat{Y}, \hat{c}$ to a decryption oracle obtaining the decryption m. It is easy to judge the equation $\hat{Z} \overset{?}{=} H(X, \hat{Y})$ through the equation $m \overset{?}{=} \hat{m}$. So, for random elements $\hat{Y}, \hat{Z}$, the adversary can answer $\hat{Z} \overset{?}{=} ccs(X, \hat{Y})$ through the decryption oracle. In general, the adversary would not be able to efficiently answer such questions of the form 'is $\hat{Z} \overset{?}{=} ccs(X, \hat{Y})$' on his own, and so the decryption oracle is leaking some information about that secret key x which could conceivably be used to break the encryption scheme[18].

In fact, when the adversary get a decryption oracle, what he need to do is compute $ccs(X, Y)$, after answering questions of the form $'is\ \hat{Z} \overset{?}{=} ccs(X, \hat{Y})'$ many times. Thus, we need a stronger assumption to ensure the security of Chosen-Ciphertext Attack(CCA).

The Strong CCS Assumption: We assume that it is hard to compute $css(X, Y)$, given random X, Y in B_{l+r}, along with access to a decision oracle for the predicate $ccsp(X, \cdot, \cdot)$, which on input $(\hat{Y}, \hat{Z})$, returns $ccsp(X, \hat{Y}, \hat{Z})$, define the predicate

$$ccsp(X, \hat{Y}, \hat{Z}) := ccs(X, \hat{Y}) \overset{?}{=} \hat{Z}$$

It is not difficult to prove that the CS encryption scheme is secure against chosen ciphertext attack when the H is modeled as a random oracle, under the strong CCS assumption and if the underlysing symmetric cipher (Enc, Dec) is itself secure against chosen ciphertext attack[5].

Compare to the CCS assumption, the Strong CCS assumption is too stronger. In genral, the weaker the assumption, the more secure the algorithm is, and the results are more rigorous. To get CCA security under the CCS assumption, we propose a new computational problem:

The Twin Conjugacy Search Problem(the twin CSP): $(g, X_1, X_2) \in B_n \times B_n \times B_n$, find $x_1, x_2 \in B_n$ such that $X_1 = x_1 g x_1^{-1}, X_1 = x_1 g x_1^{-1}$.

Like the CS encryption scheme, we propose a new encryption scheme based on the twin conjugacy search problem.

The Twin CS encryption scheme: (Enc,Dec) is a pair of symmetric key encryption algorithms while H is a hash function,$H : B_{l+r} \rightarrow \{0, 1\}^{l(k)}$, $l(k)$ is a security parameter. g is an element in B_{l+r}.

1. **KeyGeneration** Choose random elements x_1, x_2 in LB_l, compute $X_1 = x_1 g x_1^{-1}, X_2 = x_2 g x_2^{-1}$, then the public key is (X_1, X_2, g), while the private key is (x_1, x_2).
2. **Encryption** For cipher message $m \in B_{l+r}$, one chooses a random element y in RB_r, computes $Y = ygy^{-1}, Z_1 = yX_1y^{-1}, Z_2 = yX_2y^{-1}, k = H(Y, Z), c = Enc_k(m)$. The ciphertext is (Y, c).
3. **Decryption** Decipher gets the target ciphertext (Y, c), computes $Z_1 = x_1 Y x_1^{-1}, Z_2 = x_2 Y x_2^{-1}, k = H(Y, Z), m = Dec_k(c)$.

Like the conjugacy search problem, we present the security assumption related the twin conjugacy search problem.

The Twin Computational Conjugacy Search Assumption (The twin CCS assumption): Suppose that it is hard to compute Z_1, Z_2 in braid group B_{l+r}, given the values X_1, X_2, Y in braid group B_{l+r}. Define

$$(Z_1, Z_2) := 2ccs(X_1, X_2, Y) = (ccs(X_1, Y), ccs(X_2, Y))$$

where

$$X_1 = x_1 g x_1^{-1}, X_2 = x_2 g x_2^{-1}, Y = ygy^{-1}, Z_1 = (x_1 y) g (x_1 y)^{-1}, Z_2 = (x_2 y) g (x_2 y)^{-1}$$

In addition, we can present a stronger assumpution.

The Strong Twin Computational Conjugacy Search Assumption (The Strong Twin CCS assumption): Suppose that it is hard to compute $2ccs(X_1, X_2, Y)$, given the values X_1, X_2, Y in braid group B_{l+r}, along with access to a decision oracle for the predicate $ccsp(X_1, X_2, \cdot, \cdot, \cdot)$, which on input $\hat{Y}, \hat{Z}_1, \hat{Z}_2$, returns $2ccsp(X_1, X_2, \hat{Y}, \hat{Z}_1, \hat{Z}_2)$. Define the predicate

$$2ccsp(X_1, X_2, \hat{Y}, \hat{Z}_1, \hat{Z}_2) := (ccs(X_1, Y), ccs(X_2, Y)) = (Z_1, Z_2)$$

It's easy to know that the twin CS encryption scheme is secure against chosen ciphertext attack when the H is modeled as a random oracle, under the strong twin CCS assumption and if the underlysing symmetric cipher (Enc, Dec) is itself secure against chosen ciphertext attack.

Above all, we propose two encryption schemes and four kinds of security assumptions related to the conjugate problem over the braid group. Next we'll discuss the relationships of each assumption, and the security of the twin CS encryption scheme. One of our main results is the following:

Theorem 1. The CCS assumption holds if and only if the strong twin CCS assumption holds.

It is not hard to see that the twin strong CCS assumption implies the CCS assumption, while the non-trivial direction to prove is that the CCS assumption implies the strong twin CCS assumption. However, we need to defer the proof of Theorem 1 to save space.

4 A Trapdoor Test and a Proof of Theorem 1

In the following, we will propose another one of our results: trapdoor test theorem. Our theory is largely inspired by David[18]. David et al proposed the twin Diffie-Hellman problem and a trapdoor test over general cyclic group, their works are amazing, and it has greatly promoted the development of provable security theory. However, our theory is based on the conjugacy search problem over the non-commutative group. We emphasize

Lemma $\forall\ x, y \in B_n$, Remember xy^{-1} as $\frac{x}{y}$, $\forall r \in B_n$, then

$$r(\frac{x}{y})r^{-1} = \frac{rxr^{-1}}{ryr^{-1}}$$

proof :

$$\frac{rxr^{-1}}{ryr^{-1}} = rxr^{-1} \cdot (ryr^{-1}) = r(xy^{-1})r^{-1} = r\frac{x}{y}r^{-1}$$

Now, we propose the main theory:

Theorem 2 (Trapdoor Test). Let B_{l+r} be a braid group, RB_r and LB_l are right subgroup and left subgroup of the B_{l+r}, g is a random elemet on the group of B_{l+r}. Choose $X_1 \leftarrow_R B_{l+r},\ r \leftarrow_R LB_l,\ s \leftarrow RB_r$, define a random variable $X_2 = \frac{sgs^{-1}}{rX_1r^{-1}}$, if $\hat{Y}, \hat{Z}_1, \hat{Z}_2$ are random elements on the B_{l+r}. Then we have:

$(a.)$ X_2 is uniformly distributed over G;

$(b.)$ X_1 and X_2 are independent;

$(c.)$ if $X_1 = x_1gx_1^{-1}, X_2 = x_2gx_2^{-1}, x_1, x_2 \in LR_l$, then the probability that the truth value of

$$\hat{Z}_2 \cdot r\hat{Z}_1r^{-1} = s\hat{Y}s^{-1} \tag{1}$$

does not agree with the truth value of

$$\hat{Z}_1 = x_1\hat{Y}x^{-1} \wedge \hat{Z}_2 = x_2\hat{Y}x_2^{-1} \tag{2}$$

is negligible; moreover, if (3) holds, then (2) certainly holds.

proof: Observe that

$$X_2 = \frac{sgs^{-1}}{rX_1r^{-1}}$$

The elements s and r are randomly selected from RB_r and LB_l, respectively, and $X_1 \in B_{l+r}$. It is easy to verify that X_2 is uniformly distributed over B_{l+r}, and that X_1, X_2, r are mutually independent, from which $(a.)$ and $(b.)$ follow. To prove $(c.)$, condition on fixed values of X_1, X_2, suppose that $\hat{Y} = ygy^{-1}, y \in RB_r$. If (2) holds, because of

$$X_2 = \frac{sgs^{-1}}{rX_1r^{-1}}$$

then

$$yX_2y^{-1} = \frac{ysgs^{-1}y^{-1}}{yrX_1r^{-1}y^{-1}} = \frac{s\hat{Y}s^{-1}}{ryX_1y^{-1}r^{-1}}$$

That is,

$$s\hat{Y}s^{-1} = (yX_2y^{-1})(ryX_1y^{-1}r^{-1})$$

so

$$\begin{aligned}\hat{Z}_2 \cdot r\hat{Z}_1r^{-1} &= (x_2\hat{Y}x_2^{-1})r(x_1\hat{Y}x_1^{-1})r^{-1}\\ &= yX_2y^{-1}ryX_1y^{-1}r^{-1}\\ &= s\hat{Y}s^{-1}\end{aligned}$$

Thus, while (2) holds, (1) certainly holds. Conversely, if (2) does not hold, we show that (1) holds with a negligible probability. Observe that (1)

$$s\hat{Y}s^{-1} = yX_2y^{-1} \cdot (ryX_1y^{-1}r^{-1}) = \hat{Z}_2 \cdot r\hat{Z}_1r^{-1}$$

So

$$\hat{Z_2}^{-1} \cdot yX_2y^{-1} = \frac{r\hat{Z_1}r^{-1}}{ryX_1y^{-1}r^{-1}} = r\frac{\hat{Z_1}}{yX_1y^{-1}}r^{-1} \quad (3)$$

It is not hard to see, if $\hat{Z_1} = x_1\hat{Y}x_1^{-1}$ and $\hat{Z_2} \neq x_2\hat{Y}x_2^{-1}$, then (3) certainly does not hold. This leaves us with the case $\hat{Z_1} \neq x_1\hat{Y}x_1^{-1}$. But in the case, the right hand side of (3) is a random element of B_{l+r} since r is uniformly distributed over LB_l, but the left hand side is a fixed element of B_{l+r}. It is easy to see that the probability that selects an element from B_{l+r} to make it equal to a fixed element of B_{l+r} is negligible.

Now, we can prove the theorem 1 through the trapdoor test.

Theorem 1. The CCS assumption holds if and only if the strong twin CCS assumption holds.

Proof: The twin strong CCS assumption implies the CCS assumption obviously. To prove that the CCS assumption implies the strong twin CCS assumption. Let us define some terms:

Assume that an adversary B who attack the CCS assumption, an adversary A who attack the strong twin CCS assumption. B gets the challenge instance (X, Y) of the CCS assumption, the target is to compute $ccs(X, Y)$.

First, B chooses $r \leftarrow_R LB_l,\ s \leftarrow_R RB_r$, sets

$$X_1 = X,\ X_2 = \frac{sgs^{-1}}{rX_1r^{-1}}$$

and gives A the challenge instance (X_1, X_2, Y), A need to do to is compute $(Z_1, Z_2) = 2ccs(X_1, X_2, Y)$.

Second, A chooses $\hat{Y}, \hat{Z_1}, \hat{Z_2}$ to query B, then B processes each decision query $\hat{Y}, \hat{Z_1}, \hat{Z_2}$ by testing if $\hat{Z_2} \cdot r\hat{Z_1}r^{-1} = s\hat{Y}s^{-1}$ holds.

Finally, if and when A outputs (Z_1, Z_2), B tests if this output is correct by testing if $Z_2 \cdot rZ_1r^{-} = sYs^{-1}$ holds. If this does not hold, then B outputs "failure", otherwise, B outputs Z_1. The proof is easily completed using the trapdoor test.

5 Key Exchange Protocol

In the following we propose a new non-interactive key exchanege protocol based on the twin conjugacy search problem.

Non-interactive Key Exchange Protocol: Suppose that Alice and Bob are the two parties of the communication, g is a random element in braid group B_{l+r}. Alice's secret key is (x_1, x_2), $x_1, x_2 \in LB_l$ pulic key is (X_1, X_2), where $X_1 = x_1gx_1^{-1}, X_2 = x_2gx_2^{-1}$; Bob's secret key is (y_1, y_2), $y_1, y_2 \in RB_r$, public key is (Y_1, Y_2), where $Y_1 = y_1gy_1^{-1}, Y_2 = y_2gy_2^{-1}$. Keys which belong to Alice and Bob are authenticated by a trusted third party, they can share the key:

- Alice compute $x_1Y_1x_1^{-1}, x_1Y_2x_1^{-1}, x_2Y_1x_2^{-1}, x_2Y_2x_2^{-1}$
- Bob compute $y_1X_1y_1^{-1}, y_1X_2y_1^{-1}, y_2X_1y_2^{-1}, y_2X_2y_2^{-1}$

Because of $ccs(X_i, Y_j) = x_iY_jx_i^{-1} = y_jX_iy_j^{-1},\ i = 1, 2;\ j = 1, 2$, Alice and Bob can compute the same value through the same hash function H:

$$k = H(ccs(X_1, Y_1), ccs(X_1, Y_2), ccs(X_2, Y_1), ccs(X_2, Y_2))$$

Now we propose a new key agreement system:

Key Exchange Protocol: Assume that g is a random element in braid group B_{l+r}.

1. Alice chooses random secret elements $x_1, x_2 \in LB_l$ and sends (X_1, X_2) to Bob, where $X_1 = x_1gx_1^{-1}, X_2 = x_2gx_2^{-1}$;
2. Bob chooses random secret elements $y_1, y_2 \in LB_l$ and sends (Y_1, Y_2) to Bob, where $Y_1 = y_1gy_1^{-1}, Y_2 = y_2gy_2^{-1}$;
3. Alice receives X_1, X_2 and computes $x_1Y_1x_1^{-1}, x_1Y_2x_1^{-1}, x_2Y_1x_2^{-1}, x_2Y_2x_2^{-1}$;
4. Bob receives Y_1, Y_2 and computes $y_1X_1y_1^{-1}, y_1X_2y_1^{-1}, y_2X_1y_2^{-1}, y_2X_2y_2^{-1}$.

Because of $ccs(X_i, Y_j) = x_iY_jx_i^{-1} = y_jX_iy_j^{-1},\ i = 1, 2;\ j = 1, 2$, Alice and Bob can compute the same value through the same hash function H:

$$k = H(ccs(X_1, Y_1), ccs(X_1, Y_2), ccs(X_2, Y_1), ccs(X_2, Y_2))$$

6 Twin CCS-ElGamal Encryption

6.1 Security Model

The security model is portrayed by Indistinguishability-Game (IND-GAME), mainly divided into three levels: Indistinguishability-Chosen Plaintext Attack (IND-CPA) [24], Indistinguishability - (Non Adaptive) Chosen Ciphertext Attack (IND-CCA) [25], Indistinguishability - (Adaptive) Chosen Ciphertext Attack (IND-CCA2) [26]. We recall the definition for the CCA2.

Definition Indistinguishability - (Adaptive) Chosen Ciphertext Attack (IND-CCA2) [26] The IND game of public key encryption scheme under (Adaptive) chosen ciphertext attack (IND-CCA2) is as follows

1. Initialization. The Challenger B generates the password system, and the Adversary A obtains the system public key pk.
2. Training1. A sends the ciphertext C to the B, and B sends the decrypted plaintext to A.(Polynomial bounded)
3. 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.

4. Training2. A sends the ciphertext $C(C \neq C^*)$ to the B, and B sends the decrypted plaintext to A.(Polynomial bounded)
5. 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.

6.2 Security of the Twin CS Encryption Scheme

Theorem 3. Suppose that H is modeled as a random oracle, the twin CS encryption scheme is secure against Chosen Ciphertext Attack under the CCS assumption, and that the underlying symmetric cipher is itself secure against chosen ciphertext attack.

Proof: It is easy to see that the twin CS encryption scheme is secure against chosen ciphertext attack under the strong twin CCS assumption, and that the underlying symmetric cipher is itself secure against chosen ciphertext attack, H is modeled as a random oracle. However, according to theorem 1, the CCS assumption holds if and only if the strong twin CCS assumption holds. So, the twin CS encryption scheme is secure against Chosen Ciphertext Attack under the condition of the theorem 3.

7 Conclusion

In this work, we presented the twin conjugacy search problem and a trapdoor test. The trapdoor test is very useful and has many applications. In fact, our work would like to avoid making stronger assumptions, or working with specialized groups. All of the theory in this paper built in the braid group, however, our theory applies to any noncommutative group as long as the conjugacy search problem is hard over it. Compared to the original CSP-scheme, we make a little change in the process of the encryption.

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. 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.
3. Algebraic Eraser Digital Signature System, Provisional Patent, September, 2015.
4. Shpilrain, V., Ushakov, A.: Thompsons Group and Public Key Cryptography. In: Ioannidis J., Keromytis A., Yung M. (eds) ACNS 2005. LNCS, vol. 3531, pp. 151-163. Springer, Heidelberg. (2005) https://doi.org/10.1007/11496137_11
5. You, W.Q., Chen, X.M., Li, W.X.: Provably Secure Integration Cryptosystem on Non-Commutative Group. Cryptology ePrint Archive, Report 2018/512 (2018). https://eprint.iacr.org/2018/512
6. Burillo, J., Matucci, F., Ventura, E.: The conjugacy problem in extensions of Thompsons group *F*. Isr. J. Math. **216**(1), 15-59. (2016) https://doi.org/10.1007/s11856-016-1403-9
7. Yamamura A. : Security Analysis of Public Key Encryptions Based on Conjugacy Search Problem. In: Linawati, Mahendra M.S., Neuhold E.J., Tjoa A.M., You I. (eds) ICT-EurAsia 2014. LNCS, vol. 8407, pp. 554-563. Springer, Heidelberg. (2014)
8. 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)
9. Myasnkov, A., Shpilrain, V., Ushakov, A.: Non-commutative cryptography and complexity of group-theoretic problems. Providence, Rhode Island. (2011)
10. Vasco, M.I.G., Steinwandt, R.: Group Theoretic Cryptography. Chapman & Hall/CRC. (2015)
11. 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)
12. You, W.Q., Chen X.M.,et al.: Research on a mixed cryptosystem with perfect privacy. In Proceedings of IEEE 3rd Information Technology and Mechatronics Engineering Conference. pp. 966-970. (2017)
13. Proos, J., Zalka, C.: Shors Discrete Logarithm Quantum Algorithm for Elliptic Curves. Quantum Inf. Comput. **3**(4), 317-344. (2003)
14. 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)
15. Guo, F., Susilo, W., Mu, Y., Chen, R., Lai, J., Yang, G.: Iterated Random Oracle: A Universal Approach for Finding Loss in Security Reduction. In: Cheon, J., Takagi, T. (eds) ASIACRYPT 2016. ASIACRYPT 2016. LNCS, vol. 10032, pp. 745-776. Springer, Heidelberg. (2016) https://doi.org/10.1007/978-3-662-53890-6_25
16. Abe, M., Fuchsbauer, G., Groth, J. et al.: Structure-Preserving Signatures and Commitments to Group Elements. J.Cryptol. **29**(2), 363-421(2016). https://doi.org/10.1007/s00145-014-9196-7
17. Kaya, B.: The complexity of the topological conjugacy problem for Toeplitz subshifts. Isr. J. Math. **220**(2),873C897. (2017) https://doi.org/10.1007/s11856-017-1537-4
18. Cash D., Kiltz E., Shoup V. : The Twin Diffie-Hellman Problem and Applications. In: Smart N. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp.?127-145. Springer,Heidelberg. (2008) https://doi.org/10.1007/978-3-540-78967-3_8.
19. 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

20. 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
21. Garside, F.A.: The braid group and other group. Q. J. MATH. **20**(1), 235-254. (1969)
22. Artin, E.: Theory of braid. Annals of Math. **48**, 101-126. (1947)
23. You, W.Q., Chen X.M., et al.: A Public-key Cryptography Base on Braid Group. In Proceedings of the International Conference on Computer, electronics and communication Engineering. pp: 566-569. (2017)
24. Goldwasser, S., Micali, S.: Probabilistic Encryption. J. Comput. Syst. **28**(2): 270-299. (1984)
25. 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)
26. Dolev,D., Dwork, C., Naor, M.: Non-Malleable Cryptography. Proceedings of the 23 annual ACM Symposium on Theory of Computing, pp. 542-552. (1991)