ISSN 0304-9892 (Print) ISSN 2455-7463 (Online)
www.vijnanaparishadofindia.org/jnanabha
***Jñānābha*, Vol. 52(2) (2022), 218-223**
(Dedicated to Professor D. S. Hooda on His 80th Birth Anniversary Celebrations)

ALGEBRAIC BRAID GROUP PUBLIC KEY CRYPTOGRAPHY

Kamakhya Paul[1], Pinkimani Goswami[2] and Madan Mohan Singh[3]
[1]Department of Mathematics, North Eastern Hill University, Shillong-793022, Meghalaya, India
[2]Department of Mathematics, University of Science and Technology Meghalaya, Ri-Bhoi-793101, Meghalaya, India
[3]Department of Basic Sciences & Social Sciences, North Eastern Hill University, Shillong-793022, Meghalaya, India
Email: kamakhyapaul4@gmail.com, pinkimanigoswami@yahoo.com, mmsingh2004@gmail.com
(Received : October 12*,* 2022 *; In format : November* 02*,* 2022*; Revised: November* 14*,* 2022*; Accepted: November* 15*,* 2022*)*

DOI: https://doi.org/10.58250/jnanabha.2022.52225

Abstract

The braid group cryptography arises with the involvement of the braid group, which is an infinite non-commutative group arising from geometric braids. In this paper, we have proposed a new public key cryptosystem based on braid group. The security of our proposed scheme is based on two hard problems on braid group, conjugacy search problem and p-th root problem on braid group. We also checked the one-wayness, semantic security and efficiency of our proposed scheme, and found it to be computationally secured.
2020 Mathematical Sciences Classification: 94A60, 20F36
Keywords and Phrases: Public key cryptography, Braid group; Conjugacy search problem; p-th root problem.

1. Introduction

When two or more individuals want to share a piece of secret information over an insecure medium, it can be achieved by the means of an algorithmic method known as a public key cryptosystem. Diffie and Hellman[14] firstly introduced the concept of public key cryptography, also known as asymmetric cryptography in 1976. Following this, several asymmetric cryptosystems were developed based on various mathematically intractable problems such as Integer Factorization Problem (*IFP*), Discrete Logarithm Problem (*DLP*) etc.

With time, various contributions were made in public key cryptography involving numerous groups, rings and fields, and then also came the involvement of braid group in public key cryptography, which is an infinite non-commutative group arising from geometric braids. Philosophically speaking, as mentioned by Friedman [18], the identification of the exact moment of development for the first time of a mathematical theory is a rare case, we too are unaware of the exact moment of development of braid group, however some history is obviously explained about braid group. He has also examined the complete development of the braid theory from 1925 to 1950. As we all are aware that, Braid Group was firstly introduced by Artin [1] in his paper " Theorie der $Z\ddot{o}pfe$" in 1926, however, it should also be kept in mind that Hurwitz 1890s[18] did investigate braid. Artin's paper is considered the first introduction to braid because of his explicit way of studying braids [2, 3, 4, 27] which was to arithmetize braid group, i.e to present, with the tools of group theory, braid symbolically as well as the relations in the braid group and their deformations.

Despite the early discovery of the braid group, many mathematicians and physicists in the latter years paid an enormous amount of interest in the topic and many developments were made to it. Rolfsen [33] in one of his conferences spoke about new developments in the braid group and explained that the braid group can be defined in so many ways, mentioning it as many faces of the braid group and spoke about a few properties like representation, ordering and linearity [8, 9, 19, 26]. It's because of Anshel et al.[5] paper, where they gave a generalized method for the construction of key establishment protocol using computable monoids and functions which lead to the use of the non-abelian braid group in the development of new protocols. Note that a protocol is a multi-party algorithm proposed to obtain a detailed aim and a key establishment protocol is a protocol by which a piece of classified information is made to be known to two or more parties for succeeding cryptographic applications [29].

Ko et al.[25] mentioned in their paper the cryptographic importance of the braid group and specified its features for its use for cryptographic importance in three points. Their proposed scheme was based on the development of a trapdoor one-way function which was based on the hard problem, the Conjugacy search problem. Later in 2001, Anshel et al.[6] have described two key-exchange protocols based on braid group, whose security was based on the hard problem, conjugacy search problem. Moreover in past years, several studies were conducted on the braid group [12, 28] and numerous cryptosystems and signature schemes were also been developed based on braid group

[13, 15, 35] and several others with a belief that it can resist quantum attacks as mentioned by You et al. [37]. In the recent years Baev et al.[7] made a modification of Anshel-Anshel-Goldfeld algorithm.

Numerous cryptosystems [11, 21, 22, 23, 24, 32, 36] etc. were developed after McCurley[30], where two or more hard problems were merged to propose a more secured cryptosystem [34]. Recently Misra, Chaturvedi, Tripathi and Shukla [31] studied a unique key sharing protocol among three users using non-commutative group for electronic health record system. With this motivation we propose a new scheme based on two hard problems viz. conjugacy search problem and p-th root problem in the braid groups.

The rest of the paper is followed as, the description of the braid group along with some hard problems in the braid group are discussed in section 2. In section 3, we introduced a new trapdoor one-way function and proposed a new key exchange protocol and a public key cryptosystem. We conclude the paper in section 5.

2. Description to Braid Group

In this section, we will briefly describe the braid group and the hard problems in the braid group. Braid group is an infinite non-commutative group introduced by Artin. Birmans book[9] can be used as a general reference for braid theory and[10] can be used for the word problem and conjugacy problem.

Definition 2.1. *A braid on n strings is an object consisting of* 2*n points (n above and n below) and n strings such that:*

- *The beginning/ending points of the strings are (all of) the upper/lower points.*
- *The strings do not intersect.*
- *No string intersects any horizontal line more than once.*

The Artin Braid Group on n letters, B_n, is a finitely generated group with generators $\sigma_1, \sigma_2, \sigma_3, \cdots, \sigma_{(n-1)}$ which satisfy the following relations:

- $\sigma_i\sigma_j = \sigma_j\sigma_i$, when $|i - j| \geq 2$ for $i, j \in \{1, 2, 3, \cdots, (n-1)\}$,
- $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ for $i \in \{1, 2, 3, \cdots, (n-2)\}$.

These relations are referred to as the braid relations. The element n is called the *braid index*, and any element of B_n is called a $n-$braid. The braid index is the number of strings. Two braids are equivalent if one can be deformed to the other continuously in the set of braids. B_1 is trivial by definition. For all other n, B_n is infinite. B_2 is isomorphic to $\mathbb{Z}$. Now, there exists an obvious surjective group homomorphism $\pi : B_n \to S_n$, group of n-permutation called the symmetric group, simply defined by following the strands in a geometric sense and analysing their underlying permutations. Alternatively, one may write this in terms of algebraic generators by letting $\pi(\sigma_i) = \pi(\sigma_i^{-1}) = (i; i+1)$ for all $i \in \{1, 2, 3, ...(n-1)\}$. Hence, given that the symmetric group is non commutative for $n \geq 3$, so the braid group is also non commutative for $n \geq 3$. The kernel of the homomorphism between the braid group and the symmetric group is referred to as the pure braid group P_n.

2.1. Hard problems in Braid Group

Below are described two hard problems in braid group out of all mentioned by Ko et al. [25] in their paper which are mathematically hard to solve and have some interesting contribution to cryptography.

- Conjugacy Search Problem
  Instance : $(x, y) \in B_n \times B_n$ such that x and y are conjugates.
  Objective : Find $a \in B_n$ such that $y = axa^{-1}$.
- p - th Root Test
  Instance: $(y, p) \in B_n \times \mathbb{Z}$ such that $y = x^p$ for some $x \in B_n$.
  Objective: Find $z \in B_n$ such that $y = z^p$.

2.2. Proposed One-Way function

For any $e \in \mathbb{Z}$ we define an one-way function,

$$f_e : LB_l \times B_{l+r} \to B_{l+r} \times B_{l+r}$$
$$\text{as } f_e(a, x) = (a^e x a^{-e}, x).$$

The function f_e is an one-way function as for a given (a, x), it is easy to compute $a^e x a^{-e}$; however, to compute a from the given $(a^e x a^{-e}, x)$, one has to firstly compute a^e, which is the generalized conjugacy search problem and then one has to compute a from a^e, which is the e^{th} root problem.

2.3. Key Exchange protocol

Preparation Step

An appropriate pair of integers (l, r), such that LB_l and RB_r commutes, and a sufficiently complicated $(l + r)$-braid $x \in B_{l+r}$ are selected and published. Also an integer e is chosen and published.

Key Agreement

To share the secret key Alice and Bob has to perform the following steps:

(a) Alice chooses a random braid $a \in LB_l$ and sends $y = a^e x a^{-e}$ to Bob,
(b) Bob chooses a random $b \in RB_r$ and sends $z = b^e x b^{-e}$ to Alice,
(c) Alice receives z and compute $k = a^e z a^{-e}$,
(d) Bob receives y and compute $k = b^e y b^{-e}$.

Here $a^e z a^{-e} = a^e(b^e x b^{-e})a^{-e} = a^e b^e x b^{-e} a^{-e} = a^e b^e x a^{-e} b^{-e}$ and $b^e y b^{-e} = b^e(a^e x a^{-e})b^{-e} = b^e a^e x a^{-e} b^{-e} = a^e b^e x a^{-e} b^{-e}$. So $a^e z a^{-e} = b^e y b^{-e}$, which is the shared key.

2.4. Proposed Public Key Cryptosystem

Let $H : B_{l+r} \to \{0,1\}^k$ be an ideal hash function from the braid group to the message space.

Key Generation

- Choose a sufficiently complicated $(l + r)-$braid $x \in B_{(l+r)}$.
- Choose an integer $e \geq 2$.
- Choose a braid $a \in LB_l$.
- ***PUBLIC KEY***: (x, y), where $y = a^e x a^{-e}$.
- ***PRIVATE KEY***: a.

Encryption

Given a message $m \in \{0,1\}^k$.

- Choose a braid $b \in RB_r$ at random.
- Compute $c = b^e x b^{-e}$ and $d = H(b^e y b^{-e}) \oplus m$.
- Ciphertext is (c, d).

Decryption

Given the ciphertext (c, d) and for the private key a,

- Compute $H(a^e c a^{-e}) \oplus d = m$.

Verification

Here $a^e c a^{-e} = a^e b^e x b^{-e} a^{-e} = b^e y b^{-e}$.
So, $H(a^e c a^{-e}) \oplus d = H(a^e c a^{-e}) \oplus H(b^e y b^{-e}) \oplus m = m$.

3. Security of the proposed Public Key Cryptosystem

As solving any base problem of a public key cryptosystem is computationally hard, our cryptosystem is also based on two hard problem, and hence it is computationally secure. Here decrypting the ciphertext (c, d), where $c = b^e x b^{-e}$ and $d = H(b^e y b^{-e}) \oplus m$ equivalent to solving $b^e y b^{-e}$, i.e $b^e a^e x a^{-e} b^{-e}$. Also, for two different messages m_1 and m_2, different values of b is to be selected. Suppose if for same b, two messages m_1 and m_2 are generated with corresponding ciphertext (c_1, d_1) and (c_2, d_2), then message m_2 is definitely computable from (m_1, d_1, d_2) because $H(b^e y b^{-e}) = m_1 \oplus d_1 = m_2 \oplus d_2$.

A mathematical solution to conjugacy search problem was given by few authors in [16, 17, 20]. However, the known algorithms can help us find an element $a \in B_{l+r}$ and not in LB_l. Hence our proposed cryptosystem is defensive against this known algorithms.

One-wayness

In this section we check the one-wayness of our proposed cryptosystem.

Theorem 3.1. *Our proposed cryptosystem is one-way secured if and only if both conjugacy search problem and p-th root problem holds. Proof. Let us suppose that both conjugacy search problem and p-th root problem is easy i.e., given two conjugates x and y, the value of a can be easily found and also if $y = x^p$, for some p in braid group, then we can easily find a z such that $y = z^p$, which means that, there exists a PPT algorithm $\mathcal{A}$ which can solve both conjugacy search problem and p-th root problem. Our motive is to break the one-wayness of our proposed scheme by using the algorithm $\mathcal{A}$ and hence recover the plain text message m.*

Let the challenge ciphertext be (c, d), where $c = p^e x(p^{-1})^e$ and $d = H(b^e y(b^{-1})^e) \oplus m$ and the public key be (x, y), where $x \in B_{l+r}$ and $y = a^e x(a^{-1})^e$. Now, we start obtaining the value of m. Let $X = c = p^e x(p^{-1})^e$ and $Y = y$. Then the algorithm $\mathcal{A}$ can calculate $Z = H(p^e y(p^{-1})^e) = H(a^e y(a^{-1})^e)$ and hence from $d = H(b^e y(b^{-1})^e) \oplus m$, one can obtain $m = H(p^e y(p^{-1})^e) \oplus d$.

Conversely, let us assume that our proposed scheme is not one-way. Then, for a given ciphertext, there do exist a PPT algorithm $\mathcal{A}$ such that $\mathcal{A}$ can recover the original plaintext with non-negligible probability.
Let $X = q^e x(q^{-1})^e$ and $Y = H(q^e y(q^{-1})^e) \oplus m$. And our motive is to obtain the value $Z = H(q^e y(q^{-1})^e)$ with the support of the algorithm $\mathcal{A}$. Here, the public key of the proposed scheme is (x, y), where $x \in B_{l+r}$ and $y = a^e x(a^{-1})^e$ and set

$X = c = q^e x(q^{-1})^e$ and $Y = d = H(q^e y(q^{-1})^e) \oplus m$, and send (c, d) to $\mathcal{A}$. Suppose $\mathcal{A}$ respond the message m' for (c, d). Then by definition $d = H(q^e y(q^{-1})^e) \oplus m' \implies H(q^e y(q^{-1})^e) = d \oplus m'$.
And hence, one can compute $Z = H(q^e y(q^{-1})^e)$.

Semantic security
In this section we check the semantic security of our proposed cryptosystem. In semantic security the challenger generates the public key and the private key, *pk* and *sk* respectively. Keeps the private key to himself/herself and sends the public key to the adversary. Next the adversary selects two distinct messages m_0 and $m_1 \in M$ of same length and send it to the challenger. Here, the challenger selects any one of m_0 or m_1 and encrypts the corresponding ciphertext to it and send it to the adversary. On receiving the ciphertext from the challenger, the adversary objective is to identify which message was encrypted. If it can be achieved then the encryption scheme is not semantically secured else not, then semantically secured.

Conjugacy Search Assumption
Under the Conjugacy Search Assumption, we assume that it is computationally hard to obtain the value of Z, given the value of X and Y in Braid group B_{l+r}. Where $X = axa^{-1}$, $Y = byb^{-1}$ and $Z = (ab)x(ab)^{-1}$.

Decisional Conjugacy Search Assumption
The Decisional Conjugacy Search Assumption states that, given the value of X and Y in braid group B_{l+r}, the value Z looks like a random element in B_{l+r}. Where $X = axa^{-1}$, $Y = byb^{-1}$ and $Z = (ab)x(ab)^{-1}$.

Theorem 3.2. *If Decisional Conjugacy Search Assumption holds, then the scheme presented in section 3, is semantically secured. Proof. Let us presume that the scheme proposed in section 3 is not semantically secured for the purpose of contradiction. Which speaks about the existence of a polynomial time algorithm $\mathcal{A}$, which can break the semantic security of our proposed scheme. With this, our objective is that to, given $\mathcal{G} = (X, Y, Z)$, with the help of algorithm $\mathcal{A}$, it is to decide whether it is conjugacy search problem of a random one (i.e $p = ab$ or not). Where $X = axa^{-1}$, $Y = byb^{-1}$ and $Z = (ab)x(ab)^{-1}$. We first set the public key (x, y), where $y = a^e x(a^{-1})^e$; then once the adversary has chosen the messages m_0 and m_1, we overturn a bit q and we encrypt m_q as follows: $E(m_q) = (c, d)$ where $c = b^e x(b^{-1})^e$ and $d = H(p^e y(p^{-1})^e) \oplus m_q$.*

Seemingly if $\mathcal{G}$ is a conjugacy search assumption, the above is an authentic encryption of m_q and algorithm $\mathcal{A}$ will deliver the accurate output with non negligible gain. On the contrary, if $\mathcal{G}$ is not a conjugacy search assumption, we assert that even a polynomially unbounded adversary gains no information about m_q from $E(m_q)$ in a strong information-theoretic sense.

Let $p = abr$, and then the information received by the adversary is of the form $c = b^e x(b^{-1})^e$ and $d = H((abr)^e y((abr)^{-1})^e) \oplus m_q$. And then we see the value of d as $d = H((abr)^e y((abr)^{-1})^e) \oplus m_q = H(a^e b^e r^e y r^{-e} b^{-e} a^{-e}) \oplus m_q = H(a^e b^e z b^{-e} a^{-e}) \oplus m_q$, where $z = r^e y r^{-e}$. Hence $d = H((ab)^e z(ab)^{-e}) \oplus m_q$, where a small change brings a drastic change in the hash value and finally makes the value of m_q infeasible which is completely hidden in d. And thus $\mathcal{A}$ cannot guess q better than at random.

4. Efficiency of the proposed *PKC*

Suppose that the braid indexes of the proposed scheme are $l = r = n/2$ and the canonical length are $len(x) = len(a) = len(b) = p$. Then

1. A braid with p canonical factors can be represented by a bit string of size $pn \log n$.
2. For a braid $y_1, y_2 \in B_n$, $len(y_1, y_2) \leq len(y_1) + len(y_2)$. For a braid $y_1 \in LB_l$, $y_2 \in RB_r$, $len(y_1, y_2) = max\{len(y_1), len(y_2)\}$. And hence for a braid $y_1 \in B_n$ and $e \in \mathbb{Z}$, $len(y_1^e) \leq len(y_1) + len(y_1) + len(y_1) + \cdots + len(y_1)$ (e times). So $len(a^e x a^{-e})$ and $len(a^e b^e x a^{-e} b^{-e})$ are at most $3p$.

In encryption, one random braid generations, two multiplication and one left canonical form operation are involved. Again, in decryption, two multiplication and one left canonical form operation are involved. Thus, both operations have running time at most $O(p^2 n \log n)$, which is almost similar with [25].

5. Conclusion

In this paper, we have proposed a new one-way function. Based on this one-way function, we proposed a secret sharing scheme and a public key cryptosystem. Our proposed cryptosystem is being developed based on two hard problems, conjugacy search problem and p - th root problem on the braid group. After the proposition of our scheme, we looked into the security of our scheme and found it to be computationally secured against an adversary of possible threats. We also checked the one-wayness, semantic security of the proposed scheme. We also discussed the efficiency of the proposed public key cryptosystem and found it's efficiency is almost similar to the scheme proposed in [25].

Acknowledgment
The authors are very much thankful to the Editor and the anonymous reviewer for their valuable suggestions to bring the paper in its present form.

References

[1] E. Artin, Theorie der Zöpfe, *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, **4** (1926), 47-72.
[2] E. Artin, Theory of braids, *The Annals of Mathematics*, **48** (1947a), 101-126.
[3] E. Artin, Braids and permutations, *Annals of Mathematics, Second Series*, **48** (1947b), 643-649.
[4] E. Artin, The theory of braids, *American Scientist*, **38**(1) (1950), 112-119.
[5] I. Anshel, M. Anshel and D. Goldfeld, An algebraic method for public-key cryptography, *Mathematical research letters*, **3** (1999), 287-291.
[6] I. Anshel, M. Anshel, B. Fisher and D. Goldfeld, New key agreement protocols in braid group cryptography, *In Cryptographers Track at the RSA Conference*,**2001**, (2001), 13-27.
[7] D.A. Baev, L.V. Cherckesova, O.A. Safaryan, V.O. Kravchenko and P. V. Razumov, Modification of Anshel-Anshel-Goldfeld Postquantum algorithm/Protocol based on algebraic braid groups, in order to span-cyberattack neutralization, *In Journal of Physics: Conference Series*, **2131**(2) (2021), 022-079.
[8] G. Burde, H. Zieschang and M. Heusener, *Knots*, de Gruyter, 1985.
[9] J.S. Birman , Braids, links and mapping class groups, *Princeton University Press*, **82**, 1974.
[10] J.S. Birman, K.H. Ko and S.J. Lee, A new approach to the word and conjugacy problems in the braid groups, *Advances in Mathematics*, **139** (1998), 322-353.
[11] K. Paul, M.M. Singh and P. Goswami, A new public key encryption using Dickson polynomials over finite field with 2^m, *Nonlinear Dynamics and Applications*, Springer, Cham, (2022), 555-563.
[12] M. Cumplido, D. Kahrobaei and M. Noce, The root extraction problem in braid group-based cryptography, *arXiv preprint*, (2022), arXiv:2203.15898.
[13] X. Chen, W. You, M. Jiao, K. Zhang, S. Qing and Z. Wang, A cryptosystem based on positive braids, Ubiquitous Intelligence & Computing,Advanced & trusted computing, Scalable computing & communications, Cloud & big data computing, *Internet of people and smart city innovations*, 2018 *IEEE smartWorld*, (2018), 1260-1264.
[14] W. Diffie and M. Hellman, New Directions in Cryptography, (IEEE Transactions on Information Theory), **22**(6) (1976), 644-654.
[15] Y. Ding, J. Chen and Z. Peng, Digital signature method based on braid groups conjugacy and verify method thereof, *United States patent US* **7**, (May 25 2010), 725,724.
[16] D.B.A. Epstein, Word processing in groups, *AK Peters/CRC Press*, 1992.
[17] E.A. Elrifai and H.R. Morton, Algorithms for positive braids, *The Quarterly Journal of Mathematics*, **45**(4) (1994), 479-497.
[18] M. Friedman , Mathematical formalization and diagrammatic reasoning: the case study of the braid group between 1925 and 1950, *British journal for the History of Mathematics*, **34**(1) (2019), 43-59.
[19] R. Fenn, An elementary introduction to the theory of braids, *Notes by Bernd Gemein, available at the author's website*, 1999.
[20] F.A. Garside, The braid group and other groups, *The Quarterly Journal of Mathematics*, **20**(1) (1969), 235-54.
[21] P. Goswami, M.M. Singh and B. Bhuyan, A new public key cryptosystem over $\mathbf{Z}_{n^2}^*$, *Discrete Mathematics, Algorithms and Applications*, **9**(1750080) (2017), 1-11.
[22] P. Goswami, M.M. Singh and B. Bhuyan, A new public key encryption scheme based on two cryptographic assumptions, *Malaya Journal of Matematik (MJM)*, **3** (2015), 419422.
[23] P. Goswami, M.M. Singh and B. Bhuyan, A new public key scheme based on DRSA and generalized GDLP, *Discrete Mathematics, Algorithms and Applications*, **8**(4) (2016), 17.
[24] P. Goswami, M.M. Singh and B. Bhuyan, A new public key scheme based on integer factorization and discrete logarithm, *Palestine Journal of Mathematics*, **6**(2) (2017), 580584.
[25] K.H. Ko, S.J. Lee, J.H. Cheon, J.W. Han, J. Kang and C. Park, New public-key cryptosystem using braid groups, *Advances in Cryptology CRYPTO*, **2000**, (2000), 166-183.
[26] L.H. Kauffman, Knots and physics, *World Scientific*, 1991.
[27] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48**(177) (1987), 203-209.
[28] T.C. Lin, A study of non-abelian public key cryptography, *International Journal of network security*, **20**(2) (2018), 278-90.

[29] A.J. Menezes, P.C. Van Oorschot and S.A. Vanstone, Handbook of applied cryptography, *CRC Press series on Discrete Mathematics and its applications*, CRC Press, Boca Raton, FL, 1997.
[30] K.S. McCurley, A key Distribution system Equivalent to Factoring, *Journal of Cryptology*, **1** (1988), 95-105.
[31] M.K. Misra, A. Chaturvedi, S.P. Tripathi and V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, *Journal of Discrete Mathematical Sciences and Cryptography*, **22**(8) (2019), 1435-1451.
[32] D. Poulakis, A public key encryption scheme based on factoring and discrete logarithm, *Journal of Discrete Mathematical Sciences and Cryptography*, **12**(6) (2009), 745-752.
[33] D. Rolfsen, New developments in the theory of Artin's braid groups, *Topology and its Applications*, **127**(1-2) (2003), 77-90.
[34] P. Sarde and A. Banerjee, A secure and efficient designated verifier group signature scheme over braid group, *International journal of computer science and telecommunications*, **2**(4) (2011), 459-461.
[35] L. Wang, Y. Tian, Y. Pan and Y. Yang , New construction of blind signatures from braid groups, *IEEE Access*, **7** (2019), 36549-36557.
[36] W. Wei, T. Van Trung, S. Magliveras and F. Hoffman, Cryptographic primitives based on groups of hidden order, *Tatra Mountains Mathematical Publications*, **29** (2004), 147-155.
[37] W.Q. You,X .M. Chen, J. Qi and S.S. Rui, A public key cryptosystem based on braids group, *International conference on computer, electronics and communication engineering*, (2017), 566-569.