


# Cryptanalysis of Post-Quantum Signature Scheme based on the root extraction problem over braid group

Djimnaibeye Sidoine  
*dept. computer science*  
*INSTQ*  
Abeche, Chad  
dthekplus@gmail.com 

Guy Mobouale Wamba  
*dept. Mathematics and Computer Science*  
*UCAD*  
Dakar, Senegal  
wambastonn@gmail.com

Abiodoun Clement Hounkpevi  
*dept. Mathematics and Computer Science*  
*UCAD*  
Dakar, Senegal  
abiodounkpevi@gmail.com

Tieudjo Daniel  
*dept. Mathematics and Computer Science*  
*Ngaoundere University*  
Ngaoundere, Cameroun  
tieudjo@yahoo.fr

Djiby Sow  
*dept. Mathematics and Computer Science*  
*UCAD*  
Dakar, Senegal  
djiby.sow@ucad.edu.sn

**Abstract**—Cumplido, María and al. have recently shown that the Wang-Hu digital signature is not secure and has presented a potential attack on the root extraction problem. The effectiveness of generic attacks on solving this problem for braids is still uncertain and it is unknown if it is possible to create braids that require exponential time to solve these problems. In 2023, Lin and al. has proposed a post-quantum signature scheme similar to the Wang-Hu scheme that is proven to be able to withstand attacks from quantum computers [1]. This paper presents evidence of an algorithm that uses mean-set attacks to obtain the private key in two different schemes, without having to solve the root extraction problem. Additionally, in the post-quantum signature version, we demonstrate that an attacker can forge a signature that will pass verification without actually recovering the private key.

**Index Terms**—Cryptanalysis, Braid Group-based Cryptography, Signature Scheme, Mean-set Attack, post-quantum cryptography

## I. INTRODUCTION

Artin's braid groups [2] are infinite non-commutative groups in which the word problem is solvable, while the conjugation search problem and the root extraction problem (REP) have an exponential computational complexity, at least in the worst case. This makes braid groups an appropriate platform and the conjugation search problem a reasonable basis for designing cryptographic schemes. Patrick Dehornoy introduced a new method for comparing braid words that utilizes the automatic structure of braid groups and a linear ordering on braids. This algorithm is a generalization of classical words reduction in free groups and is more effective than existing methods [3]. In the past decade, there has been significant research and development in braid-based cryptography, focussing

on both cryptographic [1], [2], [4]–[7] and cryptanalytic aspects [8]–[13].

In their paper [7], Wang and al. discuss the weaknesses of public-key cryptographic algorithms based on the conjugation search and root extraction problems over braid groups. It proposes a digital signature scheme called the Wang-Hu scheme that is based on the root extraction problem and addresses these security drawbacks. The scheme proves that forging a signature requires solving an intractable problem, the group factorisation problem. Additionally, it highlights that reconstructing braid equations regarding the keys provides the attacker with limited useful information. Performance analysis proves that the proposed scheme is efficient and practical, with computational overhead comparable to modular RSA multiplications.

Recently, Cumplido, Mara, and al. prove that the Wang-Hu digital signature is not secure by presenting a possible attack (solving the root extraction problem) with some conditions on the parameters [14]. The effectiveness of generic attacks in solving the root extraction problem and the braid subgroup conjugacy search problem remains uncertain. It is still unknown if a method can be developed to create braids that would require an exponential time to solve these problems.

Recently, the article [1] introduced an isomorphism that relates the Mihailova subgroup of  $F_2 \times F_2$  to the Mihailova subgroups of a braid group. This allows for an explicit presentation of the Mihailova subgroups in the braid group. The paper also discusses the unsolvable subgroup membership problem that some Mihailova subgroups in the braid group face. On the basis of these findings, the authors propose a post-quantum signature scheme like the Wang-Hu scheme, which is shown to be resistant to quantum computational attacks.

Mosina and al. [15] presents a concept called the mean set of random group variables and applies it to the cryptanalysis of authentication scheme [12]. This attack, known as the mean-set attack, utilises the generalised Strong Law of Large Numbers (SLLN) to analyse groups represented as graphs. The article [13] significantly enhances the proposed attack, conclusively validating the results achieved by Mosina and Ushakov, while also significantly reducing the time required for the process.

Here, we kindly present evidence that supports the existence of a mean-set attack-based polynomial-time algorithm that enables the recovery of the private key in both schemes without solving the root extraction problem. For both schemas, the attacker can launch a chosen-message attack. He/She can send a set of messages  $m_1, \dots, m_l$  to the user and the corresponding signatures  $(v_1, t_1 = s_1 r^{-1}), \dots, (v_l, t_l = s_l r^{-1})$ . With the shift property  $\mathbb{E}(\xi r^{-1}) = \mathbb{E}(\xi) r^{-1}$ , the proposition  $\lim_{k \rightarrow \infty} \mathbb{S}_l(\xi_1, \dots, \xi_l) = e$ , where  $e$  is the trivial braid in  $B_n$ , we have the generalisation of the SLLN for groups in the sense that  $\mathbb{S}_l(\xi_1 r^{-1}, \dots, \xi_l r^{-1}) = \mathbb{S}_l(\xi_1, \dots, \xi_l) r^{-1}$  converges to  $r^{-1}$  when  $l \rightarrow \infty$ , with probability 1.

The results also show that in the post-quantum signature scheme, it is possible for an attacker to forge a signature without the need to recover the private key.

The document is organized as follows. In Section 2, we introduce the braid groups and Mihailova Subgroups. And we also describe the Strong Law of Large Numbers (SLLN) on the group. In Section 3, we present two signature schemes that are built upon the root extraction problem over braid group. In Section 4, we proudly present the cryptanalysis of two signature schemes.

## II. PRELIMINARIES

### A. Braid groups and Mihailova Subgroups

In this section, we give the basic definitions of braid groups and discuss some hard problems in those groups. For more information on braid groups, word problem and conjugacy problems, refer to the papers [1, 4, 5, 8, 9, 10]. The braid group on  $n$  strands  $B_n$  is the abstract group generated by  $\sigma_i$ , for  $i = 1, 2, \dots, n-1$ , with the following relations:

- 1)  $\sigma_i \sigma_j = \sigma_j \sigma_i$  for  $|i - j| \geq 2$
- 2)  $\sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}$  for  $i = 1, 2, \dots, n-1$

where  $(\sigma_1, \dots, \sigma_{n-1})$  are called the Artin generators of  $B_n$ , and the elements of  $B_n$  are called braids.

The hard problems of the braid group, such as conjugation and root extraction, are key to constructing a cryptographic system using braid groups.

**Conjugacy Decision Problem:** Given  $p, p' \in B_n$ , determine in a finite time whether  $p$  is conjugate to  $p'$ , i.e., if there exists  $x \in B_n$  such that  $p = x^{-1} p' x$ .

**Conjugacy Search Problem:** Given  $p, p' \in B_n$  where  $p$  is conjugate to  $p'$ , find in a finite time  $x \in B_n$  such that  $p = x^{-1} p' x$ .

**Root Extraction Decision Problem:** Given a braid group  $B_n$ , an element  $x \in B_n$ , and an integer  $e \geq 2$ , determine if there exists a braid  $z$  such that  $z^e = x$ .

**Root Extraction Search Problem:** Given a braid group  $B_n$ , an element  $x \in B_n$ , and an integer  $e \geq 2$ , find an algorithm that can determine, in a finite time, a braid  $Z$  satisfying  $Z^e = x$ .

They contain large subgroups such that each element of the first subgroup commutes with each element of the second. Indeed, braids involving disjoint sets of strands commute. So, if we denote by  $B_{n_1}$  (resp.  $B_{n_2}$ ) the subgroup of  $B_n$  generated by  $\sigma_1, \dots, \sigma_{m-1}$  (resp.  $\sigma_{m+1}, \dots, \sigma_{n-1}$ ) with  $m = n/2$ , every braid in  $B_{n_1}$  commutes with every braid in  $B_{n_2}$ .

1) **Normal form:** From a braid  $\beta$ , we construct a particular word that represents it. This is the normal form of  $\beta$ .  $\beta$  represents a trivial braid if and only if its normal form  $w_0$  is the normal word representing the trivial braid. Every braid in  $B_n$  has a unique expression of the form  $\Delta_n^p[\pi_1] \dots [\pi_d]$  such that  $[\pi_1]$  is not a permutation  $(n, \dots, 1)$ , and  $\pi_d$  is not the identity, and for each  $r$ , we have  $\pi_r(i) > \pi_r(i+1)$  whenever  $\pi_{r+1}^{-1}(i) > \pi_{r+1}^{-1}(i+1)$ . The expression  $\Delta_n^p[\pi_1] \dots [\pi_d]$  is the normal form.

2) **Handle Reduction:** A braid word is trivial if and only if, after handle reduction, we obtain the empty word. Handle reduction method is much more efficient in practice. We say that a braid word  $v$  is  $\sigma_i$ -handle if it is of the form  $\sigma_i^e u \sigma_i^{-e}$ , where  $u$  contains no letters  $\sigma_j^{\pm e}$  with  $j \geq i$ , and contains at most one of the letters  $\sigma_{i-1}$  and  $\sigma_{i-1}^{-1}$ . We define the reduction of  $v$  as the word  $red(v)$  obtained from  $v$  by:

- removing the letters  $\sigma_i$  and  $\sigma_i^{-1}$
- replacing each letter  $\sigma_{i-1}^{\pm 1}$  by  $\sigma_{i-1}^{-e} \sigma_i^{\pm 1} \sigma_{i-1}^e$ .

**[Mihailova subgroup [16]]** Let  $F_2$  be the free group on two generators  $x$  and  $y$ , and let  $F_2 \times F_2$  be the direct product of  $F_2$  with itself. The Mihailova subgroup of  $F_2 \times F_2$  is the set of pairs  $(w_1, w_2)$  such that  $w_1$  and  $w_2$  are equal in  $F_2$  modulo the commutator subgroup  $[F_2, F_2]$ . That is,

$$M(F_2 \times F_2) = \{(w_1, w_2) \in F_2 \times F_2 \mid w_1 [F_2, F_2] = w_2 [F_2, F_2]\}.$$

Now let  $B_n$  be the braid group on  $n$  strands, and let  $\pi : B_n \rightarrow S_n$  be the natural homomorphism to the symmetric group  $S_n$ . For any subgroup  $H$  of  $S_n$ , the Mihailova subgroup of  $B_n$  corresponding to  $H$  is the set of braids  $v$  such that  $\pi(v)$  belongs to  $H$ . That is,

$$M(B_n, H) = \{v \in B_n \mid \pi(v) \in H\}.$$

For example, it is known that: The Mihailova subgroups of  $B_n$  correspond to the symmetric groups  $S_n$  and  $S_{n-1}$  are both trivial. The Mihailova subgroup of  $B_n$  corresponding to the cyclic group  $C_n$  is isomorphic to the center of  $B_n$ .

Xiaofeng Wang and al.

Collins, Donald J [17] showed a braid group  $B_n$  with  $n \geq 6$  contains Mihailova subgroups. One can possibly use the

generators of these subgroups to generate entities' private keys in a public key cryptosystem by taking a braid group as the corresponding platform [18].

### B. Strong Law of Large Numbers (SLLN) on group

Let  $B_n$  be the group generated by a non empty set  $X$ . Let  $C_{B_n}(X)$  be the Cayley graph associated to  $B_n$ . Let  $(\Omega, \mathcal{F}, P)$  be a probability space and  $\xi : \Omega \rightarrow B_n$  a random  $B_n$ -variable. - A probability distribution is a function  $\mu : B_n \rightarrow [0, 1]$  on  $\xi$  such that:  $\mu(g) = \mu_\xi(g) = P(\{\omega \in \Omega \mid \xi(\omega) = g\}, g \in B_n)$ . Let  $\xi$  be a random  $B_n$ -variable such that  $M_\xi(\cdot)$  is totally defined. The set  $\mathbb{E}(\xi)$  of vertices  $g \in B_n$  having the smallest value of  $M_\xi$  i.e.

$$\mathbb{E}(\xi) = \{g \in B_n : M_\xi(g) \leq M_\xi(u), \forall u \in G\}$$

is called mean-set of  $\xi$ . with:

- The weight function is the function  $M_\xi : B_n \rightarrow \mathbb{R}$  defined by

$$M_\xi(g) = \sum_{s \in B_n} d^2(g, s) \mu(s)$$

where  $d(g, s)$  is the distance between  $g$  and  $s$  in the Cayley graph  $C_{B_n}(X)$  of  $B_n$ .

- The domain ( $M$ ) of the weight function  $M$  is defined by:

$$\text{domain}(M) = \left\{ g \in B_n \mid \sum_{s \in B_n} d^2(g, s) \mu(s) < \infty \right\}$$

The weight function  $M_\xi$  is totally defined if for all vertices  $g \in B_n$ ,  $M_\xi(g) < \infty$  i.e.  $\text{domain}(M) = B_n$ .

Considering:

- The relative frequency

$$\mu_n(g) = \mu_n(g, \omega) = \frac{|\{i \mid \xi_i(\omega) = g, 1 \leq i \leq n\}|}{n}$$

- The sample mean-set of  $\xi_1, \dots, \xi_n$  is the set  $\mathbb{S}_n$  defined by:

$$\mathbb{S}_n = \mathbb{S}(\xi_1, \dots, \xi_n) = \{g \in B_n : M_n(g) \leq M_n(u), \forall u \in G\}$$

The SLLN generalized on graphs and groups [15] shows the convergence of the sample mean-set  $\mathbb{S}_n$  to the mean-set  $\mathbb{E}(\xi)$  when  $n \rightarrow \infty$  :

$$\lim_{n \rightarrow \infty} \mathbb{S}(\xi_1, \dots, \xi_n) = \mathbb{E}(\xi_1)$$

with probability 1.

In [12] The following algorithm is described to compute the mean-set of a subset of  $G_1$ .

---

### Algorithm 1: Computation of the sample mean-set

---

**Data:** The group  $B_n$  by its set  $X$  of generators and a sample  $G_1 = \{g_1, \dots, g_n\} \subset B_n$ .

**Result:** An element  $g \in B_n$  having the smallest weight function

- 1 Choose a random element  $g \in B_n$  according to some probability measure  $\mu$  on  $B_n$ ;
- 2 **if** for every  $x \in X^{\pm 1}, M_n(g) \leq M_n(gx)$  **then**
- 3     **return return**  $g$ ;
- 4 **else**
- 5      $g \leftarrow gx$  {where  $x \in X^{\pm 1}$  is an element minimizing the value of  $M_n(gx)$ } ;
- 6     go to step (1);
- 7 **end**

---

$M_n(\cdot)$  is the weight function.

$$M_n(g) = \sum_{s \in G_1} \text{length}(\text{red}(gs^{-1}))^2 \mu(s)$$

with  $\text{red}(\cdot)$  the handle reduction function. (**Shift Property**). For all  $B_n$  random variable  $\xi$ , we have

$$\mathbb{E}(\xi c) = \mathbb{E}(\xi) c$$

where  $c$  is a constant element. (conjecture) Let  $B_n$  be the  $n$ -string braid group and let  $g \in B_n$  and  $\hat{t} = (t_1 = s_1 r, \dots, t_l = s_l r)$  be a sample of random  $B_n$ -variables. We have

$$\lim_{k \rightarrow \infty} \mathbb{S}_k(\hat{t}) = \lim_{k \rightarrow \infty} \mathbb{S}_k(s_1, \dots, s_l) r = r$$

This proposition present in [13], means that  $\lim_{k \rightarrow \infty} \mathbb{S}_k(s_1, \dots, s_l) = e$ , where  $e$  is the trivial braid in  $B_n$ .

### III. SIGNATURE SCHEMES

In this section, we present the Wang-Hu signature scheme [7] and its post-quantum version [1]. Both are based on the root extraction problem.

Alice astutely assumes the role of the signer, while Bob diligently takes charge as the recipient, responsible for verifying the authenticity of the signature message.

#### A. The Wang-Hu Scheme

Wang and Hu proposed the following signature scheme in [7].

The public information consists of a braid group  $B_n$  of an index  $n$ , an integer  $e \geq 2$ , and a collision-free one-way hash function  $\Theta$  that hashes an arbitrary message  $m$  of arbitrary length into a fixed  $k$ -bit binary string with  $k$  a positive integer, that is

$$\Theta : \{0, 1\}^* \rightarrow \{0, 1\}^k$$

#### Key generation:

Alice randomly chooses  $k$  non-trivial braids  $b_1, b_2, \dots, b_k$  in the commutative subgroup  $\langle \sigma_{j_1}, \dots, \sigma_{j_n} \rangle \subset B_n$  (For

arbitrary  $ju$  and  $jv$  with  $ju \neq jv$ ,  $|ju - jv| \geq 2$ ) and  $r \in B_n$ . Then she computes

$$a_i = rb_i^e r^{-1}, i = 1, 2, \dots, k$$

The public key is  $\{a_1, a_2, \dots, a_k\}$  and the secret key is  $\{b_1, b_2, \dots, b_k, r\}$ .

**Signing a message:**

Assuming that the message  $m \in \{0, 1\}^*$  is to be signed. Firstly, Alice randomly chooses a braid  $s$  in  $B_n$ . Then she calculates  $\Theta(m) = h_1 h_2 \dots h_k$  ( $h_i \in \{0, 1\}$ ),  $t = sr^{-1}$  and

$$v = s \left( \prod_{i=1}^k b_i^{h_i} \right) s^{-1}$$

The signature for the message  $m$  is  $(v, t)$ .

**Verification:**

Bob computes

$$w = \prod_{i=1}^k a_i^{h_i}$$

and verifies the equation

$$v^e = twt^{-1}$$

If the equation holds, he unquestionably accepts the signature  $(v, t)$  as a valid signature of Alice's for the message  $m$ . On the contrary, Bob absolutely and unequivocally discards the signature.

The authors argue that to forge a signature, an attacker must be able to extract the eth root for a particular braid in the braid group. They also show that in a scenario where the attacker can actively choose messages to create signature pairs, they would need to solve a difficult group factorization problem to generate a new signature.

*B. The Post-Quantum Scheme version*

In [1], Lin and *al.* proposed the following signature scheme.

The public information:

- An integer  $e \geq 2$ ;
- A collision-free one-way hash function  $\Theta$  that hashes an arbitrary message  $m$  of arbitrary length into a fixed  $k$ -bit binary string with  $k$  a positive integer, that is

$$\Theta : \{0, 1\}^* \rightarrow \{0, 1\}^k$$

- A braid group  $B_n$  of index  $n$  with  $n \geq 6k$ ;
- The Mihailova subgroups  $A_i = M_{G_{\delta(i-1)+1}}(H)$ ,  $i = 1, 2, \dots, k$ , as defined in the previous section.

One can see that since  $A_i = M_{G_i}(H)$  is a subgroup of  $G_i$  where  $G_i$  is generated by  $\sigma_i^2, \sigma_{i+1}^2, \sigma_{i+3}^2, \sigma_{i+4}^2$ , for each pair of  $i$  and  $j$ , if  $i \neq j$  then for any braid  $b_i \in A_i$  and any  $b_j \in A_j$ ,  $b_i b_j = b_j b_i$ .

**Key generation:**

Alice randomly chooses  $k$  non-trivial braids  $b_i \in A_i$ ,  $i = 1, 2, \dots, k$ , and an element  $r \in B_n$ . Then she computes

$$a_i = rb_i^e r^{-1}, i = 1, 2, \dots, k$$

The public key is  $\{a_1, a_2, \dots, a_k\}$  and the secret key is  $\{b_1, b_2, \dots, b_k, r\}$ .

**Signing a message:**  $m \in \{0, 1\}^*$

Alice randomly chooses a braid  $s$  in  $B_n$ .

Then she calculates  $\Theta(m) = h_1 h_2 \dots h_k$  ( $h_i \in \{0, 1\}$ ),

$$t = sr^{-1}$$

and

$$v_i = sb_i^{h_i} s^{-1}, i = 1, 2, \dots, k$$

The signature for the message  $m$  is  $(v_1, v_2, \dots, v_k, t)$ .

**Verification:**

Bob computes  $w_i = a_i^{h_i}$ ,  $i = 1, 2, \dots, k$ , and verifies the equations

$$v_i^e = tw_i t^{-1}, i = 1, 2, \dots, k$$

As the above security analysis showed, the reformed signature scheme is unforgettable and resistant to key-recovery attacks. Hence, no one else could create any valid evidence that the signature originated from Alice, which guarantees the non-repudiation of the signer's signature. The claim is that the signature scheme is resistant to both quantum computational attacks and all other known attacks.

## IV. CRYPTANALYSIS

### A. Key Recovery Attack

The attacker, Eve can send a set of messages  $m_1, \dots, m_l$  to the user and obtain the corresponding signatures  $(v_1, t_1), \dots, (v_l, t_l)$ . We have a shift property  $\mathbb{E}(\xi r^{-1}) = \mathbb{E}(\xi) r^{-1}$  and the generalization of the SLLN for groups in the sense that  $\mathbb{S}_l(\xi_1 r^{-1}, \dots, \xi_l r^{-1})$  converges to  $\mathbb{S}_l(\xi_1, \dots, \xi_l) r^{-1}$  when  $n \rightarrow \infty$ , with probability 1. The sample mean-set  $\hat{t} = (t_1 = s_1 r^{-1}, \dots, t_l = s_l r^{-1})$  is efficiently computable. On the set  $\hat{t} = (t_1 = s_1 r^{-1}, \dots, t_l = s_l r^{-1})$ , we use the mean-set algorithm 1 to get some  $r'$ .

So the braids  $b_1, \dots, b_k$  in the subgroup  $\langle \sigma_{j_1}, \dots, \sigma_{j_n} \rangle \subset B_n$  (For arbitrary  $ju$  and  $jv$ ,  $ju \neq jv$ ,  $|ju - jv| \geq 2$ ) are commutative. In this particular subgroup, the extraction of the eth root is relatively simple.

In the wang-Hu Scheme, an attacker was able to recover the secret key using a following algorithm:

---

**Algorithm 2:** Attack against Wang-Hu Scheme

---

**Data:**  $v_1, m_1$ , set  $\hat{a} = (a_1, \dots, a_k)$  and set  $\hat{t} = (t_1 = s_1 r^{-1}, \dots, t_l = s_l r^{-1})$ .

**Result:**  $(b_1, b_2, \dots, b_k, r)$

```
1 Apply Algorithm 1 to  $\hat{t}$  and get  $r'$ ;
2 Compute  $s'_1 = t_1 r'^{-1}$ ;
3 Compute  $\hat{b}'^e = (b'_1{}^e = r' a_1 r'^{-1}, \dots, b'_k{}^e = r' a_k r'^{-1})$ ;
4 Compute  $\hat{b}' = (b'_1, \dots, b'_k)$  an eth root sample from  $\hat{b}'^e = (b'^e, \dots, b'_k{}^e)$ ;
5 if  $v_1 == s'_1 \left( \prod_{i=1}^k b_i^{\Theta(m_1)} \right) s'^{-1}$  then
6 |   return  $(\hat{b}', r')$ ;
7 else
8 |   return 0
9 end
```

---

To achieve a moderate security level, Wang, B. C. and Hu, Y. P. suggested these parameters: braid index  $n = 90$ ,  $e = 2$ , the binary length  $k$  of the output of the hash function  $H$  be 80. The length of random words  $r$  and  $s$  equal 8. We implemented on SageMath. It is a free open-source mathematics software system licensed under the General Public License. We performed several sets of tests, all of which were run on an 11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz computer with 16 GB of RAM, running Ubuntu 22.04. The secret  $r$  is obtained with a sample of 100 signatures in 85 seconds on average.

The technique used in the quantum version is similar to the original version, but with a slight modification that allows us to recover the secret key  $(r, (b_1, \dots, b_k))$ .

---

**Algorithm 3:** Attack against Post-Quantum Scheme version

---

**Data:**  $\hat{m} = (m_1 \dots m_l)$ , set  $\hat{a} = (a_1, \dots, a_k)$ ,  $\hat{v} = (v_1 = (v_{11}, \dots, v_{1k}) \dots v_l = (v_{l1}, \dots, v_{lk}))$  and set  $\hat{t} = (t_1 = s_1 r^{-1}, \dots, t_l = s_l r^{-1})$ .

**Result:**  $(b_1, b_2, \dots, b_k, r)$

```
1 Apply Algorithm 1 to  $\hat{t}$  and get  $r'$ ;
2  $\hat{b}' = ()$ ;
3  $i = 1$ ;
4 while  $\hat{b}'$  not contain all  $b'_j$  do
5 |   Compute  $\Theta(m_i) = h_{i1} \dots h_{ik}$ ;
6 |   for  $j$  in  $(1, \dots, k)$  do
7 |   |   if  $h_{ij} == 1$  then
8 |   |   |   Compute  $b'_j = s'^{-1} v_{ij} s'$ ;
9 |   |   |   Compute  $\hat{b}' = \hat{b}' \cup (b'_j)$ ;
10 |   |   end
11 |   end
12 |    $i = i + 1$ ;
13 end
14 if  $\hat{a}i = (r' b_1^e r'^{-1}, \dots, r' b_k^e r'^{-1})$  then
15 |   return  $(\hat{b}', r')$ ;
16 else
17 |   return 0
18 end
```

---

The potential vulnerability of these signature schemes is

demonstrated by the ability of these algorithms to operate efficiently.

### B. On Forging a Signature

In the post-quantum version [1], the authors assert that to forge a signature, an attacker must extract the eth root for a specific braid in the braid group. The attacker can easily forge  $(v_1 = s b_1 s^{-1}, v_2 = s b_2 s^{-1}, \dots, v_k = s b_k s^{-1}, t = s r^{-1})$ .

Let's take a message  $m$  and signature  $(v_1, v_2, \dots, v_k, t)$  with  $v_j = s b_j^h s^{-1}$ . For  $h_j = 0$  normally we get  $v_j = e$  ( $e$  trivial braid), but we can compute  $v_j = s b_j s^{-1}$  without knowing  $s$  and  $b_j$ . All we need to do is find a message  $m'$  and its signature  $(v'_1, v'_2, \dots, v'_k, t')$  where  $h'_j = 1$ .

$$\begin{aligned} v_j &= t t'^{-1} v'_j t' t^{-1} \\ v_j &= s r^{-1} r s'^{-1} v'_j s' r^{-1} r s^{-1} \\ v_j &= s s'^{-1} v'_j s' s^{-1} \\ v_j &= s s'^{-1} s' b'_j s'^{-1} s' s^{-1} \\ v_j &= s b_j s^{-1} \end{aligned}$$

Given a message  $m_1$  and  $\Theta(m_1) = h_1^1 h_2^1 \dots h_k^1$  ( $h_i^1 \in \{0, 1\}$ ), the attacker will forge a signature

$$(v_1^1 = v_1^{h_1^1}, v_2^1 = v_2^{h_2^1}, \dots, v_k^1 = v_k^{h_k^1}, t)$$

passing the verification  $(v_i^1)^e = t a_i^{h_i^1} t^{-1}$ . Now we show that the attacker can forge a signature passing the verification without knowing secrets elements.

### CONCLUSION

In conclusion, this article presents algorithms that effectively attack two digital signature schemes mentioned in [1], [7]. The vulnerabilities exposed by these attacks emphasize the need for robust and quantum-resistant digital signature schemes to ensure the security and integrity of digital transactions in the future. Further research is essential to address these challenges and develop more secure cryptography solutions.

### REFERENCES

- [1] Hanling Lin, Xiaofeng Wang, and Min Li. Post-Quantum Signature Scheme Based on the Root Extraction Problem over Mihailova Subgroups of Braid Groups. *Mathematics*, 11(13), 7 2023.
- [2] Joan Birman, Ki Hyoung Ko, and Sang Jin Lee. A new approach to the word and conjugacy problems in the braid groups. *Advances in Mathematics*, 139(2):322–353, 1998.
- [3] Patrick Dehornoy. A fast method for comparing braids. *Advances in Mathematics*, 125(2):200–235, 1997.
- [4] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6(3):287–291, 1999.
- [5] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings 20*, pages 166–183. Springer, 2000.

- [6] Hervé Sibert, Patrick Dehornoy, and Marc Girault. Entity authentication schemes using braid word reduction. *Discrete Applied Mathematics*, 154(2):420–436, 2006.
- [7] B. C. Wang and Y. P. Hu. Signature scheme based on the root extraction problem over braid groups. *IET Information Security*, 3(2):53–59, 2009.
- [8] Jung Hee Cheon and Byungheup Jun. A polynomial time algorithm for the braid diffie-hellman conjugacy problem. In *Advances in Cryptology-CRYPTO 2003: 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003. Proceedings 23*, pages 212–225. Springer, 2003.
- [9] Alex D Myasnikov and Alexander Ushakov. Length based attack and braid groups: cryptanalysis of anshel-anshel-goldfeld key exchange protocol. In *International Workshop on Public Key Cryptography*, pages 76–88. Springer, 2007.
- [10] Anja Groch, Dennis Hofheinz, and Rainer Steinwandt. A practical attack on the root problem in braid groups. *Cryptology ePrint Archive*, 2005.
- [11] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. A practical attack on a braid group based cryptographic protocol. In *Advances in Cryptology-CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005. Proceedings 25*, pages 86–96. Springer, 2005.
- [12] Natalia Mosina and Alexander Ushakov. Mean-set attack: Cryptanalysis of Sibert et al. authentication protocol. *Journal of Mathematical Cryptology*, 4(2):149–174, 10 2010.
- [13] Sidoine Djimnaibeye, Daniel Tieudjo, and Norbert Youmbi. Probability on groups and an application to cryptography \*. *Computer Science Journal of Moldova*, 23(3):2015.
- [14] Maria Cumplido, Delaram Kahrobaei, and Marialaura Noce. The root extraction problem in braid group-based cryptography. 3 2022.
- [15] Natalia Mosina and Alexander Ushakov. Strong law of large numbers on graphs and groups. 4 2009.
- [16] KA Mihajlova. : The occurrence problem for direct products of groups. 1971.
- [17] Donald J Collins. Relations among the squares of the generators of the braid group. *Inventiones mathematicae*, 117(1):525–529, 1994.
- [18] Xiaofeng Wang, Guo Li, Ling Yang, and Hanling Lin. Groups with two generators having unsolvable word problem and presentations of mihailova subgroups of braid groups. *Communications in Algebra*, 44(7):3020–3037, 2016.