mathematics

MDPI

Article

Post-Quantum Signature Scheme Based on the Root Extraction Problem over Mihailova Subgroups of Braid Groups

Hanling Lin, Xiaofeng Wang and Min Li *

College of Mathematics and Statistics, Shenzhen University, Shenzhen 518060, China; lb@szu.edu.cn (H.L.)
* Correspondence: limin800@szu.edu.cn; Tel.: +86-1342-891-9322

Abstract: In this paper, by introducing an isomorphism from the Mihailova subgroup of $F_2 \times F_2$ to the Mihailova subgroups of a braid group, we give an explicit presentation of Mihailova subgroups of a braid group. Hence, in a braid group, there are some Mihailova subgroups experiencing unsolvable subgroup membership problem. Based on this, we propose a post-quantum signature scheme of the Wang–Hu scheme, and we show that the signature scheme is free of quantum computational attack.

Keywords: post-quantum; braid group; Mihailova subgroup; signature scheme

MSC: 18M15

1. Introduction

In the literature, the security assumptions of signature schemes are often based on a complex computational problem. For example, the RSA signature scheme [1] is based on the integer factorization problem. Elgamal's signature scheme [2] is based on the discrete logarithm problem. Additionally, Koblitz's signature scheme [3] is based on the discrete logarithm problem on elliptic curves. Both Wei's signature scheme [4] and Vermal and Sharma's signature scheme [5] are based on the factoring and discrete logarithm problem. In 1997, Shor [6] proposed a probabilistic quantum algorithm for large integer decompositions and discrete logarithm calculations. In 2003, Proos and Zalka [7] extended Shor's algorithm and obtained a quantum algorithm for solving the discrete logarithm problem on elliptic curves. These algorithms need to be run on a quantum computer to achieve the desired effect. In 2019, a group of researchers from Google published a paper [8] announcing that they realized a 53 qubits quantum computation system capable of running quantum algorithms. Hence all the above well-known cryptographic schemes would be no safer under a quantum computation circumstance. It is then obviously urgent for cryptologists to find new public key cryptosystems that can resist quantum computer attacks. Consequently, a varieties of post-quantum cryptographic schemes have been proposed. For example, lattice-based cryptography and multivariate public key cryptography (MPKC) are two ways to construct post-quantum cryptographic schemes. In [9], a general multivariate public key cryptographic proxy signature scheme (MPKC) was proposed by Chen et al.. The security of MPKC is based on an NP-hard problem. The main drawback of MPKC is that the length of the public key is too long, which makes the signature algorithm very heavy. With the performance of faster calculation, less communication cost, and having some computationally hard problems, lattices are widely believed to be promising platforms to set up post-quantum cryptographic schemes. In [10,11], signature schemes based on lattices were proposed. The security of these schemes is guaranteed by NP-hard problems. Alternatively, new quantum signature schemes which are based on the quantum information theory of physical essence have also been considered. For example, Zheng et al. [12] proposed an arbitrated quantum signature scheme with quantum teleportation by using two three-qubit GHZ states. Yang et al. [13] proposed an arbitrated quantum signature scheme based on cluster states.

Citation: Lin, H.; Wang, X.; Li, M. Post-Quantum Signature Scheme Based on the Root Extraction Problem over Mihailova Subgroups of Braid Groups. *Mathematics* **2023**, *11*, 2892. https://doi.org/10.3390/math11132892

Academic Editors: Liehuang Zhu, Meng Li and Zijian Zhang

Received: 24 April 2023
Revised: 25 June 2023
Accepted: 26 June 2023
Published: 27 June 2023

Due to the work of Anshell et al. [14] and Ko et al. [15], braid groups have been intensively used as a platform to construct public key cryptographic schemes where the safety of the schemes was claimed mainly by the conjugate search problem (for examples see [16–22] for references). However, people have found a variety of security drawbacks of these schemes, and therefore, some attack techniques have been developed [23–32]. It seems then that the conjugate search problem of braid groups is no more reliable for guaranteeing the safety of a braid group cryptography application.

The root extraction problem (REP) is another decision problem with braid groups. This decision problem is believed to be much harder than the conjugate search problem [33]. There are a number of public cryptosystems [19,34,35] that are based on the root extraction problems in braid groups. In [19], an entity authentication scheme which is based on the hardness of the REP has been put forward by Sibert et al.. Groch et al. provided a practical algorithm [36] for root extraction of a braid, and therefore, it seems that Sibert et al.'s scheme is not secure. We will show that Groch et al.'s algorithm is actually not applicable for root extraction of a braid. In [34], Lal and Chaturvedi proposed two authentication schemes that were claimed to be also based on the REP. However, the first of these two schemes has been attacked [37] without requiring solving the REP and it was pointed out [23] that the second one actually relies on the difficulty of the Deffie–Hellman decomposition problem which can be solved in polynomial time. In 2009, Wang and Hu proposed a signature scheme [35] based on the root extraction problem of braid groups. Wang and Hu proved that for an attacker to forge a valid signature for a given message m if and only if he can extract the eth root of the braid v generated in the scheme corresponding the message m. One may note that Myasnikov et al. gave a practical algorithm [38] for decomposition of a braid. This then may allow the attacker to decompose a braid v into a product of v_i's where the eth root of these v_i's are known. Therefore, the eth root of v can be computed as Wang and Hu pointed out in Section 5.3 of [35]. Therefore, Wang and Hu's signature scheme would not be sufficiently secure.

In [39], Wang, Li, and Lin have given an explicit presentation of the Mihailova subgroups of $F_2 \times F_2$, which experience unsolvable subgroup membership problems. Then by using an isomorphism, we show that for an index $n \geq 6$, a braid group B_n contains such Mihailova subgroups. This provides us a choice to enforce the safety of some braid group-based cryptosystems. In this paper, by introducing the Mihailova subgroups of a braid group and choosing some elements of Mihailova subgroups as part of public keys and secret keys, we propose a reformed signature scheme of Wang–Hu's. In the following section, we show the security of this reformed scheme is free of all known attacks, including the quantum computational attack.

The rest of this paper is organized as follows. In the Section 2, a brief review of braid groups is stated and then by an isomorphism, an explicit presentation of Mihailova subgroups of a braid group B_n with $n \geq 6$ is given. These Mihailova subgroups experience unsolvable subgroup membership problems. Section 3 serves to propose a reformed signature scheme of Wang–Hu's [35]. In the Section 4, we show that the security of the proposed reformed signature scheme is free of all known attacks.

2. Braid Groups and Mihailova Subgroups

2.1. Braid Groups and Δ-Normal Forms

A braid group B_n, which will be taken as the platform group for the post-quantum scheme, is defined by the following presentation

$$B_n = \langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} | \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j, |i-j| = 1, \sigma_i\sigma_j = \sigma_j\sigma_i, |i-j| \geq 2 \rangle$$

where $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ are called the Artin generators of B_n , and the elements of B_n are called braids.

For any elements $x, y \in B_n$, if there exists another element $a \in B_n$, such that $y = a^{-1}xa$, we then say that x, y are conjugate.

Let G be a group, x, y, g be the elements of G, such that $y = g^{-1}xg$. The conjugate search problem is defined to ask for finding an element $g^{'} \in G$, such that $y = g^{'-1}xg^{'}$.

Let G be a group, x be an element of G, and $e \geq 2$ be an integer, such that $x = y^e$ for some unknown element $y \in G$. The root extraction problem is defined to ask for finding an element $z \in G$, such that $x = z^e$.

Let G be a group, H be a subgroup generated by elements $b_1, b_2, \ldots, b_k$ of G. The membership problem of H is defined to ask for any element x of G if $x \in H$ is true. Equivalently, that is to ask if x can be expressed as the product of the powers of $b_1, b_2, \ldots, b_k$.

Let Δ_n denote the positive braid of B_n^+ inductively defined by

$$\Delta_1 = \sigma_1, \Delta_i = \sigma_1 \cdots \sigma_{i-1}\Delta_{i-1}(1 < i \leq n) \tag{1}$$

We say that a positive braid $u \in B_n^+$ is canonical if it is a left divisor of Δ_n, i.e., if we have $\Delta_n = uv$ for some positive braid v. If u is any positive braid, then there exists a maximal canonical braid u_1 that divides u, namely the left gcd of u and Δ_n. We can then write $u = u_1u'$, and repeat the operation, i.e., look for the maximal simple left divisor u_2 of u', and so we can write $u = u_1u_2 \cdots u_s$ with all u_i's are canonical. Every braid u in B_n admits a unique decomposition of the form [40,41]

$$u = \Delta_n^k u_1 u_2 \cdots u_r \tag{2}$$

where each u_i is canonical and is distinct of Δ_n and 1 and is the maximal left canonical left divisor of $u_iu_{i+1} \cdots u_r$. We call (2) the Δ-normal form of u and r the canonical length of u. There then is a homomorphism $\pi : B_n \to S_n$ from B_n to the symmetric group S_n defined by $\pi(\sigma_i) = (i, i+1)$ and restricting π to the set of canonical factors in B_n induces a bijection [40].

2.2. A Practical Attack on Root Problem

In [36] Groch et al. proposed a practical attack on the root problem in braid groups. First they proved that a braid $u \in B_n$ has Δ-normal form

$$u = \Delta_n^k u_1 u_2 \cdots u_r \tag{3}$$

and that a braid $w \in B_n$ with $w = u^e$ with $e > 1$ an integer has Δ-normal form

$$w = \Delta_n^{k'} w_1 w_2 \cdots w_{r'} \tag{4}$$

such that $l = r' - (e-1)r > 0$. Then the last l canonical factors $w_{(e-1)r+1} \cdots w_{r'}$ of the Δ-normal form of w form a tail of $u_1 \cdots u_r$, i.e.,

$$u_1u_2 \cdots u_r = u'w_{(e-1)r+1} \cdots w_{r'}$$

for some positive braid $u' \in B_n$. They then let u_R be the tail of u and $u_L \in B_n^+$ be the remaining canonical part of u, such that

$$u = \Delta_n^k u_L u_R$$

For any canonical factor $v \in B_n$, by writing $\bar{v}$ for $\pi(v)$, they then claimed that by extracting the eth roots of permutation $\bar{w}$ one can extracting the eth roots of w in B_n. To find the solution to the equation

$$\bar{w} = x^e \tag{5}$$

in the symmetric group S_n, they let $y = \bar{w}$ and suppose $x \in S_n$ is a solution to Equation (5). Let x be a product of disjoint cycles $C_1, C_2, \cdots, C_q$. Then

$$y = x^e = C_1^e C_2^e \cdots C_q^e$$

By writing y as a product of disjoint cycles $D_1, D_2, \cdots, D_v$ and letting $\mathcal{L} = \bigcup_{i=1}^{v}\{|D_i|\}$ each eth root x of y then can be expressed as

$$x = \prod_{l \in \mathcal{L}} x_l$$

such that each x_l is an eth root of the product

$$y_l = \prod_{|D_i|=l} D_i$$

They, of course, can effectively find solutions to Equation (5). It followed that they then claimed that by the inverse of π the eth root of w may be extracted by checking if $(\Delta_n^k \pi^{-1}(\overline{u_L})u_R)^e = w$ where $\pi^{-1}(\overline{u_L})$ is obtained in turn from $\overline{u}$ by setting $\overline{u} = x$.

2.3. Mihailova Subgroups

Consider H as a group that is defined by

$$\Gamma = \langle x_1, x_2, \ldots, x_k | R_1, R_2, \ldots, R_m \rangle$$

with integer $k \geqslant 2$, and let F_k denote the free group on $x_1, x_2, \ldots, x_k$. Then, in the article [42], Mihailova associated with H in the Mihailova subgroup, denoted as $M(H)$, of the direct product of $F_k \times F_k$ defined by

$$M(H) = \{(\omega_1, \omega_2) | \omega_1 = \omega_2, \omega_1 \in H, \omega_2 \in H\}$$

Mihailova [42] then proved the following theorem.

Theorem 1 (Mihailova [42]). *The subgroup membership problem for $M(H)$ in $F_k \times F_k$ is solvable if and only if the word problem for H is solvable.*

In their paper [43], Bogopolski and Venura proved a theorem that gives an explicit representation of Mihailova subgroup $M(H)$ in $F_k \times F_k$ under the assumption that the group H satisfies certain conditions. In [39], Wang, Li, and Lin gave a finite presentation of a group H, which is generated by just two elements and experiences an unsolvable word problem. Additionally, they proved that the presentation of H satisfies the conditions required in Bogopolski and Venura's theorem in [43]. It followed that they then gave an explicit presentation of the generators and infinitely countable defining relators of the Mihailova subgroup $M(H)$ in $F_2 \times F_2$ as the following:

$$D = \langle (u,u), (t,t), (1, \mathcal{S}_i) | \mathcal{S}_i^{-1}(\delta^{-1}\mathcal{S}_k^{-1}\gamma_k^{-1}\delta)^{-1}\mathcal{S}_i(\delta^{-1}\mathcal{S}_k^{-1}\gamma_k^{-1}\delta),\ \mathcal{S}_i^{-1}\gamma_i^{-1}\mathcal{S}_i\gamma_i \rangle$$

where $\delta \in F_2 \times F_2$, $\mathcal{S}_i = (\mathcal{R}_i^{(r)}(t,u))^{-1}\mathcal{R}_i^{(l)}(t,u)$, $\mathcal{R}_i^{(r)}(t,u)$ and $\mathcal{R}_i^{(l)}(t,u)$ are defined in the Presentation C in [39], $i, k = 1, 2, \ldots, 27$.

Since the word problem in H is unsolvable using the main theorem in [42], it followed that the membership problem for the Mihailova subgroup $M_{F_2 \times F_2}(H)$ of $F_2 \times F_2$ is unsolvable

For a braid group B_n with $n \geqslant 6$, a result established by Collins in [44] indicated that the subgroups G_i of B_n generated by σ_i^2, σ_{i+1}^2, σ_{i+3}^2 and σ_{i+4}^2 $(1 \leq i \leq n-5)$ denoted by

$$G_i = \langle \sigma_i^2, \sigma_{i+1}^2, \sigma_{i+3}^2, \sigma_{i+4}^2 \rangle,\ 1 \leq i \leq n-5$$

is isomorphic to the direct product $F_2 \times F_2$.

In Theorem 1.1 of [43], we let $k = 2$ and let ϕ be the isomorphism that maps the group $F_2 \times F_2$ to the subgroup G_i and defined by

$$\phi : (x_1, 1) \mapsto \sigma_i^2,\ (x_2, 1) \mapsto \sigma_{i+1}^2,\ (1, x_1) \mapsto \sigma_{i+3}^2,\ (1, x_2) \mapsto \sigma_{i+4}^2$$

Through this isomorphism we obtained the Mihailova subgroups $M_{G_i}(H)$ of B_n which have an unsolvable membership problem. Since the defining relations of Presentation C′ in [39] are of the following form

$$\mathcal{R}_j : \mathcal{R}_j^{(r)}(u,t) = \mathcal{R}_j^{(l)}(u,t),\ j = 1,2,\cdots,27$$

we denote

$$\mathcal{S}_{ij} = \mathcal{R}_j^{(r)}(\sigma_i^2, \sigma_{i+1}^2))^{-1}\mathcal{R}_j^{(l)}(\sigma_i^2, \sigma_{i+1}^2),$$

where $j = 1,2,\cdots,27$, and

$$\mathcal{T}_{ij} = \mathcal{R}_j^{(r)}(\sigma_{i+3}^2, \sigma_{i+4}^2))^{-1}\mathcal{R}_j^{(l)}(\sigma_{i+3}^2, \sigma_{i+4}^2)$$

where $j = 1,2,\cdots,27$. Then for each i, by the above isomorphism ϕ, the generators of $M_{G_i}(H)$ are as follows:

$$d_1 = \sigma_i^2\sigma_{i+3}^2,\ d_2 = \sigma_{i+1}^2\sigma_{i+4}^2,$$
$$1\mathcal{T}_{ij} = \mathcal{T}_{ij},\ \mathcal{S}_{ij}1 = \mathcal{S}_{ij}$$

where $j = 1,2,\cdots,27$ and all the $\mathcal{S}_{ij}$ are listed in the Appendix A at the end of the article (one can obtain the descriptions of all the $\mathcal{T}_{ij}$'s by replacing all occurrences of σ_i^2 with σ_{i+3}^2 and all occurrences of σ_{i+1}^2 with σ_{i+4}^2 in $\mathcal{S}_{ij}$, $j = 1,2,\ldots,\cdots,27$).

3. The Post-Quantum Scheme

In the signature scheme, Alice acts as the signer, while Bob serves as the recipient responsible for verifying the signature message.

3.1. The Wang–Hu Scheme

In [35], Wang and Hu proposed the following signature scheme.

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

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

Key generation: Alice randomly chooses $k+1$ non-trivial braids $b_1,\ b_2,\ \cdots,\ b_k,\ r$ in B_n such that b_i and b_j commute, $i,\ j = 1,\ 2,\ \cdots,\ k$. Then she computes

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

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

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 $\Theta(m) = h_1h_2\cdots h_k (h_i \in \{0,1\})$, $t = sr^{-1}$ and

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

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 accepts the signature (v, t) as a valid signature of Alice's for the message m. Otherwise, Bob discards the signature.

3.2. The Post-Quantum Scheme

The public information:

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

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

- A braid group B_n of index n with $n \geq 6k$;
- The Mihailova subgroups $A_i = M_{G_{6(i-1)+1}}(H)$, $i = 1, 2, \cdots k$, 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 $\sigma_i, \sigma_{i+1}, \sigma_{i+3}, \sigma_{i+4}$, for each pair of i and j, if $i \neq j$ then for any braid $b_i \in A_i$ and any $b_j \in A_j$, $b_i b_j = b_j b_i$ if $i \neq j$.

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

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

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

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 $\Theta(m) = h_1 h_2 \cdots h_k (h_i \in \{0, 1\})$, $t = sr^{-1}$ and

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

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

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

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

If all the equations hold, he accepts the signature $(v,\ t)$ as a valid signature of Alice's for the message m. Otherwise, Bob discards the signature.

Why verification works: The following shows that the verification works

$$tw_i t^{-1} = ta_i^{h_i} t^{-1} = t(rb_i^e r^{-1})^{h_i} t^{-1} = (trb_i^{h_i} r^{-1} t^{-1})^e = (sb_i^{h_i} s^{-1})^e = v_i^e,\ i = 1,\ 2,\ \cdots,\ k$$

4. Security Analysis and Parameters

4.1. Key Recovery Attack

As Wang and Hu pointed out in [35], since any attacker does not know the secret key $(b_1, b_2, \cdots, b_k)$, he cannot construct k equations $a_i = rb_i^e r^{-1}$, $i = 1, 2, \cdots, k$. Therefore, it is impossible for him to find $r' \in B_n$ such that $r' b_i^e r'^{-1} = a_i$, $i = 1, 2, \cdots, k$.

4.2. On Forging a Signature

Let m be a given message and let $\Theta(m) = h_1 h_2 \cdots h_k$. Then

$$w_i = a_i^{h_i} = (rb_i^e r^{-1})^{h_i} = (rb_i^{h_i} r^{-1})^e,\ i = 1, 2, \cdots, k$$

Provided an attacker wants to forge a valid signature for m, say $(v'_1, v'_2, \cdots, v'_k, t')$. Then he must have the following equations:

$$v_i^e = t' w_i t'^{-1} = t'(r b_i^{h_i} r^{-1})^e t'^{-1} = (t' r b_i^{h_i} r^{-1} t'^{-1})^e,\ i = 1, 2, \cdots, k$$

Hence, as Wang and Hu pointed in [35], an attacker is able to forge Alice's signature in our post-quantum scheme in the previous section if and only if he can extract the eth roots for the braids w_i, $i = 1, 2, \cdots, k$.

We first show that Groch et al.'s root extraction algorithm is not applicable. Clearly, the bijection π in Section 2.1 from the set of all canonical braids in B_n to the symmetric group S_n is not a bijection from B_n^+ to S_n. Now, for each i if we choose $b_i \in A_i$ such that in the Δ-normal form of $w_i = \Delta_n^{r'_i} w_{i'_1} \cdots w_{i'_s}$ (as in (4)) the length of the product of canonical factors $w_{i_1} \cdots w_{i'_s}$ is greater than $en^2 + n$. Let $\pi(w_i) = \bar{w}_i$. Working with Groch et al.'s root extraction algorithm one can find all solutions in S_n of equation $\bar{w}_i = x_i^e$ as in Equation (5). Let x_i be any one of the solutions and write $x_i = C_{i_1} C_{i_2} \cdots C_{i_q}$ being a product of disjoint cycles. Then $i_q < n$. Since the inverse of π of each cycle C_{i_j} is a canonical braid of length less than n, then the length of e power of $\pi^{-1}(x_i)$ (product of canonical factors) is less than en^2. However, the length of the product of canonical factors of w_i is greater than $en^2 + n$. Thus, the inverse of π of x_i could not be an eth root of w_i.

Therefore, if h_i is not 0, then $r b_i^{h_i} r^{-1} \in r A_i r^{-1}$. However, w_i is an element of the subgroup $r A_i r^{-1}$, which is isomorphic to the Mihailova subgroup A_i. Hence the membership problem of $r A_i r^{-1}$ is also unsolvable. Furthermore, based on González-Meneses' result in [45], we know that the eth root of a braid is unique up to conjugacy. Therefore, the only way for an attacker to extract the eth root of w_i is to find an element $d_i \in r A_i r^{-1}$ such that $d_i^e = w_i$ for all $i \neq 0$. However, firstly since he does not know r, he is not sure which conjugate of A_i is. Furthermore, since $r A_i r^{-1}$ is a Mihailova subgroup, there is no algorithm for him to find such d_i's.

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.

4.3. Suggested Parameters

To work against Groch et al.'s root extraction algorithm attack, we require in our post-quantum scheme that the word size of each $b_i \in A_i$ should be large enough such that in the Δ-normal form of $w_i = \Delta_n^{r'_i} w_{i'_1} \cdots w_{i'_s}$ (as in (4)) the length of the product of canonical factors $w_{i_1} \cdots w_{i'_s}$ is greater than $en^2 + n$. Moreover, for less computational complexity, we suggest that for each i, b_i can be chosen to be generated by the same strategy in terms of the generators of the Mihailova subgroup A_i. Thus, to compute the normal forms of all b_i's (similarly all a_i's), one can compute just one of them and then use replacements to have all the normal forms of all others. For example, from the normal form of b_1, by replacing σ_1 with $\sigma_{6(j-1)+1}$, σ_2 with $\sigma_{6(j-1)+2}$, σ_4 with $\sigma_{6(j-1)+4}$, and σ_5 with $\sigma_{6(j-1)+5}$ one can have all the normal forms of b_j, $j = 1, 2, \cdots, k$.

5. Conclusions

In order to set up a highly safe braid group-based post-quantum signature scheme, in this paper, we first introduced Mihailova subgroups of a braid group B_n with $n \geq 6$ and gave its explicit presentation. These Mihailova subgroups experience an unsolvable subgroup membership problem. This unsolvability provides us with the possibility of proposing subgroup-based post-quantum cryptosystems. In fact, by choosing secret keys and public keys from the elements of some Mihailova subgroups, we proposed a reformed signature scheme of Wang–Hu's. Security analysis shows that our reformed scheme satisfies

verifiability, non-forgeability, and non-repudiation. Additionally, our proposed signature scheme is free of the quantum computational attack as well as all the other known attacks.

In further studies, we may apply the unsolvability of the subgroup membership problem of Mihailova subgroups of a braid group to construct other cryptographic systems, such as identity verification, information authenticity, and integrity verification.

Author Contributions: Conceptualization, H.L., X.W. and M.L.; methodology, H.L. and X.W.; validation, H.L.; formal analysis, H.L. and X.W.; writing—original draft preparation, H.L.; writing—review and editing, X.W. and M.L.; supervision, X.W.; funding acquisition, H.L. and M.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (No. 62272313, No. 62072312), the Project of Educational Commission of Guangdong Province (No. 2022KTSCX106), and Shenzhen Basic Research Project (No. JCYJ20210324094009026).

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

The appendix is a list of all the $\mathcal{S}_{ij}$:

$$\mathcal{S}_{i1}: (\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{10}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^4\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4$$

$$\mathcal{S}_{i2}: (\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^4\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{10}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^4\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4$$

$$\mathcal{S}_{i3}: (\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^6\sigma_{i+1}^4\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^6\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{10}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^6\sigma_{i+1}^4\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^6$$

$$\mathcal{S}_{i4}: (\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^8\sigma_{i+1}^4\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^8\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{10}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^8\sigma_{i+1}^4\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^8$$

$$\mathcal{S}_{i5}: (\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^4\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{10}\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^4\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{14})^{10}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^4\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{10}$$

$$\mathcal{S}_{i6}: (\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16})^{10})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2$$

$$\mathcal{S}_{i7}: (\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^4\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16})^{10})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^4\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4$$

$$\mathcal{S}_{i8}: (\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^6\sigma_{i+1}^4\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^6(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16})^{10})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^4\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^6\sigma_{i+1}^4\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^6$$

$$\mathcal{S}_{i9}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^{10})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}$$

$$\mathcal{S}_{i,10}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^{10})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}$$

$$\mathcal{S}_{i,11}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}$$

$$\mathcal{S}_{i,12}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}$$

$$\mathcal{S}_{i,13}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}$$

$$\mathcal{S}_{i,14}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}$$

$$\mathcal{S}_{i,15}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}$$

$$\mathcal{S}_{i,16}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20}\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14}\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20}$$

$$\mathcal{S}_{i,17}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20}$$

$$\mathcal{S}_{i,18}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-12}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{12}\sigma_{i+1}^{4}\sigma_i^{-12}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{12}(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^{3}(\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20})^{3}(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^{9})^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-12}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{12}\sigma_{i+1}^{4}\sigma_i^{-12}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{12})^{3})(\sigma_{i+1}^{-4}\sigma_i^{-20}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{20}\sigma_{i+1}^{4}\sigma_i^{-20}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{20})^{9}(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^{3})\sigma_{i+1}^{-4}\sigma_i^{-12}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{12}\sigma_i^{4}\sigma_{i+1}^{-12}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{12}$$

$$\mathcal{S}_{i,19}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^{-1}\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14}\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16}\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,20}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^2\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^2)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^2\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^2\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}$$
$$\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,21}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^3\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^3)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^3\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^3\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}$$
$$\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,22}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^4\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^4)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^4\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^4\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}$$
$$\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,23}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^5\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^5)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^5\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^5\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,24}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^6\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-4}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{4}\sigma_{i+1}^{4}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{4}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^6)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^6\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}$$
$$\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^6\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,25}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^7\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-10}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{10}\sigma_{i+1}^{4}\sigma_i^{-10}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{10}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^7)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^7\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}$$
$$\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^7\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,26}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^8(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^3(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^8)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^8\sigma_{i+1}^{-4}\sigma_i^{-6}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{6}\sigma_{i+1}^{4}\sigma_i^{-6}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{6}(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^3(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^8\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

$$\mathcal{S}_{i,27}: \quad (\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^9(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^3(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^9)^{-1}(\sigma_{i+1}^{-4}\sigma_i^{-14}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{14}\sigma_{i+1}^{4}\sigma_i^{-14}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{14})^9\sigma_{i+1}^{-4}\sigma_i^{-8}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{8}\sigma_{i+1}^{4}\sigma_i^{-8}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{8}(\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{2}\sigma_{i+1}^{4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{2})^3(\sigma_{i+1}^{-4}\sigma_i^{-16}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{16}\sigma_{i+1}^{4}\sigma_i^{-16}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{16})^9\sigma_{i+1}^{-4}\sigma_i^{-18}\sigma_{i+1}^{2}\sigma_i^{2}\sigma_{i+1}^{-2}\sigma_i^{18}\sigma_{i+1}^{4}\sigma_i^{-18}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{2}\sigma_i^{18}$$

References

1. Rivest, R.; Shamir, A.; Adleman, L. A method for obtaining digital signatures and public key cryptosystems. *Comm. ACM* **1978**, *21*, 120–126. [CrossRef]
2. Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logrithems. *IEEE Trans. Inf. Theory* **1985**, *26*, 469–472. [CrossRef]
3. Koblitz, N. Ellipitic curve cryptosystem. *Math. Comput.* **1987**, *4*, 203–209. [CrossRef]
4. Wei, S. Digital Signature Scheme Based on Two Hard Problems. *Int. J. Comput. Sci. Netw. Secur.* **2007**, *12*, 207–209. [CrossRef]
5. Vermal, S.; Sharma, B.K. A New Digital Signature Scheme Based on Two Hard Problems. *Int. J. Pure Appl. Sci. Technol.* **2011**, *2*, 55–59.
6. Shor, P. Polynomail-time algorithms for prime factorization and discrete logarithms on a quantum Computer. *SIAM J. Comput.* **1997**, *5*, 1484–1509. [CrossRef]
7. Proos, J.; Zalka, C. Shors discrete logarithm quantum algorithm for elliptic curves. *Quantum Inf. Comput.* **2003**, *3*, 317–344.
8. Arute, F.; Arya, K.; Babbush, R.; Shi, W. Quantum supremacy using a programmable superconducting processor. *Nature* **2019**, *574*, 505–510. [CrossRef]
9. Chen, J.; Ling, J.; Ning, J.; Panaousis, E.; Loukas, G.; Liang, K.; Chen, J. Post quantum proxy signature scheme based on the multivariate public key cryptographic signature. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720914775. [CrossRef]
10. Lu, X.; Yin, W.; Wen, Q.; Liang, K.; Chen, L.; Chen, J. Message Integration Authentication in the Internet-of-Things via Lattice-Based Batch Signatures. *Sensors* **2018**, *18*, 4056. [CrossRef]
11. Lu, X.; Wen, Q.; Yin, W.; Liang, K.; Chen, J. Quantum-resistant identity-based signature with message recovery and proxy delegation. *Symmetry* **2019**, *11*, 272. [CrossRef]
12. Zheng, T.; Chang, Y.; Zhang, S.B. Arbitrated quantum signature scheme with quantum teleportation by using two three-qubit GHZ states. *Quantum Inf. Process.* **2020**, *19*, 163. [CrossRef]
13. Yang, Y.G.; Lei, H.; Liu, Z.C.; Bardin, C.C.; Barends, R. Arbitrated quantum signature scheme based on cluster states. *Quantum Inf. Process.* **2016**, *15*, 2487–2497. [CrossRef]
14. Anshel, I.; Anshel, M.; Goldfeld, D. An algebraic method for public-key cryptography. *Math. Res. Lett.* **1999**, *6*, 287–291. [CrossRef]
15. Ko, K.H.; Lee, S.J.; Cheon, J.H.; Han, J.W.; Kang, J.S.; Park, C. New public-key cryptosystem using braid groups. In *CRYPTO 2000: Advances in Cryptology—CRYPTO 2000*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2000; Volume 1880, pp. 166–183.
16. Ko, K.H.; Choi, D.H.; Cho, M.S.; Lee, J.W. A New Signature Scheme Using Conjugacy Problem; Cryptology ePrint Archive: Report 2002/168. 2002. Available online: http://eprint.iacr.org/2002/168 (accessed on 23 April 2023).
17. Shpilrain, V.; Ushakov, A. An authentication scheme based on the twisted conjugacy problem. In Proceedings of the ACNS'08 Proceedings of the 6th International Conference on Applied Cryptography and Network Security, Kyoto, Japan, 19–22 June 2008; pp. 366–372.
18. Shpilrain, V.; Zapata, G. Combinatorial group theory and public key cryptography. *Appl. Algebra Engrg. Comm. Comput.* **2006**, *17*, 291–302. [CrossRef]
19. Sibert, H.; Dehornoy, P.; Girault, M. Entity authentication schemes using braid word reduction. *Discret. Appl. Math* **2006**, *154*, 420–436. [CrossRef]
20. Wang, L.C.; Wang, L.H.; Cao, Z.F.; Yang, Y.X.; Niu, X.X. Conjugate adjoining problem in braid groups and new design of braid-based signatures. *Sci. China Inform. Sci.* **2010**, *53*, 524–536. [CrossRef]
21. You, W.Q.; Chen, X.M.; Qi, J.; Shao, R.R. A Public-key Cryptography Base on Braid Group. In Proceedings of the International Conference on Computer, Electronics and Communication Engineering (CECE 2017), Sanya, China, 25–26 June 2017.
22. Anshel, I.; Anshel, M.; Goldfeld, D. Non-abelian key agreement protocols. *Discret. Appl. Math.* **2003**, *130*, 3–12. [CrossRef]
23. Cheon, J.H.; Jun, B. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In *LNCS, Proceedings of the Advances in Cryptology-CRYPTO 2003, CRYPTO 2003, Santa Barbara, CA, USA, 17–21 August 2003*; Boneh, D., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2729, pp. 212–225.
24. Franco, N.; Gonzales-Meneses, J. Conjugacy problem for braid groups and Garside groups. *J. Algebra* **2003**, *266*, 112–132. [CrossRef]
25. Garber, D.; Kaplan, S.; Teicher, M.; Tsaban, B.; Vishne, U. Length-based conjugacy search in the Braid group. *Contemp. Math.* **2006**, *418*, 75–87.
26. Gebhardt, V. A new approach to the conjugacy problem in Garside groups. *J. Algebra* **2005**, *292*, 282–302. [CrossRef]

27. Hofheinz, D.; Steinwandt, R. A practical attack on some braid group based cryptographic primitives. In Proceedings of the Public Key Cryptography—PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography, Miami, FL, USA, 6–8 January 2003; Springer: Berlin/Heidelberg, Germany, 2002; pp. 187–198.
28. Hughes, J. A linear algebraic attack on the AAFG1 braid group cryptosystem. In *LNCS, Proceedings of the Information Security and Privacy, 7th Australian Conference-ACISP 2002, Melbourne, Australia, 3–5 July 2002*; Batten, L., Seberry, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2002; Volume 2384, pp. 176–189.
29. Kallka, A.G. Representation attacks on the braid Diffie-Hellman public key encryption. *Appl. Algebra Eng. Commun. Comput.* **2006**, *17*, 257–266. [CrossRef]
30. Lee, S.J.; Lee, E. Potential Weaknesses of the Commutator Key Agreement protocol Based on Braid Groups. In Proceedings of the Advances in Cryptology—EUROCRYPT 2002: International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, 28 April–2 May 2002; Proceedings 21; Springer: Berlin/Heidelberg, Germany, 2002; pp. 14–28.
31. Lee, E.; Park, J.H. Cryptanalysis of the public-key encryption based on braid groups. In Proceedings of the Advances in Cryptology—EUROCRYPT 2003, EUROCRYPT 2003, Warsaw, Poland, 4–8 May 2003.
32. Myasnikov, A.D.; Ushakov, A. Length based attack and braid groups: Cryptanalysis of Anshel-Anshel-Goldfeld key exchange protocol. In Proceedings of the Public Key Cryptography–PKC 2007: 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, 16–20 April 2007; Proceedings 10; Springer: Berlin/Heidelberg, Germany, 2007; pp. 76–88.
33. Lee, E. Braid groups in cryptology. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2004**, *87*, 986–992.
34. Lal, S.; Chaturvedi, A. Authentication Schemes Using Braid Groups. *arXiv* **2005**, arXiv:cs/0507066. [CrossRef]
35. Wang, B.C.; Hu, Y.P. Signature scheme based on the root extraction problem over braid groups. *IET Inf. Secur.* **2009**, *3*, 53–59. [CrossRef]
36. Groch, A.; Hofheinz, D.; Steinwandt, R. A Practical Attack on the Root Problem in Braid Groups. In Proceedings of the Public Key Cryptography-PKC 2003, 6th International Workshop on Theory and Practic Key Cryptography, Miami, FL, USA, 6–8 January 2003; Springer: Berlin/Heidelberg, Germany, 2003.
37. Tsaban, B. On an Authentication Scheme Based on the Root Problem in the Braid Group. *arXiv* **2005**, arXiv:cs/0509059v3. [CrossRef]
38. Myasnikov, A.; Shpilrain, V.; Ushakov, A. A Practical Attack on a Braid Group Based Cryptographic Protocol. In *Advances in Cryptology–CRYPTO 2005. CRYPTO 2005*; Lecture Notes in Computer Science; Shoup, V., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3621.
39. Wang, X.; Li, G.; Yang, L.; Lin, H. Groups with two generators having unsolvable word problem and presentations of Mihailova subgroups. *Commun. Algebra* **2016**, *44*, 3020–3037. [CrossRef]
40. Elrifai, E.A.; Morton, H.R. Algorithms for positive braids. *Q. J. Math.* **1994**, *45*, 479–497. [CrossRef]
41. Garside, F.A. The braid group and other groups. *Q. J. Math.* **1969**, *20*, 235–254. [CrossRef]
42. Mihailova, K.A. The occurence problem for direct products of groups. *Math. USSR* **1968**, *4*, 241–251.
43. Bogopolski, O.; Ventura, E. A recursive presentation for Mihailovas subgroup. *Group Geom. Dyn.* **2008**, *4*, 407–417.
44. Collins, D.J. Relations among the squares of the generators of the braid group. *Invent. Math.* **1994**, *117*, 525–530. [CrossRef]
45. González-Meneses, J. The nth root of a braid is unique up to conjugacy. *Algebr. Geom. Topol.* **2003**, *3*, 1103–1118. [CrossRef]