Double shielded Public Key Cryptosystems *

Xiaofeng Wang, Chen Xu†, Guo Li, Hanling Lin and Weijian Wang
School of Mathematics, Shenzhen University
Shenzhen 518060, P. R. China

Abstract. By introducing extra shields on Shpilrain and Ushakov's Ko-Lee-like protocol based on the decomposition problem of group elements we propose two new key exchange schemes and then a number of public key cryptographic protocols. We show that these protocols are free of known attacks. Particularly, if the entities taking part in our protocols create their private keys composed by the generators of the Mihailova subgroups of B_n, we show that the safety of our protocols are very highly guarantied by the insolvability of subgroup membership problem of the Mihailova subgroups.

Key words: public key protocol, braid group, subgroup membership problem, quantum computational attack

1 Introduction

In 2000, Ko *et al* proposed a key exchange scheme (called Ko-Lee Scheme) in [30] based on the conjugacy search problem in Braid groups. Followed then braid groups have been intensively taken as platforms by people to set up public key mechanisms (see [3, 9, 15, 33, 45, 47, 48, 49, 51, 52] for references). However, people also found a number of attacks on these protocols, for examle, the length based attack [29, 34, 26, 21, 39, 40], the Burau representation attack [28, 34, 35], the Lawrence-Krammer representation attack [10, 32], the super summit set attack [18], and the Ultra summit set attack [22]. Based on decomposition problem (DP, see [53]) in groups people also suggested a number of public key cryptographic schemes [9, 44] which actually are the generalizations of Ko-Lee scheme. Unfortunately, there are also some cryptanalyses [10, 39] on these schemes.

In this article, taking a non-abelian infinite group as a platform, we introduce a new technic by attaching extra shields on the exchange data during the interactive process setting up protocols. We show that with these enforced protections our proposed protocols are safe against all known attacks. In [53] we have given an explicit presentation of Mihailova subgroup of the group $F_2 \times F_2$ and therefore, this Mihailova subgroup enjoys unsolvable subgroup menbership problem (GWP [53]). Collins [12] had shown that for $n \geq 6$ there are subgroups of B_n isomorphic to $F_2 \times F_2$. Therefore, in the application of our proposed protocols if the entities take a braid group B_n with $n \geq 12$ as the platform and use the generators of Mihailova subgroup of B_n which are translated from the explicit presentation of Mihailova subgroup [53] to create their private keys, the correspondent protocol would be also free of the quantum computational attack (the attack based on Shor's quantum computation algorithm [43]) due to the insolvability of subgroup membership problem of Mihailova subgroup of the group $F_2 \times F_2$.

This paper is organized as follows. In Section 2, we propose a number of new public key crypt protocols by adding extra shields during the exchange procedures. In Section 3, we first present the translation into a braid group of the explicit presentation of a Mihailova subgroup given in [53], and then we suggest that a braid group is chosen to be the platform for our proposed protocols and propose two strategies of choosing private keys in the braid group where in one of the strategy we require that the

*Applications of the protection of intellectual property of all protocols proposed in this paper have been made to State Intellectual Bureau of China with patent application numbers: 201310382299.7 in 27/08/2013 and 201380001693.X in 04/12/2013, and made to Patent Cooperation Treaty(PCT) with international application numbers: PCT/CN2013/001119 in 22/09/2013 and PCT/CN2013/088475 in 04/12/2013.

†Correspondence author.

private keys are created by the generators of Mihailova subgroups. Finally in section 4, we show that our protocols are free of the most known attacks and point out that security of the protocols setting up by taking the second strategy is in the very high level even against the quantum computational attack.

2 The shielded Ko-Lee-like schemes

Based on decomposition problem Shpilrain and Ushakov suggested the following key exchange protocol in [44] (also see [9]). We will call this protocol a Ko-Lee-like scheme since it would be traced back to Ko-Lee scheme in [30].

Shpilrain and Ushakov's Ko-Lee-like protocol

(0) Alice and Bob agree on a nonabelian group G and two subgroups A, B of G, such that $ab = ba$ for any $a \in A$ and any $b \in B$.

(1) Alice privately chooses two elements $a_1 \in A$ and $b_1 \in B$, a randomly chosen element $g \in G$, and computes $x = a_1 g b_1$. Alice then sends (x, g) to Bob.

(3) Bob privately chooses two elements $a_2 \in A$ and $b_2 \in B$, and computes $y = b_2 g a_2$ and $k = b_2 x a_2 = b_2 a_1 g b_1 a_2$. Bob then sends y to Alice.

(4) Alice computes $k' = a_1 y b_1 = a_1 b_2 g a_2 b_1$.

Since $a_1 b_2 = b_2 a_1$ and $a_2 b_1 = b_1 a_2$, $k' = k$ which is then the shared key by Alice and Bob.

However, as they pointed out in [46] that if an attacker can solve the following decomposition problem (also see [53]) in G, he then is able to obtain the shared key.

Decomposition problem Given an element g of a group G, two subsets $A, B \subseteq G$ and an element $u = xgy \in G$ with $x \in A$ and $y \in B$, find elements $x' \in A$ and $y' \in B$ such that $x'wy' = xwy$.

Indeed, suppose that the attacker is able to solve the above problem in G to find $a' \in A$ and $b' \in B$ such that $a'gb' = a_1 g b_1$ and followed he can obtain the shared key by computing $a'yb' = a'b_2 g a_2 b' = b_2 a' g b' a_2 = b_2 a_1 g b_1 a_2 = k$.

To avoid the above possible attack, in the following we proposed two new public key primitives by introducing extra "shields" on the exchange data during the interactive process setting up protocols.

The shielded key exchange protocol 1

(0) Alice and Bob agree on a nonabelian group G, an randomly chosen element $g \in G$ and two subgroups A, B of G, such that $ab = ba$ for any $a \in A$ and any $b \in B$.

(1) Alice chooses four elements $a_1, a_2, b_1, b_2 \in A$, computes $x = b_1 a_1 g a_2 b_2$, and then sends x to Bob.

(2) Bob chooses six elements $c_1, c_2, d_1, d_2, d_3, d_4 \in B$, computes $y = d_1 c_1 g c_2 d_2$ and $w = d_3 c_1 x c_2 d_4$, and then sends (y, w) to Alice.

(3) Alice chooses two elements $b_3, b_4 \in A$, computes $z = b_3 a_1 y a_2 b_4$ and $u = b_1^{-1} w b_2^{-1}$, and then sends (z, u) to Bob.

(4) Bob sends $v = d_1^{-1} z d_2^{-1}$ to Alice.

(5) Alice computes $K_A = b_3^{-1} v b_4^{-1}$.

(6) Bob computes $K_B = d_3^{-1} u d_4^{-1}$ which is equal to K_A and then is Alice and Bob's common secret key.

Proof of why $K_B = K_A$:

Since $a_1, a_2, b_1, b_2, b_3, b_4 \in A$, $c_1, c_2, d_1, d_2, d_3, d_4 \in B$, $a_1, a_2, b_1, b_2, b_3, b_4$ commute with $c_1, c_2, d_1, d_2, d_3, d_4$ respectively, we have

$$\begin{aligned} K_B &= d_3^{-1} u d_4^{-1} \\ &= d_3^{-1} b_1^{-1} w b_2^{-1} d_4^{-1} \\ &= d_3^{-1} b_1^{-1} d_3 c_1 x c_2 d_4 b_2^{-1} d_4^{-1} \\ &= b_1^{-1} c_1 b_1 a_1 g a_2 b_2 c_2 b_2^{-1} \\ &= c_1 a_1 g a_2 c_2 \end{aligned}$$

and

$$\begin{aligned} K_A &= b_3^{-1} v b_4^{-1} \\ &= b_3^{-1} d_1^{-1} z d_2^{-1} b_4^{-1} \\ &= b_3^{-1} d_1^{-1} b_3 a_1 y a_2 b_4 d_2^{-1} b_4^{-1} \\ &= d_1^{-1} a_1 d_1 c_1 g c_2 d_2 a_2 d_2^{-1} \\ &= a_1 c_1 g c_2 a_2 = K_B \end{aligned}$$

The shielded key exchange protocol 2

(0) Alice and Bob agree on a nonabelian group G, an randomly chosen element $g \in G$ and two subgroups A, B of G, such that $ab = ba$ for any $a \in A$ and any $b \in B$.

(1) Alice chooses four elements $a_1, b_1 \in A$ and $c_2, d_2 \in B$, computes $x = b_1 a_1 g c_2 d_2$, and then sends x to Bob.

(2) Bob chooses six elements $a_2, b_2, b_3 \in A$ and $c_1, d_1, d_3 \in B$, computes $y = d_1 c_1 g a_2 b_2$ and $w = d_3 c_1 x a_2 b_3$, and then sends (y, w) to Alice.

(3) Alice chooses two elements $b_4 \in A$ and $d_4 \in B$, computes $z = b_4 a_1 y c_2 d_4$ and $u = b_1^{-1} w d_2^{-1}$, and then sends (z, u) to Bob.

(4) Bob sends $v = d_1^{-1} z b_2^{-1}$ to Alice.

(5) Alice computes $K_A = b_4^{-1} v d_4^{-1}$.

(6) Bob computes $K_B = d_3^{-1} u b_3^{-1}$ which is equal to K_A and then is Alice's and Bob's common secret key.

Proof of why $K_B = K_A$:

Also since $a_1, a_2, b_1, b_2, b_3, b_4 \in A$, $c_1, c_2, d_1, d_2, d_3, d_4 \in B$, $a_1, a_2, b_1, b_2, b_3, b_4$ commute with $c_1, c_2, d_1, d_2, d_3, d_4$ respectively, we have

$$\begin{aligned} K_B &= d_3^{-1} u b_3^{-1} \\ &= d_3^{-1} b_1^{-1} w d_2^{-1} b_3^{-1} \\ &= d_3^{-1} b_1^{-1} d_3 c_1 x a_2 b_3 d_2^{-1} b_3^{-1} \\ &= b_1^{-1} c_1 b_1 a_1 g c_2 d_2 a_2 d_2^{-1} \\ &= c_1 a_1 g c_2 a_2 \end{aligned}$$

and

$$\begin{aligned} K_A &= b_4^{-1} v d_4^{-1} \\ &= b_4^{-1} d_1^{-1} z b_2^{-1} d_4^{-1} \\ &= b_4^{-1} d_1^{-1} b_4 a_1 y c_2 d_4 b_2^{-1} d_4^{-1} \\ &= d_1^{-1} a_1 d_1 c_1 g a_2 b_2 c_2 b_2^{-1} \\ &= a_1 c_1 g a_2 c_2 = K_B \end{aligned}$$

Based on the protocol 1 in the above, by using the technic in [30] one then can easily set up the following public key encryption protocol and digital signature protocol. Analogously, one also can set up correspondent public key application protocols based on our shielded key exchange protocol 2.

The shielded public key encryption protocol

Key generation:

Alice chooses a nonabelian group G, an element $g \in G$, two subgroups A, B of G satisfying $ab = ba$ for any $a \in A$ and any $b \in B$, and two elements $b_1, b_2 \in A$. Alice also chooses a collision free hash function $\Theta : G \to \{0,1\}^k$ where k is a positive integer large enough such that $\{0,1\}^k$ can cover all the message. Alice publishes

$$(G, A, B, g, \Theta)$$

as her public key. Alice's private key is (b_1, b_2).

Let $m \in \{0,1\}^k$ is the message which is going to be sent to Alice by Bob. Bob and then Alice processe the following encryption.

Encryption:

(1) Bob chooses four elements $c_1, c_2, d_1, d_2 \in B$, computes $y = d_1c_1gc_2d_2$, and then sends y to Alice.

(2) Alice chooses four elements $a_1, a_2, b_3, b_4 \in A$, computes $x = b_1a_1ga_2b_2$ and $z = b_3a_1ya_2b_4$, and then sends (x, z) to Bob.

(3) Bob chooses two elements $d_3, d_4 \in B$, computes $w = d_3c_1xc_2d_4$ and $v = d_1^{-1}zd_2^{-1}$, and then sends (w, v) to Alice.

(4) Alice computes $K_A = b_3^{-1}vb_4^{-1}$ and $u = b_1^{-1}wb_2^{-1}$, and then sends u to Bob.

(5) Bob computes $K_B = d_3^{-1}ud_4^{-1}$ and $t = \Theta(K_B) \oplus m$ where $\oplus$ is the *exclusive or* operation. Bob then sends t to Alice which is the ciphertext.

Decryption:

Alice recovers the message m by computing $\Theta(K_A) \oplus t = m$.

Proof of why the above decryption works:
First we already have $K_A = K_B$. Therefore,

$$\Theta(K_A) \oplus t = \Theta(K_B) \oplus \Theta(K_B) \oplus m = m$$

The shield digital signature protocol

Let $m \in \{0, 1\}^k$ be the document which is going to be signed by Alice. Alice then processes the following procedure.

Key generation:

Alice chooses a group G, an element $g \in G$, two subgroups A, B of G such that $ab = ba$ for any $a \in A$ and any $b \in B$, and two elements $b_1, b_2 \in A$. Alice publishes

$$(G, A, B, g, \Theta)$$

as her public key. Alice's private key is (b_1, b_2).

Signing the document m:

(1) Alice chooses two elements $a_1, a_2 \in A$, computes $x = b_1a_1ga_2b_2$, and then sends x to Bob.

(2) Bob chooses six elements $c_1, c_2, d_1, d_2, d_3, d_4 \in B$, computes $y = d_1c_1gc_2d_2$ and $w = d_3c_1xc_2d_4$, and then sends (y, w) to Alice.

(3) Alice chooses two elements $b_3, b_4 \in A$, computes $z = b_3a_1ya_2b_4$ and $u = b_1^{-1}wb_2^{-1}$, and then sends (z, u) to Bob.

(3) Bob computes $v = d_1^{-1}zd_2^{-1}$, and then sends v to Alice.

(4) Alice computes $e = b_3^{-1}vb_4^{-1}$ and sends Bob $S = \Theta(me)$.

Verification:

(1) Bob computes $e' = d_3^{-1}ud_4^{-1}$

(2) Bob computes $S' = \Theta(me')$.

(3) Bob accepts S as a valid signature of Alice's for m if $S' = S$. Otherwise, he rejects it.

Proof of why the above verification works:
Since we already have known that $e' = e$, indeed then $S' = S$.

The shield Sibert-Dehornoy-Girault-like authentication protocol

Based on our shielded key exchange protocol 1 and the idea setting up an authentication protocol given by Sibert *et al* in [49] we then have the following authentication protocol. One also can obtain an analogous protocol based on our shielded key exchange protocol 2.

Here Alice is the prover and Bob the verifier.

Key generation:

Alice chooses a group G, an element $g \in G$, two subgroups A, B of G such that $ab = ba$ for any $a \in A$ and any $b \in B$, four elements $a_1, a_2, b_1, b_2 \in A$, and a collision free hash function $\Theta : G \to \{0,1\}^k$ where k is a positive integer large enough such that $\{0,1\}^k$ can cover all the message. Alice computes $x = b_1 a_1 g a_2 b_2$. Alice publishes

$$(G, A, B, g, x, \Theta)$$

as her public key. Alice's private key is (b_1, b_2).

Authentication:

(1) Alice selects two element $c_1, c_2 \in B$, and sends Bob the commitment $z = \Theta(c_1 a_1 g a_2 c_2)$.

(2) Bob chooses a random bit h and sends it to Alice.

(3) If $h = 0$, then Alice computes $u = b_1^{-1} c_1$, $v = c_2 b_2^{-1}$, and sends (u, v) to Bob and Bob checks if the equality $z = \Theta(uxv)$.

(4) If $h = 1$, then Alice computes $u = c_1 a_1$, $v = a_2 c_2$, and sends (u, v) to Bob and Bob checks if the equality $z = \Theta(ugv)$.

Proof of why the above verification works:

If Alice knows a_1, a_2 and answers correctly, she is accepted by Bob: for $h = 0$, since b_1, b_2 commute with c_1, c_2 respectively, we have

$$\begin{aligned} \Theta(uxv) &= \Theta(b_1^{-1} c_1 x c_2 b_2^{-1}) \\ &= \Theta(b_1^{-1} c_1 b_1 a_1 g a_2 b_2 c_2 b_2^{-1}) \\ &= \Theta(c_1 a_1 g a_2 c_2) \\ &= z \end{aligned}$$

While, for $h = 1$, since $v = ca$ we have

$$\begin{aligned} \Theta(uxv) &= \Theta(a_1 c_1 g a_2 c_2)) \\ &= \Theta(c_1 a_1 g c_2 a_2) \\ &= z \end{aligned}$$

One can see that if Alice want to cheat by sending a correct answer in both cases: in the case $h = 0$, it suffices that Alice has to have gussied in advance that $h = 0$ and then had created the commitment $z = \Theta(uxv)$ with $u = c_1$ and $v = c_2$; and in the case $h = 1$, it suffices that Alice has to have gussied in advance that $h = 1$ and then had created the commitment $z = \Theta(ugv)$ with $u = c_1$ and $v = c_2$. But a cheater cannot choose his commitment so as to answer correctly in both cases: if he anticipates $h = 0$, the probability of answering correctly for $h = 1$ is negligible, and, symmetrically, if he anticipates $h = 1$, the probability of answering correctly for $h = 0$ is negligible. So, globally, a cheater has no more than 0.5 chance to be accepted. Thus, by repeating the exchanges l times, we can make the probability that a cheater be accepted as small as $1/2^l$.

3 Platform group and parameters

3.1 Braid groups

We suggest that the infinite nonabelian braid groups B_n with $n \geq 12$ can be taken as the platform groups for the protocols in the above section where B_n is defined by the following presentation.

Definition 3.1 The n-th braid group has a presentation as the following:

$$B_n = \langle \sigma_1, \cdots, \sigma_{n-1} | \sigma_i \sigma_j = \sigma_j \sigma_i, \sigma_{i+1} \sigma_i \sigma_{i+1} = \sigma_i \sigma_{i+1} \sigma_i, 1 \leq i \leq n-1, |i-j| > 1, \rangle$$

where $\sigma_1, \sigma_1, \cdots, \sigma_{n-1}$ are called the Artin generators of B_n, and each element of B_n is called an n-braid. For more details of the fundamental facts of Braid groups we refer the reader to [4, 15].

Denote B_n^+ the submonoid generated by $\sigma_1, \sigma_1, \cdots, \sigma_{n-1}$ and call each element of B_n^+ a positive braid. Let Δ_n denoted the positive braid inductively defined by

$$\Delta_1 = 1,\ \Delta_2 = \sigma_1\Delta_1,\ \cdots,\ \Delta_{i+1} = (\sigma_1 \cdots \sigma_i)\Delta_i, \quad 1 \leq i \leq n$$

In particular, Δ_n is called the fundamental braids and denoted as $\Delta := \Delta_n$.

For $u, v \in B_n$ we denote $v \leq w$ if and only if there exist positive braids $\alpha, \beta \in B_n^+$ such that $w = \alpha v \beta$. Obviously $\leq$ is a partial ordering relation on the set of all elements of B_n. An element $\alpha \in B_n$ is then said to be a canonical factor if $\alpha \leq \Delta$.

A factorization $\gamma = \alpha\beta$ of a positive braid γ into a canonical factor α and a positive braid β is said to be *left-weighted* if and only if α has the maximal length among all such decompositions. Similarly, one can define the idea of a *right-weighted* factorization. For any braid $\omega \in B_n$, notation $\sup \omega$ is the greatest $i \in \mathbb{Z}$ with $\Delta^i \leq \omega$, and the notation $\inf \omega$ is the smallest $i \in \mathbb{Z}$ with $\omega \leq \Delta^i$. Now, every braid $\alpha \in B_n$ can be written uniquely as

$$\alpha = \Delta^r W_1 \cdots W_s$$

where $r = \inf\omega$, $s = \sup\omega - \inf\omega$ and each W_i are canonical factors such that $W_i W_{i+1}$ is left-weighted for $1 \leq i < s$ (see [20, 16, 30]). This expression of α in the above is called the Δ-*normal form* of α with *canonical length* s. There are three facts [30] (also see [17, 16]) about the computation complexities of Δ-normals of n-braids.

- Let α be a word on $\{\sigma_1, \sigma_2, \cdots, \sigma_{n-1}\}$ with word length l. Then the Δ-normal form of α can be computed in time $O(l^2 n \log n)$.
- Let $\alpha = \Delta^r W_1 \cdots W_p$ and $\gamma = \Delta^t U_1 \cdots U_q$ be the Δ-normal forms of n-braids α and γ , respectively. Then one can compute the Δ-normal form of $\alpha\gamma$ in time $O(pqn \log n)$.
- If $\Delta^r W_1 \cdots W_p$ is the Δ-normal form of an n-braid α, then one can compute the Δ-normal of α^{-1} in time $O(pn)$.

Given a braid group B_n, let

$$LB_n = \langle \sigma_1, \sigma_2, \ldots, \sigma_{\lfloor \frac{n}{2} \rfloor - 1} \rangle$$

and

$$RB_n = \langle \sigma_{\lfloor \frac{n}{2} \rfloor + 1}, \sigma_{\lfloor \frac{n}{2} \rfloor + 2}, \ldots, \sigma_{n-1} \rangle$$

be the subgroups of B_n generated by $\{\sigma_1, \sigma_2, \ldots, \sigma_{\lfloor \frac{n}{2} \rfloor - 1}\}$ and $\{\sigma_{\lfloor \frac{n}{2} \rfloor + 1}, \sigma_{\lfloor \frac{n}{2} \rfloor + 2}, \ldots, \sigma_{n-1}\}$, respectively. Then by the definition of B_n, we have $ab = ba$ for any $a \in LB_n$ and any $b \in RB_n$. We call LB_n the *left half subgroup* of B_n and RB_n the *right half subgroup* of B_n.

For a braid group B_n with $n \geq 6$, by a result of Collins [12] there is a subgroup of B_n of the following form

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

such that G_i is isomorphic to the direct product $F_2 \times F_2$ with F_2 the free group of rank 2.

3.2 Presentations of Mihailova subgroups of B_n

Since the group H defined by Presentation C in [53] is generated by two elements t, u and the the subgroups

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

of B_n with $n \geq 6$ in §3.1 is isomorphic to the group $F_2 \times F_2$, we now can apply Theorem 3.3 of [53] to present an explicit countable presentation for Mihailova subgroup $M_{G_i}(H)$ of G_i. To do so we introduce some notations as follows.

If a relation R_j in Presentation D in [53] is of the form

$$R_j : R_j^{(l)}(u, t) = R_j^{(r)}(u, t)$$

with both $R_j^{(l)}(u,t)$ and $R_j^{(r)}(u,t)$ being words on the set $\{u,t,u^{-1},t^{-1}\}$ then we denote

$$S_{ij}=(R_j^{(r)}(\sigma_i^2,\sigma_{i+1}^2))^{-1}R_j^{(l)}(\sigma_i^2,\sigma_{i+1}^2)$$

by replacing all occurrences of u with σ_i^2 and all occurrences of t with σ_{i+1}^2, and denote

$$T_{ij}=(R_j^{(r)}(\sigma_{i+3}^2,\sigma_{i+4}^2))^{-1}R_j^{(l)}(\sigma_{i+3}^2,\sigma_{i+4}^2)$$

by replacing all occurrences of u with σ_{i+3}^2 and all occurrences of t with σ_{i+4}^2.

In Theorem 1.1 of [6], we let $k=2$ and ϕ be the isomorphism sending the group $F_2\times F_2$ with F_2 generated by (x_1,x_2) to the subgroup G_i with $1\leq i\leq n-5$ and $n\geq 6$ defined by

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

Therefore, the generators of the presentation in Presentation D of [53] are $d_1=\sigma_i^2\sigma_{i+3}^2$, $d_2=\sigma_{i+1}^2\sigma_{i+4}^2$, $1T_{ij}=T_{ij}$, and $1S_{ij}=S_{ij}$, $j=1,2,\cdots,27$.

Clearly, one can check that $\mathrm{root}(S_{ij})=S_{ij}$ and $\mathrm{root}(T_{ij})=T_{ij}$, $j=1,2,\cdots,27$. Thus, by replacing each occurrence of u with $\sigma_i^2\sigma_{i+3}^2$ and each occurrence of t with $\sigma_{i+1}^2\sigma_{i+4}^2$ of each R_j we then have

$$r_{ij}=(R_j^{(r)}(\sigma_i^2\sigma_{i+3}^2,\sigma_{i+1}^2\sigma_{i+4}^2))^{-1}R_j^{(l)}(\sigma_i^2\sigma_{i+3}^2,\sigma_{i+1}^2\sigma_{i+3}^2),\quad j=1,2,\cdots,27$$

where r_{ij} is defined as r_i in the the presentation given in Theorem 1.1 [6].

Finally, by Theorem 1.1 [6] we then have an explicit countable presentation with 56 generators for Mihailova subgroup $M_{G_i}(H)$ of B_n with $n\geq 6$ as the following.

Presentation D

56 generators:

$$\sigma_i^2\sigma_{i+3}^2,\ \sigma_{i+1}^2\sigma_{i+4}^2,\ S_{ij},\ T_{ij},\quad j=1,2,\cdots,27$$

Countable number of relators:

$$S_{ij}^{-1}(\delta^{-1}S_{ik}^{-1}r_{ik}^{-1}\delta)^{-1}S_{ij}(\delta^{-1}S_{ik}^{-1}r_{ik}^{-1}\delta),\quad T_j^{-1}(\delta^{-1}S_{ik}^{-1}r_{ik}^{-1}\delta)^{-1}T_j(\delta^{-1}S_{ik}^{-1}r_{ik}^{-1}\delta)$$
$$S_{ij}^{-1}(\delta^{-1}T_{ik}^{-1}r_{ik}^{-1}\delta)^{-1}S_{ij}(\delta^{-1}T_{ik}^{-1}r_{ik}^{-1}\delta),\quad T_{ij}^{-1}(\delta^{-1}T_{ik}^{-1}r_{ik}^{-1}\delta)^{-1}T_{ij}(\delta^{-1}T_{ik}^{-1}r_{ik}^{-1}\delta)$$
$$T_{ij}^{-1}r_{ij}^{-1}T_{ij}r_{ij},\ S_{ij}^{-1}r_{ij}^{-1}S_{ij}r_{ij},\quad j,k=1,2,\cdots,27$$

where $\delta\in\langle\sigma_i^2,\sigma_{i+1}^2\rangle\cup\langle\sigma_{i+3}^2,\sigma_{i+4}^2\rangle$.

For being used in setting up a public cryptograph mechanism in the following sections we give the details of the descriptions of all the generators S_{ij}, $j=1,2,\cdots,27$ in Presentation D as follows. We point out that one can obtain all the descriptions of generators T_{ij} in Presentation D 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 S_{ij}, $j=1,2,\cdots,27$.

S_{i1}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{12})^{-1}$
$\sigma_{i+1}^{-12}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i2}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10})^{-1}$
$\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i3}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8)^{-1}$
$\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i4}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6)^{-1}$

$\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i5}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4)^{-1}$
$\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i6}: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^{-1}$
$\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i7}: $(\sigma_i^2\sigma_{i+1}^4\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{12})^{-1}$
$\sigma_{i+1}^{-12}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i8}: $(\sigma_i^2\sigma_{i+1}^6\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10})^{-1}$
$\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

S_{i9}: $(\sigma_i^2\sigma_{i+1}^8\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8)^{-1}$
$\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,10}$: $(\sigma_i^2\sigma_{i+1}^{10}\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^9$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6)^{-1}$
$\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,11}$: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^{-1}$
$\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,12}$: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^{-1}$
$\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,13}$: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{12})^{-1}$
$\sigma_{i+1}^{-12}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,14}$: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10})^{-1}$
$\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,15}$: $(\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8)^{-1}$
$\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2$

$S_{i,16}$: $(\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{20}\sigma_i^4\sigma_{i+1}^{-20}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{20}\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}\sigma_i^{-4}\sigma_{i+1}^{-20}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{20}\sigma_i^4\sigma_{i+1}^{-20}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6$

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

$S_{i,18}$: $(\sigma_i^{-4}\sigma_{i+1}^{-12}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{12}\sigma_i^4\sigma_{i+1}^{-12}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4$
$\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-18}\sigma_i^2$
$\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{20}\sigma_i^4\sigma_{i+1}^{-20}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{20}(\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2)^2$
$\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$(\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2)^{-2}\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^2\sigma_{i+1}^2\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-18}\sigma_i^2$
$\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{20}\sigma_i^4\sigma_{i+1}^{-20}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{20}(\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2)^3$
$\sigma_i^{-4}\sigma_{i+1}^{-12}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{12}\sigma_i^4\sigma_{i+1}^{-12}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}$

$S_{i,19}$: $(\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}$
$\sigma_i^{-4}\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$

$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$
$\sigma_i^{-4}\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^6\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^6\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16}$
$\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$

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

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

$S_{i,22}$: $(\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^4$
$\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8\sigma_i^{-4}\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4$
$(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^3\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^3$
$\sigma_i^{-4}\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8$
$(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^4\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$

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

$S_{i,24}$: $(\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^6$
$\sigma_i^{-4}\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8$
$\sigma_i^{-4}\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^4\sigma_i^4\sigma_{i+1}^{-4}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^4(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^5$
$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^5$
$\sigma_i^{-4}\sigma_{i+1}^{-8}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^8\sigma_i^4\sigma_{i+1}^{-8}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^8\sigma_i^{-4}\sigma_{i+1}^{-10}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{10}\sigma_i^4\sigma_{i+1}^{-10}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{10}$
$(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^6\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$

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

$S_{i,26}$: $(\sigma_{i+1}^{-4}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{18}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^8$
$(\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2)^3(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^7$

$\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2)^{-1}$
$\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14}(\sigma_i^{-4}\sigma_{i+1}^{-14}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{14}\sigma_i^4\sigma_{i+1}^{-14}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{14})^7$
$\sigma_i^{-4}\sigma_{i+1}^{-6}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{6}\sigma_i^4\sigma_{i+1}^{-6}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{6}(\sigma_i^{-4}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^2\sigma_i^4\sigma_{i+1}^{-2}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2)^3$
$(\sigma_i^{-4}\sigma_{i+1}^{-16}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{16}\sigma_i^4\sigma_{i+1}^{-16}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^{16})^8\sigma_i^{-4}\sigma_{i+1}^{-18}\sigma_i^2\sigma_{i+1}^2\sigma_i^{-2}\sigma_{i+1}^{18}\sigma_i^4\sigma_{i+1}^{-18}\sigma_i^{-2}\sigma_{i+1}^{-2}\sigma_i^2\sigma_{i+1}^2$

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

Now, since the word problem of the group G defined by Presentation C is unsolvable, Mihailova's theorem[38] implies the following conclusion.

Theorem 3.2 *The membership problem for Mihailova subgroups $M_{G_i}(H)$ of B_n with $n \geq 6$ are unsolvable.*

For $n \geq 12$, one can see that Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ of B_n is also a subgroup of the left half subgroup LB_n, and Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$ of B_n is also a subgroup of the right half subgroup RB_n.

3.3 Requirements

We suggest that in the application of our proposed protocols in §2 the platform group G is chosen to be a braid group B_n with $n \geq 12$, and the subgroups A and B of G in the protocols is chosen to be the left half subgroup LB_n and the right half subgroup RB_n of B_n, respectively. Furthermore, there are two strategies of elements choosing as follows.

Strategy 1

The elements $a_1, a_2,\ b_1, b_2,\ b_3, b_4$ are chosen from LB_n, and the elements $c_1, c_2,\ d_1, d_2,\ d_3, d_4$ are chosen from RB_n.

Strategy 2

(1) The elements $a_1, a_2,\ b_3, b_4$ are chosen from LB_n, and the elements $c_1, c_2,\ d_3, d_4$ are chosen from RB_n.

(2) The elements b_1, b_2 should be chosen from the Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$, and the elements d_1, d_2 should be chosen from the Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$.

4 The security analysis

We first point out that in the application of Shpilrain and Ushakov's Ko-Lee-like protocol if Alice and Bob agree on the braid group B_n with $n \geq 12$, and subgroups A and B of B_n in the protocols being chosen to be the Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ and the Mihailova subgroup $M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$, respectively. Thus Alice's private keys are $a_1 \in M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ and $b_1 \in M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$, and Bob's private keys are $a_2 \in M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ and $b_2 \in M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$. However, its not necessary for the attacker to solve the membership problem and decomposition problem to find elements $a' \in\in M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ and $b' \in M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$ such that $a'gb' = a_1gb_1$ to obtain the shared key by computing $a'yb' = a'b_2ga_2b' = b_2a'gb'a_2 = b_2a_1gb_1a_2 = k$, since it is sufficient for her to attack the shared key by just solving the decomposition problem to find $a' \in LB_n$ and $b' \in RB_n$ such that $a'gb' = a_1gb_1$ and then obviously she also can obtain the shared key.

We only give the analysis of the security of key exchange protocol 1 since the analysis for key exchange protocol 2 is similar.

The security of Strategy 1 of key exchange protocol 1

First, in the exchange procedure of the protocol what the attacker Eve can have would be the braid group B_n, two subgroups LB_n, RB_n of B_n, and the following elements of B_n

$$g, x, y, z, w, u, v$$

where

$$x = b_1a_1ga_2b_2, y = d_1c_1gc_2d_2, z = b_3a_1d_1c_1gc_2d_2a_2b_4, w = d_3c_1b_1a_1ga_2b_2c_2d_4$$

and

$$u = d_3c_1a_1ga_2c_2d_4 = b_1^{-1}wb_2^{-1}, v = b_3a_1c_1gc_2a_2b_4 = d_1^{-1}zd_2^{-1}$$

Therefore, to attack the shared key Eve has to get rid of the shields b_1 and b_2 in x to have the element a_1ga_2 as well as the shields d_1 and d_2 in y to have the element c_1gc_2. Then she would try to solve the decomposition problem by finding elements a_1', a_2' in LB_n and c_1', c_2' in RB_n such that $a_1'ga_2' = a_1ga_2$ and $c_1'gc_2' = c_1gc_2$. Followed therefore she can obtain the shared key by computing

$$a_1'c_1'gc_2'a_2' = a_1'c_1gc_2b_2' = c_1a_1'ga_2'c_2 = c_1a_1ga_2c_2 = K_A = K_B$$

Clearly, for the pair (g, x) of elements g and x, what Eve is capable do is to solve the decomposition problem by finding elements $h_1, h_2 \in LB_n$ such that $h_1gh_2 = b_1a_1ga_2b_2 = x$. However, she couldn't guaranty that $h_1 = b_1a_1$ and $h_2 = a_2b_2$. Even though in the case that she does have $h_1 = b_1a_1$ and $h_2 = a_2b_2$, she clearly has no way to factorize them to obtain elements a_1, b_1, a_2, and b_2. So, she couldn't have the element a_1ga_2 from the equation $h_1gh_2 = b_1a_1ga_2b_2 = x$. Similarly, Eve also couldn't do anything over element pairs (y, g), (z, y), and (w, x).

Therefore, for Eve to launch the attack she may have to solve the decomposition problem with the elements pairs (w, u), and (z, v) with relations $w = b_1ub_2$ and $z = d_1vd_2$.

One can check that among all known attacks on the Braid based public key protocols there are three cryptanalysis methods of solving decomposition problem in braid groups: the Burau representation attack in [35], the Lawrence-Krammer representation attack in [10], and the length based attack in [39]. However, by using one of these methods, what the attacker Eve at most can do is only capable of finding elements $b_1', b_2' \in LB_n$ and $d_1', d_2' \in RB_n$ such that $b_1'ub_2' = b_1ub_2 = w$ and $d_1'vd_2' = d_1vd_2 = z$. However, in most cases, there are infinitely many such pair of elements $b_1', b_2' \in LB_n$ and $d_1', d_2' \in RB_n$. For example, let $n = 2m \geq 12$, g be an element of G represented by σ_m, a_1, a_2 be elements of the subgroup of LB_n generated by σ_1, σ_2, and $b_1', b_2' \in LB_n$ be such a pair with $b_1'ub_2' = w$. Then for any integer l the element b_0 represented by σ_4^l, the pair of elements $b_1'b_0, b_0^{-1}b_2' \in LB_n$ are also satisfying

$$b_1'b_0ub_0^{-1}b_2' = b_1'b_0d_3c_1a_1ga_2c_2d_4b_0^{-1}b_2' = b_1'd_3c_1a_1ga_2c_2d_4b_0b_0^{-1}b_2' = b_1'd_3c_1a_1ga_2c_2d_4b_2'b_1'ub_2' = w$$

since b_0 commutes with $d_3, c_1, a_1, g, a_2, c_2, d_4$. Therefore, Eve must verify if $b_1' = b_1$, $b_2' = b_2$, $d_1' = d_1$, and $d_2' = d_2$ since these equalities are what Eve has to have for her to get rid of the shields in x and y. Obviously Eve has no way to do the verifications.

The security of Strategy 2 of key exchange protocol 1 In case the quantum computation systems come to reality, we suggest that one takes the consideration of using Strategy 2 since in the analysis above, after the attacker Eve has found elements $b_1', b_2' \in LB_n$ and $d_1', d_2' \in RB_n$ such that $b_1'ub_2' = b_1ub_2 = w$ and $d_1'vd_2' = d_1vd_2 = z$, she must verify if $b_1' = b_1$, $b_2' = b_2$, $d_1' = d_1$, and $d_2' = d_2$. Hence she must solve the membership problem to decide if b_1', b_2' are elements of $M_{G_{\lfloor \frac{n}{2} \rfloor - 5}}(H)$ and if d_1', d_2' are elements of $M_{G_{\lfloor \frac{n}{2} \rfloor + 1}}(H)$. These are definitely impossible since the two subgroups enjoy unsolvable subgroup membership problem and hence the protocol is secured against the quantum computational attack.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public-key cryptography. Math. Res. Lett. 6(1999), 287-291.

[2] I. Anshel, M. Anshel, B. Fisher, New key agreement protocols in braid group cryptography, in NACCACHE D. (ED.): Topics in CryptologyCCT-RSA, San Francisco, CA, USA, 8C12 April 2001, (LNCS, 2020), 13C27.

[3] I. Anshel, M. Anshel, D. Goldfeld, Non-abelian key agreement protocols, Discrete Appl. Math., 130(2003), 3C12.

[4] J. S. Birman, Braids links and mapping class groups, Annals of Math. Study 82, Princeton University Press, 1974.

[5] W. W. Boone, The word problem, Annals of Mathematics, 70(2)(1959), 207-265.

[6] O. Bogopolski, and E. Ventura, A recursive presentation for Mihailova's subgroup, Groups, Geometry, and Dynamics, 4(3)(2010), 407-417.

[7] V.V. Borisov, Simple examples of groups with unsolvable word problems, Math. Notes, 6(1969), 768-775 (Mat. Zametki, 6(1969), 521-532, in Russian).

[8] G.S. CIJTIN, An associative calculus with an insoluble problem of equivalence, Trudy Mat. Inst. Steklov, 52 (1957), 172-189.

[9] J. C. Cha, K.H. Ko, S. Lee, J.W. Han, J.H. Cheon, An efficient implementation of braid groups, in BOYD C. (ED.): Advances in Cryptology, ASIACRYPT 2001, Gold Coast, Australia, 9-13 December 2001, (LNCS, 2248), 144-156.

[10] J. H. Cheon and B. Jun, A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem, in BONEH D. (ED.): Advances in Cryptology-CRYPTO 2003, Santa Barbara, CA, USA, 17-21 August 2003, (LNCS, 2729), 212-225.

[11] M. Chiswell, D.J. Collins and J. Huebschmann, Aspherical group presentation, Math. Z., 178 (1981), 1-36.

[12] D. J. Collins, Relations among the squares of the generators of the braid group, Invent. Math., 117(1994), 525-530.

[13] D. J. Collins, A simple presentation of a group with unsolvable word problem, Illnois J. Math., 30(2)(1986), 230-234.

[14] P Dehornoy, Braid-based cryptography, Contemp. Math., 360(2004), 5-33.

[15] P Dehornoy, Using shifted conjugacy in braid-based cryptography, Arxiv ePrint Archive, Report 0609091v1, http://arxiv.org/abs/cs/0609091.

[16] E. A. Elrifai and H. R. Morton, Algorithms for positive braids, Quarterly Journal of Mathematics, 45(1994), 479-497.

[17] D. Epstein, J. Cannon, D. Holt, S. Levy, M. Paterson and W. Thurston, Word processing in groups, Jones and Bartlett, 1992.

[18] N. Franco and J. Gonzales-Meneses, Conjugacy problem for braid groups and Garside groups, J. Algebra, 266(2003), 112-132.

[19] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, Probabilistic solutions of equations in the braid group, Advances in Applied Mathematics 35(2005), 323-334.

[20] F. A. Garside, The braid group and other groups, Quarterly Journal of Mathematics, 20(1969), 235-254.

[21] D. Garber, S. Kaplan, M. Teicher, B. Tsaban, U. Vishne, Length-based conjugacy search in the Braid group, Contemp. Math., Amer. Math. Soc. 418(2006), 75-87.

[22] V. Gebhardt, A new approach to the conjugacy problem in Garside groups, J. Algebra, 292(1)(2005), 282-302.

[23] F.J. Grunewald, On some groups which cannot be finitely presented, J. London Math. Soc., 17(2)(1978), 427-436.

[24] A. Groch, D. Hofheinz, R. Steinwandt, A practical attack on the root problem in braid groups, Contemp. Math., 418(2006), 121-132.

[25] G. Higman, B. H. Neumann and H. Neumann, Embedding theorems for groups, J. London Math. Sco., 24(1949), 247-254.

[26] D. Hofheinz, R. Steinwandt, A practical attack on some braid group based cryptographic primitives, in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptography, in: PKC 2003 (Y. G. Desmedt, ed.), Lecture Notes Comp. Sc. 2567(2002), 187-198.

[27] J. Hughes, The left SSS attack on Ko-Lee-Cheon-Han-Kang-Park key agreement scheme in B45, Rump session Crypto 2000.

[28] J. Hughes, A linear algebraic attack on the AAFG1 braid group cryptosystem, in BATTEN L.M., SEBERRY J. (EDS.): Information Security and Privacy, 7th Australian Conf.-ACISP 2002, Melbourne, Australia, July 2002, (LNCS, 2384), 176-189.

[29] J. Hughes, A. Tannenbaum, Length-based attacks for certain group based encryption rewriting systems, Inst. for Mathematics and its applic. (Minneapolis MN) 2000, http://www.ima.umn.edu/preprints/apr2000/1696.pdf, or http://arxiv.org/abs/cs/0306032.

[30] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, New public-key cryptosystem using braid groups, Advances in cryptology—CRYPTO 2000 (Santa Barbara, CA), 166-183, Lecture Notes in Comput. Sci. 1880, Springer, Berlin, 2000.

[31] K. H. Ko, D. H. Choi, M. S. Cho, J. W. Lee, A new signature scheme using conjugacy problem, Cryptology ePrint Archive, Report 2002/168, http://eprint.iacr.org/2002/168.

[32] A. G. Kallka, Representation attacks on the braid Diffie-Hellman public key encryption, Appl. Algebra Eng. Commun. Comput., 17(3-4)(2006), 257-266.

[33] S. La, A. Chaturvedi, Authentication schemes using braid groups, Arxiv ePrint Archive, Report 0507066v1, http://arxiv.org/abs/cs/0507066.

[34] S. J. Lee, E. Lee, Potential Weaknesses of the Commutator Key Agreement protocol Based on Braid Groups. In: Advances in cryptology-Eurocrypt 2002, 14-28 (Lecture Notes Comp. Sc., vol. 2332) Berlin Heidelberg New York Tokyo: Springer 2002.

[35] E. Lee, and J. H. Park, Cryptanalysis of the public-key encryption based on braid groups, in BIHAM E. (ED.): Advances in Cryptology, EUROCRYPT 2003, Warsaw, Poland, 4-8 May 2003, (LNCS, 2656), 477-490.

[36] J. Longrigg and A. Ushakov, Cryptanalysis of shifted conjugacy authentication protocol, Arxiv ePrint Archive, Report 0708.1768, http://arxiv.org/abs/0708n1768

[37] S. Maffre, A Weak Key Test for Braid Based Cryptography, Designs, Codes and Cryptography, 39(3)(2006), 347-373.

[38] K. A. Mihailova, *The occurence problem for direct products of groups*, Dokl. Akad, Nauk SSSR 119,1958,1103-1105.Mat. Sb. (N.S.), 70(112:2)(1966), 241C251.

[39] A. D. Myasnikov, V. Shpilrain, and A. Ushakov, A Practical Attack on a Braid Group Based Cryptographic Protocol, Advances in Cryptology-CRYPTO 2005, Lecture Notes in Computer Science Volume 3621, 2005, 86-96.

[40] A. D. Myasnikov and A. Ushakov, Length based attack in braid groups, in PKC 2007, Lecture Notes in Computer Science, 4450(2007), 76-88.

[41] P. S. Novikov, On the algorithmic unsolvability of the word problem in group theory, Trudy Mat. Ins. Steklov, 44(1955), 143 pages, Translation in Amer. math. Soc. Transl, 9(2)(1958), 1-122.

[42] D. Ruinskiy, A. Shamir, B. Tsaban, Cryptanalysis of group-based key agreement protocols using subgroup distance functions, in PKC 2007, Lecture Notes Comp. Sc., 4450(2007), 61-75.

[43] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum ComputerSIAM J. Comput., 26:5(1997): 1484-1509

[44] V. Shpilrain and A. Ushakov, Thompson's group and public key cryptography, in ACNS 2005, Lecture Notes Comp. Sc., 3531(2005), 151-164.

[45] V. Shpilrain, A. Ushakov, An authentication scheme based on the twisted conjugacy problem,Proceeding ACNS'08 Proceedings of the 6th international conference on Applied cryptography and network security, Springer-Verlag, 2008, 366-372.

[46] V. Shiplrain, A. Ushakov, The conjugacy search problem in public key cryptography: unnecessary and insufficient, Appl. Alg. in Eng., Communi. and Comp., 17(3-4)(2006), 285-289.

[47] V. Shpilrain and G. Zapata, Combinatorial group theory and public key cryptography, Appl. Algebra Engrg. Comm. Comput. 17(2006), 291-302.

[48] V. Shpilrain and G. Zapata, Using the subgroup membership search problem in public key cryptography, Contemp. Math., Amer. Math. Soc., 418(2006), 169-179.

[49] H. Sibert, P. Dehornoy, M. Girault, Entity authentication schemes using braid word reduction, Discrete Applied Math. 154(2)(2006), 420-436.

[50] H. Tietze, $\ddot{U}$ber die topologischen invarianten mehrdimensionaler mannigfaltigkeiten, Monatsh, Math. Phys., 19(1908), 1-118.

[51] B. Tsaban, On an authentication scheme based on the root problem in the braid group, lanl.arXiv.org ePrint Archive, September 2005, Online available at http://arxiv.org/ps/cs.CR/0509059.

[52] B.C. Wang, Y.-P. Hu, Signature scheme based on the root extraction problem over braid groups, IET Inf. Secur., 3(2)(2009), 53C59.

[53] X. Wang, C. Xu, G. Li and H. Lin, Groups with two generators having unsolvable word problem and presentations of Mihailova subgroups, Cryptology ePrint Archive, Report 2014.528, http://eprint.iacr.org.

Xiaofeng Wang
School of Mathematics and Computational Science
Shenzhen University
Shenzhen City 518060, China wangxf@szu.edu.cn

Chen Xu
School of Mathematics and Computational Science
Shenzhen University
Shenzhen City 518060, China xuchen@tom.com