CRYPTANALYSIS OF THE SHPILRAIN-USHAKOV PROTOCOL FOR THOMPSON'S GROUP

FRANCESCO MATUCCI

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
matucci@math.cornell.edu

Abstract. This paper shows that an eavesdropper can always recover efficiently the private key of one of the two parts of the public key cryptography protocol introduced by Shpilrain and Ushakov in [9]. Thus an eavesdropper can always recover the shared secret key, making the protocol insecure.
2000 Mathematics Subject Classification: 68P25, 94A60, 20F10, 37E05
Key words and phrases: Decomposition Problem; Conjugacy Problem; Infinite Groups; Normal Form; Piecewise-Linear Homeomorphism.

1. Introduction

Recent advances in public key cryptography have underlined the need to find alternatives to the RSA cryptosystem. It has been proposed to use algorithmic problems in non-commutative group theory as possible ways to build new protocols. The *conjugacy search problem* was introduced in several papers as a generalization of the *discrete logarithm problem* in the research of a new safe encryption scheme. The former problem asks whether or not, given a group G and two elements $a, b \in G$ that are conjugate, we can find at least one $x \in G$ with $a^x := x^{-1}ax = b$. It is thus important to look for a platform group G where this problem is computationally hard. Seminal works by Anshel-Anshel-Godlfeld [1] and Ko-Lee et al. [6] have proposed the braid group B_n on n strands as a possible platform group.

It has been observed that Thompson's group F and the braid groups B_n have some similarities. Belk proved in his thesis [2] that F and the braid groups have a similar classifying space. Loosely speaking, the elements of F appear as braids, but with merges and splits instead of twists (this representation of F uses *strand diagrams* which are introduced in [2]). Dehornoy defined in [4] a group of *parenthesized braids* which contains both F and B_n in a very natural way. However, for cryptographic purposes, F has still not proved to be a good platform. Kassabov and Matucci have proved in [5] that the simultaneous conjugacy problem is efficiently solvable, making it insecure to apply protocols based on the conjugacy problem.

Shpilrain and Ushakov in [9] have proposed using a particular version of the *decomposition problem* as a protocol and the group F as a platform.

The new problem is: given a group G, a subset $X \subseteq G$ and two elements $w_1, w_2 \in G$ with the information that there exist $a, b \in X$ such that $aw_1b = w_2$, find at least one such pair a, b. In this paper we show how to recover efficiently the shared secret key of this protocol.

The paper is organized as follows. In Section 2 and Section 3 we recall the protocol and give a description of Thompson's group F. In Section 4 we recall the choice of parameters proposed in [9]. In section 5 we give an efficient attack that always recovers the secret key. In Sections 6 and 7 we show another type of attack. In Section 8 we make some comments on possible generalizations of this protocol.

History and related works. The first attack on this protocol was announced by Ruinskiy, Shamir and Tsaban in November 2005 at the Bochum Workshop *Algebraic Methods in Cryptography*, showing that the paramaters given in [9] should be increased to have higher security of the system. Their attack was improved in other announcements and was finalized in [7] at the same time that this paper was written. Their attack describes a more general procedure which uses length functions. We remark that the same authors have been developing new techniques involving "subgroup distance functions" and that they applied them on the same protocol for F as a test case [8]. The approach of Ruinskiy, Shamir and Tsaban in their mentioned papers is heuristic, and its success rates are good but not 100%. Our approach is deterministic, and provably succeeds in all possible cases.

Acknowledgements. The author would like to thank Martin Kassabov, Boaz Tsaban and Vladimir Shpilrain for helpful discussions. The author would also like to thank Ken Brown and the referees for many helpful comments.

2. The Protocol

The protocol proposed in [9] is based on the *decomposition problem*: given a group G, a subset $X \subseteq G$ and $w_1, w_2 \in G$, find $a, b \in X$ with $aw_1b = w_2$, given that such a, b exist. Here is the protocol in detail:

Public Data. A group G, an element $w \in G$ and two subgroups A, B of G such that $ab = ba$ for all $a \in A$, $b \in B$.

Private Keys. Alice chooses $a_1 \in A$, $b_1 \in B$ and sends the element $u_1 = a_1wb_1$ to Bob. Bob chooses $b_2 \in B$, $a_2 \in A$ and sends the element $u_2 = b_2wa_2$ to Alice. Alice then computes the element $K_A = a_1u_2b_1 = a_1b_2wa_2b_1$ and Bob computes the element $K_B = b_2u_1a_2 = b_2a_1wb_1a_2$. Since A and B commute elementwise, $K = K_A = K_B$ becomes Alice and Bob's shared secret key.

Eavesdropper's Data. Eve has all the public data and the two elements u_1 and u_2, observed during Alice and Bob's exchange.

3. The Group F and the Subgroups A_s, B_s

Thompson's group F was introduced by R. Thompson while working on problems in logic. The standard introduction to F is [3]. One of Thompson's original definitions of F is the following: for $I = [0, 1]$ we define $PL_2(I)$ to be the group of piecewise linear homeomorphisms of the interval I with finitely many breakpoints such that:

- all slopes are integral powers of 2, and
- all breakpoints are in $\mathbb{Z}[\frac{1}{2}]$, the ring of dyadic rational numbers;

the product of two elements is given by the composition of functions. We thus define F to be the group $PL_2(I)$. F can also be described using the following presentation:

$$F = \langle x_0, x_1, x_2, \dots \mid x_n x_k = x_k x_{n+1}, \forall\, k < n \rangle.$$

This presentation has the advantage that the elements of F can be uniquely written in the following *normal form*

$$x_{i_1} \dots x_{i_u} x_{j_v}^{-1} \dots x_{j_1}^{-1}$$

such that $i_1 \leq \dots \leq i_u$, $j_1 \leq \dots \leq j_v$ and if both x_i and x_i^{-1} occur, then either x_{i+1} or x_{i+1}^{-1} occurs, too. Since $x_k = x_0^{1-k} x_1 x_0^{k-1}$ for $k \geq 2$, the group F is generated by the elements x_0 and x_1. The generators x_k of the infinite presentation can be represented as piecewise-linear homeomorphisms by shrinking the function x_0 shown in figure 1 onto the interval $[1 - \frac{1}{2^k}, 1]$ and extending it as the identity on $[0, 1 - \frac{1}{2^k}]$:

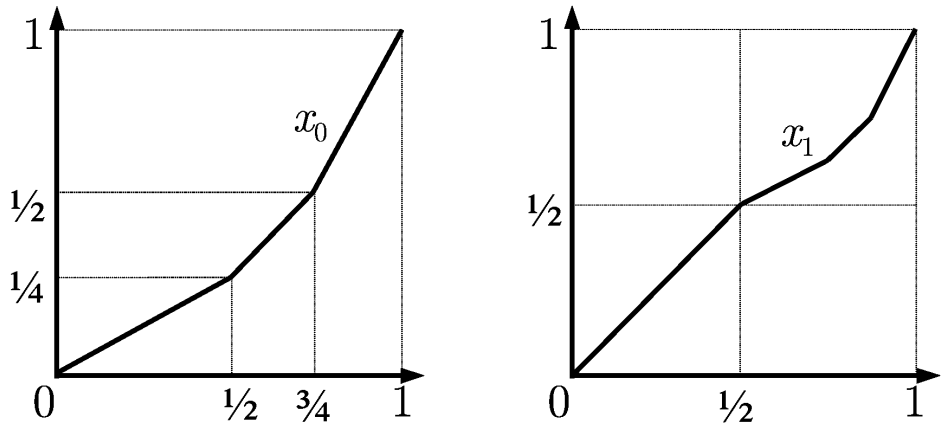

Figure 1. Two of the elements of the generating set of F.

We now introduce a notation which will be useful for the definition of the subgroups A and B. For every positive integer k we call

$$\varphi_k := 1 - \frac{1}{2^{k+1}}.$$

From the definition of x_k, we get

$$x_k^{-1}([\varphi_k, 1]) = [\varphi_{k+1}, 1] \subseteq \left[\frac{3}{4}, 1\right]$$

implying that, for $t \in [\varphi_k, 1]$, we have

$$\frac{d}{dt} x_0 x_k^{-1}(t) = x_0'(x_k^{-1}(t))(x_k^{-1})'(t) = 2 \cdot \frac{1}{2} = 1$$

which means $x_0 x_k^{-1}$ is the identity in the interval $[\varphi_k, 1]$. For any $s \in \mathbb{N}$, Shpilrain and Ushakov define in [9] the following sets

$$S_{A_s} = \{x_0 x_1^{-1}, \ldots, x_0 x_s^{-1}\}$$

and

$$S_{B_s} = \{x_{s+1}, \ldots, x_{2s}\}$$

and then define the subgroups $A_s := \langle S_{A_s} \rangle$ and $B_s := \langle S_{B_s} \rangle$. The previous argument immediately yields that that all elements of A_s commute with all elements of B_s (see figure 2), i.e.

Lemma 3.1 (Shpilrain-Ushakov [9])**.** *For every fixed $s \in \mathbb{N}$, $ab = ba$ for every elements $a \in A_s$ and $b \in B_s$.*

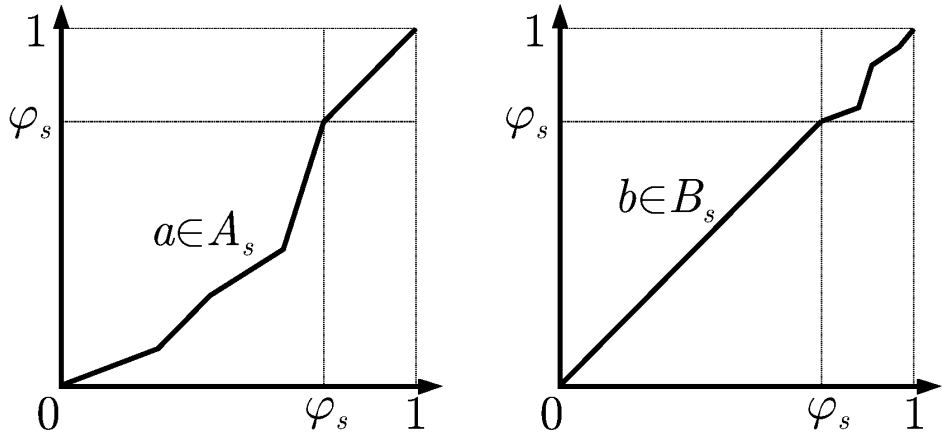

FIGURE 2. An example of an element of A_s and one of B_s.

Notation 3.2. For every dyadic number $d \in [0, 1]$ we denote by $PL_2([0, d])$ the set of functions in $PL_2(I)$ which are the identity on $[d, 1]$. Moreover, if we are given a piecewise linear map defined only on $[0, d]$ we will assume it is extended to $[0, 1]$ by defining it as the identity on $[d, 1]$. Similar remarks apply to $PL_2([d, 1])$.

Parts (i) and (iii) of the following Lemma are in [9], while part (ii) is a simple observation.

Lemma 3.3. *(i) A_s is the set of elements whose normal form is of the type*

$$x_{i_1} \dots x_{i_m} x_{j_m}^{-1} \dots x_{j_1}^{-1}$$

where $i_k - k < s$ and $j_k - k < s$, for all $k = 1, \dots, m$.

(ii) $B_s = PL_2([\varphi_s, 1])$.

(iii) Let $a \in A_s$ and $b \in B_s$ be such that their normal forms are

$$a = x_{i_1} \dots x_{i_m} x_{j_m}^{-1} \dots x_{j_1}^{-1}$$
$$b = x_{c_1} \dots x_{c_u} x_{d_v}^{-1} \dots x_{d_1}^{-1}.$$

Then the normal form of ab is

$$ab = x_{i_1} \dots x_{i_m} x_{c_1+m} \dots x_{c_u+m} x_{d_v+m}^{-1} \dots x_{d_1+m}^{-1} x_{j_m}^{-1} \dots x_{j_1}^{-1}.$$

Theorem 3.4 (Shpilrain-Ushakov [9])**.** *In Thompson's group F, the normal form of a given word w can be computed in time $O(|w| \log |w|)$, where $|w|$ is the length of the normal form in the generators $x_0, x_1, x_2, \dots$*

4. Suggested Parameters for the Encryption

We now illustrate briefly the choice of parameters proposed in [9]. Alice and Bob select an integer $s \in [3, 8]$ and an even integer $M \in [256, 320]$ uniformly and randomly. Morever, they also choose a random element $w \in \langle x_0, x_1, \dots, x_{s+2} \rangle$ with $|w| = M$, where $|w|$ is as in Theorem 3.4. The numbers s, M and the element w are now part of the the public data.

To proceed with the protocol described in Section 2, Alice chooses random elements $a_1 \in A_s, b_1 \in B_s$, with $|a_1| = |b_1| = M$, while Bob chooses random elements $a_2 \in A_s, b_2 \in B_s$, with $|a_2| = |b_2| = M$. Now they both compute the shared secret key:

$$K = a_1 b_2 w a_2 b_1.$$

Shpilrain and Ushakov remark that this choice of parameters gives a key space which increases exponentially in M, i.e., $|A_s(M)| \geq \sqrt{2}^M$, thereby making it difficult for Eve to perform a brute force attack.

5. Recovering the Shared Secret Key

We begin this section by providing the theoretical background for the attack. We will use the piecewise-linear point of view to understand why the attack works and then rephrase it combinatorially. We will now describe how Eve, by knowing the elements w, u_1, u_2, can always recover one of the two legitimate parties' private keys. She chooses whose key to crack, depending on whether the graph of w is above or below the point (φ_s, φ_s).

5.1. **Recovering Bob's Private Keys: $w(\varphi_s) \leq \varphi_s$.** Since $w(t) \leq \varphi_s$ for all $t \in [0, \varphi_s]$, we observe the following identity

$$u_2(t) = b_2 w a_2(t) = w a_2(t), \ \forall t \in [0, \varphi_s].$$

Therefore, Eve may apply w^{-1} to the left of both sides of the previous equation to obtain

$$w^{-1} u_2(t) = a_2(t), \ \forall t \in [0, \varphi_s]$$

and so $w^{-1}u_2 \in A_s B_s$ and

$$a_2(t) = \begin{cases} w^{-1}u_2(t) & t \in [0, \varphi_s] \\ t & t \in [\varphi_s, 1]. \end{cases}$$

Now Eve has the elements a_2, w and $u_2 = b_2 w a_2$ and she computes

$$b_2 = u_2 a_2^{-1} w^{-1}$$

thereby detecting Bob's private keys and the shared secret key K.

5.2. **Recovering Alice's Private Key: $w(\varphi_s) > \varphi_s$.** Since $w^{-1}(t) < \varphi_s$ for all $t \in [0, \varphi_s]$, we have

$$u_1^{-1}(t) = b_1^{-1} w^{-1} a_1^{-1}(t) = w^{-1} a_1^{-1}(t), \ \forall t \in [0, \varphi_s].$$

By applying the same technique as in the previous subsection Eve recovers a_1^{-1} and obtains that $u_1 w^{-1} \in A_s B_s$. Thus, she is able to detect a_1, b_1 and the shared secret key K. Alternatively, Eve observes

$$w^{-1} u_1(t) = w^{-1} a_1 w b_1(t) = b_1(t), \ \forall t \in [\varphi_s, 1]$$

and so

$$b_1(t) = \begin{cases} t & t \in [0, \varphi_s] \\ w^{-1}u_1(t) & t \in [\varphi_s, 1]. \end{cases}$$

5.3. **Outline of the attack.** We expand on the previous discussion to describe a combinatorial attack. Assume that Eve has the elements w, u_1, u_2.

(1) Eve writes the normal forms of $z_1 := u_1 w^{-1}$ and $z_2 := w^{-1} u_2$.
(2) By the previous discussion, either $z_1 \in A_s B_s$ or $z_2 \in A_s B_s$ (or both). She can detect which one using Lemma 3.3(i) and selects this z_i.
(3) She computes the A_s-part a_{z_i} of z_i.
(4) If $i = 1$, she computes $b_{z_1} := w^{-1} a_{z_1}^{-1} u_1$. If $i = 2$, she computes $b_{z_2} := u_2 a_{z_2}^{-1} w^{-1}$.
(5) Eve computes K from $u_1, u_2, a_{z_i}, b_{z_i}$.

The only point of this procedure which needs further explanation is (2). When we have the normal forms of z_1, z_2, we know that one of them is in $A_s B_s$. We write the normal form $z_i = x_{i_1} \dots x_{i_e} x_{j_f}^{-1} \dots x_{j_1}^{-1}$ and we look at the notation of Lemma 3.3(i): we need to find the the smallest index r in z_i such that either i_{r+1} or j_{r+1} does not satisfy the index condition in Lemma 3.3(i). To verify if $z_i \in A_s B_s$, we need to check whether it has the form described in Lemma 3.3(iii): we remove the first r letters and the last

r letters of z_i from the word and we lower all the indices of the remaining letters by r; if what remains is a word whose indices are in $\{s+2,\dots,2s\}$, then we have an element of B_s, otherwise $z_i \notin A_sB_s$. If $z_i \in A_sB_s$, then a_{z_i} will be the product of the first r elements of z_i and the last r ones.

5.4. **Complexity of the attack.** By Theorem 3.4 we know that computing normal forms can be done in time $O(M \log M)$, where M is the size of the inputs suggested in Section 4. Part (2) of the attack can be executed in time $O(M)$, by just reading the indices of the normal forms and finding when the relation of Lemma 3.3(i) breaks down. Finally, the last steps are just multiplications and then simplifications so they can again be performed in time $O(M \log M)$. Therefore, Eve can recover the shared secret key in time $O(M \log M)$.

Remark 5.1. The previous discussion shows that there is no need to pass from words to piecewise-linear functions and back. The attack can be performed entirely by using the combinatorial point of view which is used for encryption. The piecewise-linear point of view is necessary only to prove that the combinatorial attack works. We also remark that the complexity of the attack is independent of the parameter s.

6. Transitivity of A_s and B_s

The previous section showed how to recover the shared secret key of one of the two involved parties, based on whether the graph of w lies above or below the point (φ_s, φ_s). However, it is possible to find the shared secret key even in the cases not studied in the previous section. More precisely, it is possible to attack Alice's word in the case $w(\varphi_s) \leq \varphi_s$ and Bob's word in the case $w(\varphi_s) > \varphi_s$. We need a better description of the subroups A_s. If $s = 1$, we observe that $A_1 = \langle x_0 x_1^{-1} \rangle$ is a cyclic group. For larger values of s, A_s becomes the full group of piecewise linear homeomorphism on $[0, \varphi_s]$.

Lemma 6.1. $A_2 = PL_2\left([0, \frac{7}{8}]\right)$.

Proof. Let a, b be the two generators of $PL_2([0, \frac{1}{2}])$ shown in figure 3. One sees that $a = x_0^2 x_1^{-1} x_0^{-1}$ and that $b = x_0 x_1^2 x_2^{-1} x_1^{-1} x_0^{-1}$ and so a conjugation of $PL_2([0, \frac{1}{2}])$ by x_0^2 yields $PL_2([0, \frac{7}{8}]) = \langle x_0^2 a x_0^{-2}, x_0^2 b x_0^{-2} \rangle$. By Lemma 3.3 we have

$$x_0^2 a x_0^{-2} = x_0^4 x_1^{-1} x_0^{-3} \in A_2$$
$$x_0^2 b x_0^{-2} = x_0^3 x_1^2 x_2^{-1} x_1^{-1} x_0^{-3} \in A_2$$

so that $PL_2([0, \frac{7}{8}]) \subseteq A_2$. The other inclusion is obvious. □

Theorem 6.2. *$A_s = PL_2([0, \varphi_s])$, for every $s \geq 2$.*

Proof. A straightforward computation shows that

$$x_0^{-1} PL_2([0, \varphi_s]) x_0 = PL_2([0, \varphi_{s+1}]), \forall s \geq 0.$$

Therefore $A_2 = PL_2([0, \varphi_2])$ and the definition of A_s imply

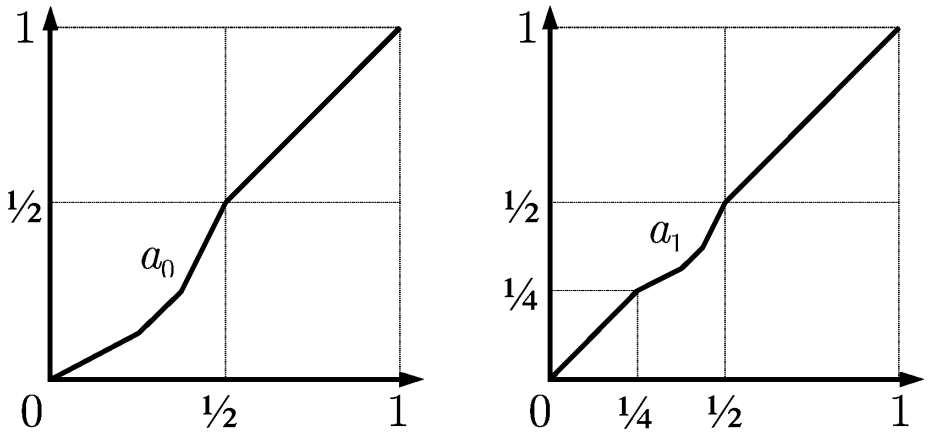

FIGURE 3. The two standard generators for $PL_2([0, \frac{1}{2}])$.

$$PL_2([0, \varphi_s]) = x_0^{s-2} A_2 x_0^{2-s} \subseteq A_s \subseteq PL_2([0, \varphi_s])$$

therefore implying that $A_s = PL_2([0, \varphi_s])$. □

Corollary 6.3. *$A_s \cong B_s \cong F$, for every $s \geq 2$.*

The previous Theorem and Lemma 2.5 in [5] yield the following corollaries:

Corollary 6.4 (Transitivity of A_s)**.** *For any $t_1, t_2 \in \mathbb{Z}\left[\frac{1}{2}\right] \cap [0, \varphi_s]$ we can construct an $a \in A_s$ with $a(t_1) = t_2$.*

Corollary 6.5 (Extendability of A_s)**.** *Let $t_0 \in \mathbb{Z}\left[\frac{1}{2}\right] \cap [0, \varphi_s]$ and $\bar{a}(t) = a|_{[0,t_0]}$ for an element $a \in A_s$. Assume we know $\bar{a}$, but that we do not know a. Then we can construct an $a_\sigma \in A_s$ such that $a_\sigma(t) = \bar{a}(t)$ for all $t \in [0, \varphi_s]$.*

Remark 6.6. The analogues of the last two corollaries are true for the interval $[\varphi_s, 1]$ and B_s too.

7. Using Transitivity to Attack the Shared Secret Key

With the new description of A_s and B_s given in section 6, it is now possible to attack the secret keys in the cases left open from section 5.

7.1. Attacking Alice's word for the case $w(\varphi_s) \leq \varphi_s$.

We have

$$u_1(t) = a_1 w(t), \forall t \in [0, \varphi_s],$$

thus

$$a_1(t) = u_1 w^{-1}(t), \forall t \in [0, w(\varphi_s)]$$

and so a_1 is uniquely determined in $[0, w(\varphi_s)]$. We apply corollary 6.5 to find an element $a_\sigma \in A_s$ such that $a_\sigma = a_1$ on the interval $[0, w(\varphi_s)]$. If we define

$$b_\sigma := w^{-1} a_\sigma^{-1} u_1$$

then we have that

$$b_\sigma(t) = w^{-1} a_\sigma^{-1} a_1 w(t) = w^{-1} w(t) = t, \forall t \in [0, \varphi_s]$$

Therefore $b_\sigma \in B_s$ and $a_\sigma w b_\sigma = u_1$ and so Eve can recover the shared secret key K by using the pair (a_σ, b_σ).

Remark 7.1. We observe that any extension of $a_1|_{[0,w(\varphi_s)]}$ to an element a_σ of $PL_2([0, \varphi_s])$ will yield a suitable element to attack Alice's key. Moreover, any element $a_1' \in A_s$ such that $a_1' w b_1' = u_1$, for some suitable $b_1' \in B_s$, will be an extension of $a_1|_{[0,w(\varphi_s)]}$.

7.2. **Attacking Bob's word for the case $w(\varphi_s) > \varphi_s$.** Eve considers $u_2^{-1} = a_2^{-1} w^{-1} b_2^{-1}$ and recovers a pair $(a_\sigma^{-1}, b_\sigma^{-1})$ to get the shared secret key in the same fashion of the previous subsection.

Remark 7.2. Both the techniques of this section have been carried out using the transitivity of A_s (Corollary 6.4). They can also be solved by using the analogue of Corollary 6.5 for B_s to get another pair (a_σ, b_σ) which can be used to retrieve the secret key.

8. Comments and Alternatives to the Protocol

This section analyzes possible alternatives and weaknesses of our methods. We observe that, if instead of $PL_2(I)$ we had used a larger group of piecewise linear homeomorphisms of the unit interval, the same technique would have worked, as long as the commuting subgroups A and B had disjoint supports. More generally, we can copy this idea if the given group G acts on some space and we have A, B with disjoint support. We will now see some examples of how this is possible.

8.1. **Choice of the subgroups A and B.** We recall the following result:

Theorem 8.1 (Kassabov-Matucci [5])**.** *Let $A = \langle a_1, \dots, a_m \rangle \leq F$ be a finitely generated subgroup. Then*

(i) There exists a dyadic partition of $[0,1] = I_1 \cup \ldots \cup I_n$ such that the centralizer $C_F(A) := \{f \in F \mid af = fa, \forall a \in A\}$ is a product of subgroups $C_1, \dots, C_n$, where $C_r \leq \{f \in F \mid f(t) = t, \forall t \notin I_r\}$. Moreover, we have

- *$C_r = PL_2(I_r)$ if and only if of $a_i|_{I_r} = id$, for all $i = 1, \dots, r$.*
- *$C_r \cong \mathbb{Z}$ if and only if $a_1|_{I_r}, \dots, a_m|_{I_r}$ have a common root on I_r.*
- *$C_r = 1$ if and only if there are $i \neq j$ such that $a_i|_{I_r}, a_j|_{I_r}$ have no common root on I_r.*

(ii) There exist two elements $g_1, g_2 \in F$ such that $C_F(A) = C_F(g_1) \cap C_F(g_2)$.

Going back to the protocol introduced in Section 2 we observe that, after we choose a finitely generated subgroup $A = \langle f_1, \ldots, f_m \rangle$, we are very restricted in our choice of the subgroup B. Since $B \leq C_F(A)$, we must make sure that the elements of B, when restricted to I_r, are powers of common roots of the a_i's, if at least one a_i is non-trivial on I_r. This gives a tight restriction on the subgroup B whose support is essentially disjoint from that of A, except in the intervals where they all are powers of a common root. An attack similar to that of Section 5 can thus be applied on each interval I_r: if their supports are disjoint on I_r, we can act as before, otherwise elements of A and B are powers of a common root on I_r.

With more general commuting subgroups, the attack of Section 5 does not immediately give either of the two keys. However, the discussion above suggests that the choice of A and B must be done much more carefully in order to avoid similar attacks.

8.2. **Alternative Protocol and Attacks.** Ko-Lee et al. [6] introduced a slightly different protocol based on the decomposition problem (They worked with braid groups, but we will apply their protocol to Thompson's group). In their protocol, Alice picks $a_1, a_2 \in A$ and sends $u_1 = a_1 w a_2$ to Bob, while Bob chooses $b_1, b_2 \in B$ and sends $u_2 = b_1 w b_2$ to Alice. We can still attempt to solve this new protocol, by again dividing the problem into various cases. We assume that we use the same subgroups A_s and B_s and we work in the case $w(\varphi_s) \leq \varphi_s$ to show how to attack the private keys of Bob. We apply the analogue for B_s of Corollary 6.4 and find a b_0 such that $b_0^{-1}(w^{-1}(\varphi_s)) = u_2^{-1}(\varphi_s) = b_2^{-1}w^{-1}(\varphi_s)$. We define

$$\begin{aligned} b_1' &= b_1 \\ b_2' &= b_2 b_0^{-1} \\ u_2' &= b_1' w b_2' \end{aligned}$$

so that $b_2'(w^{-1}(\varphi_s)) = w^{-1}(\varphi_s) > \varphi_s$. Thus we have

$$u_2'(t) = b_1'(t) w b_2'(t) = w b_2'(t), \forall t \in [0, w^{-1}(\varphi_s)]$$

hence

$$b_2'(t) = w^{-1} u_2'(t), \forall t \in [0, w^{-1}(\varphi_s)].$$

Thus b_2' is uniquely determined in $[0, w^{-1}(\varphi_s)]$. We apply corollary 6.5 for B_s to find a $b_{\sigma_2} \in B_s$ such that $b_{\sigma_2} = b_2'$ on $[0, w^{-1}(\varphi_s)]$ and we define

$$b_{\sigma_1} := u_2' b_{\sigma_2}^{-1} w^{-1}.$$

Thus

$$b_{\sigma_1}(t) = b_1' w b_2' b_{\sigma_2}^{-1} w^{-1}(t) = b_1'(t) = t, \forall t \in [0, \varphi_s]$$

therefore $b_{\sigma_1} \in B_s$. Therefore the pair $(b_{\sigma_1}, b_{\sigma_2})$ satisfies $u_2' = b_{\sigma_1} w b_{\sigma_2}$ and so Eve can recover the shared secret key K. A similar argument can be used to attack the element $a_1 w a_2$, with the transitivity results for A_s.

8.3. **A comment on the Alternative Protocol.** The weakness in the protocol discussed in the previous subsection arises from the fact that the chosen subgroups A_s and B_s are transitive on the intervals on which they act nontrivially. This suggests that a possible way to avoid such attacks is for A and B to be chosen to be not transitive on their support.

Remark 8.2. We observe that the attacks of section 7 and section 8 can be carried out in a fashion similar to that of Section 5, still producing a solution in polynomial time.

References

[1] I. Anshel, M. Anshel, and D. Goldfeld. An algebraic method for public-key cryptography. *Math. Res. Lett.*, 6(3-4):287–291, 1999.

[2] J.M. Belk. *Thompson's Group F*. PhD thesis, Cornell University, 2004. `arXiv:math.GR/0708.3609v1`.

[3] J.W. Cannon, W.J. Floyd, and W.R. Parry. Introductory notes on Richard Thompson's groups. *Enseign. Math. (2)*, 42(3-4):215–256, 1996.

[4] P. Dehornoy. The group of parenthesized braids. *Adv. Math.*, 205(2):354–409, 2006.

[5] M. Kassabov and F. Matucci. The simultaneous conjugacy problem in Thompson's group F. *preprint*. `arXiv:math.GR/0607167v2` .

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

[7] D. Ruinskiy, A. Shamir, and B. Tsaban. Length-based cryptanalysis: The case of Thompson's group. *Journal of Mathematical Cryptology*. to appear, `arXiv:cs/0607079v4`.

[8] D. Ruinskiy, A. Shamir, and B. Tsaban. Cryptanalysis of group-based key agreement protocols using subgroup distance functions. In *Proceedings of the 10th International Conference on Practice and Theory in Public-Key Cryptography PKC07*, volume 4450 of *Lecture Notes in Comput. Sci.*, pages 61–75. 2007.

[9] V Shpilrain and A. Ushakov. Thompson's group and public key cryptography. In *ACNS 2005*, volume 3531 of *Lecture Notes in Comput. Sci.*, pages 151–163. 2005.