Theoretical and Applied Informatics
Vol. 29 (2017), no. 1-2, pp. 14–24
DOI: 10.20904/291-2014

Cryptosystems using subgroup distortion

Indira Chatterji[1*] Delaram Kahrobaei[2†] Ni Yen Lu[3‡]

[1]Laboratoire J.A. Dieudonné de l'Université de Nice, France
[2]CUNY Graduate Center, PhD Program in Computer Science
[3]CUNY Graduate Center, City University of New York

Abstract In this paper we propose cryptosystems based on subgroup distortion in hyperbolic groups. We also include concrete examples of hyperbolic groups as possible platforms.

Keywordshyberbolic groups; symmetric key; distortion

Received 13 JUL 2017 **Revised** 02 FEB 2018 **Accepted** 02 FEB 2018

1 Introduction

Using algorithmic problems in non-commutative groups for cryptography is a fairly new but very active field for over a decade (see for instance [1]). In this paper we propose new cryptosystems using subgroup distortion. The algorithmic problems which are proposed for non-commutative group-based cryptography so far are: Conjugacy Search Problem, Endomorphism Search Problem, Word Choice problem, Membership search problem and Twisted Conjugacy Problem among others. There has not been yet any proposal to use the Geodesic Length Problem or Complexity of Distortion in Subgroups as we do in this paper. We propose a couple of symmetric cryptosystems based on these problems, and analyze their security.

The paper is organized as follows: in Sec. 2.1 we discuss the notion of subgroup distortion and in Sec. 2.2 we discuss the problem of finding the geodesic length of an element in a group in polynomial time, and explain how in a Gromov hyperbolic group this can be done in polynomial time. In Sec. 3 we explain two possible protocols based on subgroup distortion, and in Sec. 4 we give a few concrete examples of hyperbolic groups that can be used as platforms for the cryptosystems described in Sec. 3.

*E-mail: indira.chatterji@math.cnrs.fr
†E-mail: dkahrobaei@gc.cuny.edu
‡E-mail: nlu@gradcenter.cuny.edu

2 Background from group theory

2.1 Subgroup distortion

Let G be a finitely generated group and $S \subseteq G$ a finite generating set. Then for $g \in G$ the *word length associated to* S is given by

$$\ell_S(g) = \min\{n \in \mathbb{N} | g = s_1 \dots s_n, s_i \in S \cup S^{-1}\}. \tag{1}$$

For any two finite generating sets S, S' of G, there is a constant $C \geq 1$ such that, for any $g \in G$ one has

$$\ell_S(g) \leq C\ell_{S'}(g). \tag{2}$$

For $H < G$ a finitely generated subgroup, if $T \subset H$ is a generating set, then for any $h \in H$

$$\ell_{S\cup T}(h) \leq \ell_T(h). \tag{3}$$

Indeed, there are 'shortcuts' to the identity when one is allowed to use both elements from the generating set from G and H. Those shortcuts may no longer be there when we are restricted to the generating set of H and hence the other inequality is in general not true. The degree of failure of this inequality is used to define the distortion. In the rest of the paper we will assume that $T \subseteq S$, so that $S \cup T = S$.

Definition 1. Let G be a finitely generated group and $H < G$ be a finitely generated subgroup. The *distortion* of H in G is the function

$$\begin{aligned} \mathrm{Dist}_H^G : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \max\{\ell_T(h) \,|\, \ell_S(h) \leq n\}. \end{aligned} \tag{4}$$

Remark 2. Notice that *a priori* this function depends on the generating sets S and T for G and H, but two finite generating sets will give *equivalent* distortion functions D_1 and D_2. That D_1 and D_2 are equivalent means that there is a constant $C \geq 1$ satisfying

$$\frac{1}{C}D_2(\frac{n}{C}) \leq D_1(n) \leq CD_2(Cn) \tag{5}$$

for every $n \in \mathbb{N}$.

The following are very natural examples of finitely generated groups with distorted subgroups.

Example 3. The metabelian *Baumslag-Solitar group*:

$$G = \mathrm{BS}(1,2) = \langle a, b \,|\, aba^{-1} = b^2 \rangle. \tag{6}$$

If we take $H \simeq \mathbb{Z} = \langle b \rangle$, then one checks that for any $n \in \mathbb{N}$ one has

$$a^n b a^{-n} = a^{n-1}b^2a^{-(n-1)} = a^{n-1}ba^{-1}aba^{-(n-1)} = a^{n-2}b^4a^{-(n-2)} = \dots = b^{2^n}. \tag{7}$$

Hence $\ell_{\{b\}}(b^{2^n}) = 2^n$ whereas $\ell_{\{a,b\}}(b^{2^n}) = 2n + 1$ so that Dist_H^G is equivalent to an exponential.

Example 4. The integer *Heisenberg group*, given by

$$G = H_{\mathbb{Z}} = \langle a, b, c \,|\, [a, c] = [b, c] = e, [a, b] = c \rangle. \tag{8}$$

If we take $H \simeq \mathbb{Z} = \langle c \rangle$, this is the center of G and then one checks that for any $n \in \mathbb{N}$, using that $ab = cba$ and that $a^{-1}b^{-1} = cb^{-1}a^{-1}$ one has

$$\begin{aligned} a^n b^n a^{-n} b^{-n} &= a^{n-1} abb^{n-1} a^{-n} b^{-n} = a^{n-1} cbab^{n-1} a^{-n} b^{-n} \\ &= ca^{n-1} bab^{n-1} a^{-n} b^{-n} = ca^{n-1} b^2 cab^{n-2} a^{-n} b^{-n} \\ &= c^2 a^{n-1} b^2 ab^{n-2} a^{-n} b^{-n} = \cdots = c^n a^{n-1} b^n a^{-n+1} b^{-n} \\ &= \cdots = c^{2n} a^{n-2} b^n a^{-n+2} b^{-n} = \cdots = c^{n^2} b^n b^{-n} = c^{n^2} \end{aligned} \tag{9}$$

and hence $\ell_{\{c\}}(c^{n^2}) = n^2$ whereas $\ell_{\{a,b,c\}}(c^{n^2}) = 4n$ so that Dist_H^G is equivalent to a quadratic polynomial.

2.2 The Geodesic Length Problem

For a word w in the alphabet $X^{\pm 1}$ we denote by $|w|$ the length of w. The geodesic length of an element $g \in G$ relative to S, denoted by $\ell_S(g)$, is the length of a shortest word $w \in F(S)$ representing g, i.e., $\ell_S(g) = \min\{|w| \,|\, w \in F(S), w^\mu = g\}$. To simplify notation we write, sometimes, $\ell_S(w)$ instead of $\ell_S(w^\mu)$. A word $w \in F(S)$ is called geodesic in G relative to S, if $|w| = \ell_S(w)$. Here we give definitions of the Geodesic Problem and Geodesic Length Problem, (see [1] for more).

Definition 5 (The Geodesic Problem (GP))**.** Given a word $w \in F(S)$ find a geodesic (in G) word $\tilde{w} \in F(S)$ such that $w^\mu = \tilde{w}^\mu$.

The following is a variation of GP.

Definition 6 (The Geodesic Length Problem (GLP))**.** Given a word $w \in F(S)$ find $\ell_S(w)$.

A solution of GP gives a solution to the GLP because once one finds a geodesic representing a word, its length gives the length of the word. The GLP seems hard in general, and not much studied. In [2] it is shown that this problem is NP-complete in the free-metabelian group $S_{r,2}$. It is also known that in free groups or Right Angled Artin groups given by standard generating sets, there are fast algorithms for computing the geodesic length of elements [1]. In braid groups, or nilpotent groups, the computation of the geodesic length of elements is hard [1].

There are many groups of exponential growth where the Geodesic Problem is decidable in polynomial time, for example, hyperbolic groups (implicit in [3], see also Theorem 1 below) or metabelian Baumslag-Solitar group BS(1,n), [4]. Notice that, a priori, the Geodesic Problem is a bit harder than the Geodesic Length Problem: indeed, once one has found a geodesic, one automatically has its length, but knowing the length of a geodesic doesn't give the geodesic. However, according to Elder and Rechnitzer in [5], those two problems are polynomially reducible to each other, meaning that a polynomial time solution to one of the problems is equivalent to a polynomial time solution to the other one.

In the case where G is hyperbolic in the sense of Gromov, the following is easy:

Theorem 1. *Let G be a Gromov hyperbolic group, then the Geodesic Problem (hence the Geodesic Length Problem as well) is solvable in linear time.*

Proof. According to [6] (Part III.Γ.2), in a Gromov hyperbolic group a word w has a normal form which is a quasi-geodesic q. By stability of quasi-geodesics (see for instance Theorem 1.7 of [6]), the neighborhood of a quasi-geodesic between two points coincides with the neighborhood of a geodesic between those two points. In our case this means that there is a constant $K \geq 1$ and the neighborhood

$$N_K(q) = \{\gamma \in G \,|\, d(\gamma, q) \leq K\} \tag{10}$$

of q is contained in a neighborhood $N_L(g)$ of a geodesic g representing the word w, for some constant $L \geq 1$. Now, that neighborhood $N_L(g)$ has cardinality bounded by a constant times the length of the geodesic g, which is smaller than the length of w. One then enumerates all the paths in $N_K(q)$ to find the geodesic length. □

2.3 The membership search problem

Given G a finitely generated group, with a finite generating set S and H a subgroup with its own generating set T, one can ask the following.

Question 1 (Membership search problem)**.** *Given $h \in H$ expressed in terms of the generating set S, how long is it needed to express h in terms of elements of T?*

The difficulty of the membership search problem has been used in cryptography by Shpilrain and Zapata in [7], but here we will be needing examples in which the membership search problem is polynomial, see Lemma 7.

3 The Cryptosystems Using Subgroup Distortion

3.1 The protocol I: basic idea

Assume that Alice and Bob would like to communicate over an insecure channel. Here $G = \langle g_1, \ldots, g_l | R\rangle$ is a public group and $H = \langle t_1, \ldots, t_s\rangle \subset \langle g_1, \ldots, g_l\rangle = G$ is a secret subgroup of G, that is distorted and shared between only between Alice and Bob. We further assume that the geodesic length problem is polynomial both in G and H, and that the membership search problem is polynomial in H. Then:

1. Alice picks $h \in H$ with $\ell_H(h) = n$, expresses h in terms of generators of G with $\ell_G(h) = m \ll n$ and sends h to Bob.

2. Bob then converts h back in terms of generators of H and computes $\ell_H(h) = n$ in polynomial time to recover n.

3.1.1 Security

Although H is not known to anyone except to Alice and Bob and h being sent with length $m \ll n$ gives infinitely many possible guesses for the eavesdropper Eve, the security of the scheme is weak since Eve will have intercepted enough elements of H to generate H (one can think of the group $\mathbf{Z}$ of the integers, it is enough to intercept two relatively prime integers to generate the whole group).

3.2 The protocol I: secure version

We suggest making it impossible for Eve to tell which elements in the sent form belong to H by sending along h several elements that do not belong to H. To determine how Bob can tell which elements belong to H to retrieve the correct message we will consider below the subgroup membership problem and the random number generator.

3.2.1 Subgroup membership problem

Suppose we have a group in which the subgroup membership problem is solved efficiently then we will send some random words and the receiver first checks whether each word belongs to H and then computes its length.
Protocol: Let $G = \langle g_1, \cdots, g_l | R_G \rangle$ be a group that is known to the public and $H = \langle h_1, \ldots, h_s \rangle$ be a secret subgroup of G that is exponentially distorted. Assume that the subgroup membership problem in G efficiently solvable, and that as in Protocol I the word problem is polynomial in G, the geodesic length problem and the membership problems are both polynomial in H. Then:

1. Alice picks $h \in H$ with $\ell_H(h) = n$, expresses $h = g_1 \cdots g_m$ in terms of generators of G with $\ell_G(h) = m \ll n$. She randomly generates $a_0, \ldots, a_m \in G \setminus H$ and sends these words to Bob.

2. Since Bob knows the generating set for H, he find $h \in H$ (since he could check the subgroup membership problem efficiently) he only uses $h \in H$, in terms of generators of H and computes $\ell_H(g) = n$ in polynomial time according to our assumptions to recover n.

3.2.2 Random Number Generator

Suppose we have a random number generator and two parties that share the same random number generator and the same seed, they will get a same random sequence. We would like to use this idea but instead on groups.

This notion is possible if we are given a one-to-one correspondence between the countably infinite set of integers and a countably infinite group G. There is a natural ordering of elements in the group of integers and so if we are given a one-to-one correspondence with the infinite set of integers, it will impose this ordering on G. Generating m random numbers is then the same as generating m elements in group G. The advantage here is that given the same random number generator and the same seed, two parties would produce the same sequence of random numbers and by using the 'same ordering' in G, they would get the same sequence of random elements of G.

We will use the idea of random number generator for group in the protocol below.

Protocol: Let $G = D_1 * D_2 * \cdots * D_n$ where each D_i is a Gromov hyperbolic group that is known to the public. Alice and Bob share $H = \langle d, \ldots, d_s \rangle \subset D_1 \coloneqq \langle d_1, \ldots, d_l | R_1 \rangle$ which is an exponentially distorted hyperbolic subgroup of D_1 (and hence G), a one-to-one correspondance between $D_2 * \cdots * D_n$ and the integers, a random number generator and a way to choose a seed. (For example, they could use the date and time for the seed: 02032016123342 where 02-03-2016 is today date and 12:33:42pm is the current time of message being sent. They could also add to this the number sent by previous message).

1. Alice picks $h \in H$ with $\ell_H(h) = n$, expresses $h = d_1 \cdots d_m$ in terms of generators of D_1 with $\ell_G(h) = m \ll n$. She randomly generates a sequence of $(m+1)$ numbers from the random number generator and picks $a_0, \ldots, a_m$ that belong to $D_2 * \cdots * D_n$ that is in a one-to-one correspondence with the sequence of $(m+1)$ numbers. She then sends $a_0 d_1 a_1 d_2 \ldots d_m a_m$ to Bob (the a_i's are expressed in a fixed generating set for $D_2 * \cdots * D_n$).

2. Bob knows the random number generator and the seed so he knows which a_i's are sent along with h. He uses a_i's inverses to get back $h = d_1 \cdots d_m$. Since he also knows H, he converts h back in terms of generators of H and computes $\ell_H(g) = n$ in polynomial time according to Theorem 1 to recover n.

3.2.3 Security

The security of the scheme relies on the fact that:

- $H < G$ is not known to anyone except to Alice and Bob.
- Since h is sent with length $\ell_G(h) = m \ll n$, there are infinitely many guesses for Eve that are greater than m.
- For both protocols, only Bob can tell which elements sent in the form of h belong to H. For the second protocol, the random number generator and the seed are known to only Alice and Bob, so there is no way for Eve to tell which elements among $\{h, a_i\}$ belong to H to try to generate H.

3.3 The protocol II: basic idea

Let $G = \langle S | R_1 \rangle$ be a secret group that is only known only to Alice and Bob and that has polynomial geodesic length problem. Let $H = \langle T \rangle$ be a public distorted subgroup of G. Here T is a subset of S.

1. Alice wants to send a message $n \in \mathbb{N}$ to Bob. She picks $g \in G$ with $\ell_G(g) = n$. She then expresses $g = t_1 t_2 t_3 \cdots t_m$, where $m \gg n$ and $t_i \in T$ and sends to Bob.

2. Bob converts g back in terms of generators of G and by assumption computes its length in polynomial time to recover n.

3.3.1 Security

Although G is not known to anyone except Alice and Bob, the security of this scheme is not strong since the eavesdropper could potentially guess the value of n based on the upper bound m.

3.4 The protocol II: secure version

Instead of sending g with $\ell_G(g) = m \gg n$ we can embed H exp(exp) distorted in another group K so that we can transmit message of size $\leq \log n < m$. For the cryptosystem below, we need the following groups:

$$G = \langle g_1, \ldots, g_l | R_G \rangle, \tag{11}$$
$$H = \langle h_1, h_2, \ldots, h_k | R_H \rangle, \tag{12}$$
$$K = \langle k_1, \ldots, k_q | R_K \rangle, \tag{13}$$

where H is a distorted subgroup of G and embedded exp(exp) distorted in K. The group H is known to the public whereas G and K are known to only Alice and Bob.

1. Alice wants to send a message $n \in \mathbb{N}$ to Bob.
   (a) She picks $g \in G$ with $\ell_G(g) = n$, $g = g_1 g_2 \cdots g_n$.
   (b) Since H is distorted in G, there is $m > n$ with $\ell_H(g) = m$. Alice then expresses $g = h_1 h_2 \ldots h_m$, in terms of generators of H.
   (c) Since H is embedded exp(exp) distorted in K, there exist $p \lll m$ and $k_1, k_2, \ldots k_p$ in the generating set of K such that $g = k_1 k_2 \cdots k_p$.
   (d) Alice sends g in this form to Bob.
2. Bob will do the following:
   (a) He uses his knowledge of K and H and the fact H is exp(exp) in K to convert $g = k_1 k_2 \cdots k_p$ ($p \ll m$) to $g = h_1 h_2 \ldots h_m$.
   (b) Since he knows that H is distorted in G, he converts $g = h_1 h_2 \ldots h_m$ to $g = g_1 g_2 \ldots g_n$ back in terms of generators of G.
   (c) He then computes the length of h to recover n.

3.4.1 Security

The security of the scheme relies on the fact that finding the geodesic length problem in H for the eavesdropper is impossible due to the fact that:

- G and K are not known to anyone except to Alice and Bob.
- g is sent in terms of generators of K so there is no way for Eve to figure out H.
- With $\ell_K(g) = p \ll n$, there are infinitely many choices of numbers greater than p for guessing.

4 Possible platforms

For both protocols, Gromov hyperbolic groups seem to provide interesting platforms. Indeed, according to Theorem 1 the geodesic length problem is solvable in polynomial time. There are many examples of hyperbolic groups with exponentially distorted hyperbolic subgroups, see for instance [8] for geometric examples such as surface subgroups in fundamental groups of hyperbolic 3-manifolds, but we do not know about membership search problems there.

4.1 Free-by-cyclic platforms for protocol I

One possible weakness of Protocol I is that the public group G does not contain enough exponentially distorted subgroups H, so Eve could make a group theoretic search and find all the distorted subgroups. To avoid that problem, one could use hyperbolic groups which can be written as free-by-cyclic groups in infinitely many ways. Such groups are constructed in [9]. More precisely, the authors construct groups G which are hyperbolic, and have infinitely many homomorphisms to $\mathbb{Z}$, with free kernel. Given any such homomorphism, one has an expression $G = F_n(a_1, \ldots, a_n) \rtimes_\phi \langle t \rangle$, where the first factor is the free group on the generators $a_1, \ldots, a_n$, and ϕ is an automorphism of $F_n(a_1, \ldots, a_n)$ such that $ta_it^{-1} = \phi(a_i)$ for all i.

We fix one such $G = F_n(a_1, \ldots, a_n) \rtimes_\phi \langle t \rangle$ (including a choice of generators $a_1, \ldots, a_n, t$) as the public group G.

Now Alice and Bob together choose one of the (infinitely many) other homomorphisms of G to $\mathbb{Z}$, say $G = F_m(b_1, \ldots, b_m) \rtimes \langle s \rangle$ and take $H = F_m(b_1, \ldots, b_m) < G$.

Lemma 7. *The membership search problem for $H < G$ is solvable in polynomial time.*

Proof. Given a word $w = w(a_1, \ldots, a_n, t)$ a word in the public generators $a_1, \ldots, a_n, t$ of G, which represents an element $h \in H$, we need to show that there is a polynomial time algorithm to write h in terms of the generators $b_1, \ldots, b_m$ of H.

Since $G = F_n(a_1, \ldots, a_n) \rtimes_\phi \langle t \rangle = F_m(b_1, \ldots, b_m) \rtimes \langle s \rangle$, each a_i can be written as a word in $b_1, \ldots, b_m, s$. Thus by hyperbolicity, w can be changed into a word $v = v(b_1, \ldots, b_m, s)$ in linear time, and there is a constant K, depending only on H, such that $|v| \leq K|w|$.

The word v may have some powers of s and s^{-1}, but since it represents the element h of H, it has an expression u which is a word in just $b_1, \ldots b_m$. Applying Britton's lemma (see for instance Ch IV of [10]) to $u^{-1}v$, we see that v must have an innermost s, s^{-1} pair: i.e., v must have a subword of the form sxs^{-1} or $s^{-1}xs$, where x is a word in just $b_1, \ldots b_m$. Replace this subword with $\phi(x)$ or $\phi^{-1}(x)$ respectively, to get a word v_1 representing h with fewer s's and s^{-1}'s than v. Continuing this procedure, after finitely many steps we will have written down an expression for h in terms of $b_1, \ldots, b_m$. Since $ta_it^{-1} = \phi(a_i)$ for all i, applying the automorphism ϕ increases the length linearly only. Moreover, the number of steps is bounded above by the number of s, s^{-1} pairs, which is at most $|v|/2 < K|w|$. □

4.2 Exponential and Exp(exp) distortion for protocol II

We now provide concrete examples of hyperbolic groups with an exponentially and an exp(exp) distorted subgroup that could be used in protocol II (improved version). Those examples are a

particular case of the more general techniques developed in [11]. Here we describe a specific type which may fit our needs, although it is not clear that they have a fast enough membership search problem.

Let

$$G_1 \coloneqq \langle a_1, a_2, \ldots, a_{14}, t_1 | t_1^{-1} a_j t_1 = w_{1j} (1 \leq j \leq 14) \rangle \tag{14}$$

and

$$G_{14} \coloneqq \langle a_1, a_2, \ldots, a_{14^2}, t_1, \ldots, t_{14} | t_i^{-1} a_j t_i = w_{ij} (1 \leq i \leq 14, 1 \leq j \leq 14^2) \rangle, \tag{15}$$

where w_{1j}'s are positive words on a_j's, of length 14 such that $a_i a_j$ appears at most once as a subword of w_{1j} and similarly for w_{ij}. We obtain w_{1j} by noting that the following word

$$(a_1 a_1 a_2 a_1 a_3 a_1 \cdots a_{14})(a_2 a_2 a_3 a_2 \cdots a_{14}) \cdots (a_{13} a_{13} a_{14}) a_{14} \tag{16}$$

has length 14^2 so we can split it into 14 subwords of length 14, each corresponding to w_{1j}.

4.3 Exponentially Distorted Subgroups

The subgroup

$$F_1 \coloneqq \langle a_1, \cdots, a_{14} \rangle \tag{17}$$

is free of rank 14 and is exponentially distorted in G_1.

Here is an example. The word $t_1^{-n} a_1 t_1^n$ has length $2n+1$ in G_1. On the other hand,

$$\begin{aligned} t_1^{-n} a_1 t_1^n &= t_1^{-n+1} t_1^{-1} a_1 t_1 t_1^{n-1} \\ &= t_1^{-n+1} w_{11} t_1^{n-1} \\ &= t_1^{-n+1} a_1 a_1 a_2 a_1 \cdots a_7 a_1 t_1^{n-1} \\ &= t_1^{-n+2} t_1^{-1} a_1 t_1 t_1^{-1} a_2 \cdots t_1^{-1} a_7 t_1 t_1^{-1} a_1 t_1 t_1^{n-2} \\ &= t_1^{-n+2} w_{11} w_{11} w_{12} \cdots w_{17} w_{11} t_1^{n-2} \\ &= \cdots a_j^{(1)} \cdots . \end{aligned} \tag{18}$$

Since $l_{G_1}(t_1^{-n} a_1 t_1^n) = 2n+1$ and $l_{F_1}(t_1^{-n} a_1 t_1^n) = 14^n$, the subgroup F_1 is at least exponentially distorted in G_1.

4.4 Exponentially Exponentially Distorted Subgroups

Define $H \coloneqq G_1 *_{F_1} G_{14}$. Denote

$$F_1 \coloneqq \langle a_1^{(1)}, \cdots, a_{14}^{(1)} \rangle \tag{19}$$

and

$$F_2 \coloneqq \langle a_1^{(2)}, \cdots, a_{14}^{(2)}, \cdots, a_{14^2}^{(2)} \rangle. \tag{20}$$

Let $w_1 = t^{-n} a_1^{(1)} t^n$ and

$$\begin{aligned} w_2 &= w_1^{-1} a_1^{(2)} w_1 \\ &= (t^{-n} a_1^{(1)} t^n)^{-1} a_1^{(2)} t^{-n} a^{(1)} t^n \in H \\ &= (\cdots a_j^{(1)} \cdots)^{-1} a_1^{(2)} (\cdots a_j^{(1)} \cdots) \\ &= (\cdots t_j \cdots)^{-1} a_1^{(2)} (\cdots t_j \cdots) \\ &= \cdots a_k^{(2)} \cdots , \end{aligned} \tag{21}$$

where $a_1^{(2)} \in F_2$, $w_1 \in F_1$ and the third equality follows by the previous computation and the fourth equality follows since F_1 is identified with the subgroup of G_{14} generated by $\langle t_1, \ldots, t_{14} \rangle$. There are 14^n elements in each of $(\cdots a_j^{(1)} \cdots)$ so 14^n t_j's on each side of $a_1^{(2)}$. Since $l_H(w_2) = 4n+2$ and $l_{F_2}(w_2) = 14^{14^n}$, F_2 is at least exp(exp) distorted in H.

Acknowledgemnts The authors thank Pallavi Dani for conversations on an earlier draft and for pointing out free-by-cyclic groups as a possible platform as well as Lemma 7. Indira Chatterji is partially supported by the Institut Universitaire de France (IUF). Delaram Kahrobaei is partially supported by a PSC-CUNY grant from the CUNY Research Foundation, the City Tech Foundation, and ONR (Office of Naval Research) grant N00014-15-1-2164. Delaram Kahrobaei has also partially supported by an NSF travel grant CCF-1564968 to IHP in Paris.

References

[1] A. Myasnikov, V. Shpilrain, and A. Ushakov. *Non-commutative Cryptography and Complexity of Group-theoretic Problems*. American Mathematical Society, 2011. DOI: 10.1090/surv/177.

[2] A. Myasnikov, V. Roman'kov, A. Ushakov, and A. Vershik. The word and geodesic problems in free solvable groups. *Transactions of the American Mathematical Society*, 362(9):4655–4682, 2010. DOI: 10.1090/s0002-9947-10-04959-7.

[3] D. B. A. Epstein, M. S. Paterson, J. W. Cannon, D. F. Holt, S. V. Levy, and W. P. Thurston. *Word Processing in Groups*. A. K. Peters, Ltd., Natick, MA, USA, 1992.

[4] M. Elder. A linear-time algorithm to compute geodesics in solvable Baumslag–Solitar groups. *Illinois J. Math.*, 54(1):109–128, 2010. DOI: 10.1214/10-AAP256.

[5] M. Elder and A. Rechnitzer. Some geodesic problems in groups. *Groups – Complexity – Cryptology*, 2(2), 2010. DOI: 10.1515/gcc.2010.014.

[6] M. R. Bridson and A. Haefliger. Non-positive curvature and group theory. In *Grundlehren der mathematischen Wissenschaften*, pages 438–518. Springer Berlin Heidelberg, 1999. DOI: 10.1007/978-3-662-12494-9_22.

[7] V. Shpilrain and G. Zapata. Using the subgroup membership search problem in public key cryptography, 2006. DOI: 10.1090/conm/418/07955.

[8] M. Mitra. Coarse extrinsic geometry: a survey. In *The Epstein Birthday Schrift*. Mathematical Sciences Publishers, 1998. DOI: 10.2140/gtm.1998.1.341.

[9] T. Mecham and A. Mukherjee. Hyperbolic groups which fiber in infinitely many ways. *Algebraic & Geometric Topology*, 9(4):2101–2120, 2009. DOI: 10.2140/agt.2009.9.2101.

[10] R. C. Lyndon and P. E. Schupp. Combinatorial group theory. Reprint of the 1977 edition. Classics in Mathematics, 2001.

[11] J. Barnard, N. Brady, and P. Dani. Super-exponential distortion of subgroups of CAT(-1) groups. *Algebraic & Geometric Topology*, 7(1):301–308, 2007. DOI: 10.2140/agt.2007.7.301.