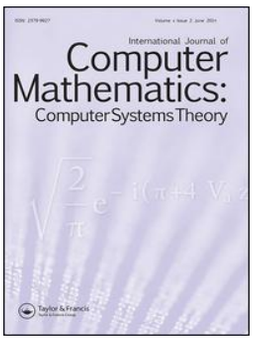

International Journal of Computer Mathematics: Computer Systems Theory

ISSN: 2379-9927 (Print) 2379-9935 (Online) Journal homepage: https://www.tandfonline.com/loi/tcom20

A cryptographic application of the Thurston norm

Ramón Flores, Delaram Kahrobaei & Thomas Koberda

To cite this article: Ramón Flores, Delaram Kahrobaei & Thomas Koberda (2020): A cryptographic application of the Thurston norm, International Journal of Computer Mathematics: Computer Systems Theory, DOI: 10.1080/23799927.2020.1716074

To link to this article: https://doi.org/10.1080/23799927.2020.1716074

Accepted author version posted online: 21 Jan 2020.
Published online: 29 Jan 2020.

INTERNATIONAL JOURNAL OF COMPUTER MATHEMATICS: COMPUTER SYSTEMS THEORY
https://doi.org/10.1080/23799927.2020.1716074

A cryptographic application of the Thurston norm

Ramón Flores[a], Delaram Kahrobaei[b,c] and Thomas Koberda[d]

[a]Department of Geometry and Topology, University of Seville, Seville, Spain; [b]Department of Computer Science, The University of York, York, UK; [c]Department of Computer Science, CUNY Graduate Center, New York University, New York, NY, USA; [d]Department of Mathematics, University of Virginia, Charlottesville, VA, USA

ABSTRACT

We discuss some applications of 3-manifold topology to cryptography. In particular, we propose a public-key and a symmetric-key cryptographic scheme based on the Thurston norm on the first cohomology of hyperbolic manifolds.

ARTICLE HISTORY
Received 13 August 2019
Revised 8 January 2020
Accepted 9 January 2020

KEYWORDS
Hyperbolic; 3-manifold; Thurston norm; cryptography; public key

2010 MATHEMATICS SUBJECT CLASSIFICATION
57M50

1. Introduction

Geometric group theory and low-dimensional topology have developed many powerful tools for studying groups, and many group-theoretic ideas have been productive in group-based cryptography. Here, we propose importing ideas from hyperbolic geometry to build new cryptoschemes with certain security advantages.

Specifically, we consider the Thurston norm on $H^1(M, \mathbb{R})$, the first cohomology of a finite volume hyperbolic 3-manifold, as introduced in [30]. The Thurston norm measures the Euler characteristic of the simplest surface in M which represents a second homology class which is Poincaré dual to an integral cohomology class and extends it to the entirety of $H^1(M, \mathbb{R})$. The Thurston norm has a remarkable linear nature which makes computations with it tractable, and as outlined below, organizes the fibrations of a fibred hyperbolic 3-manifold.

We will use the Thurston norm to build a new symmetric-key cryptographic scheme. Combined with a certain group-based public key exchange, we obtain a public-key cryptoscheme which has two levels of security and in which all communications are over public channels.

National Security Agency (NSA) announced plans to upgrade current security standards in 2015; the goal is to replace all deployed cryptographic protocols with quantum secure protocols, due to the increasing possibility of quantum attacks. This transition requires a new, post-quantum, security standard to be accepted by the National Institute of Standards and Technology (NIST). Proposals for quantum secure cryptosystems and protocols have been submitted for the standardization process. There are six main primitives currently proposed to be quantum-safe: (1) lattice-based (2) code-based (3) isogeny-based (4) multivariate-based (5) hash-based, and (6) *group-based* cryptographic schemes. Applications to post-quantum group-based cryptography could be shown if the underlying security problem is NP-complete or unsolvable; ideally one could analyse the relationship of the problems

CONTACT Ramón Flores ramonjflores@us.es, cluje28@gmail.com

under consideration here to the hidden subgroup problem (HSP), then analyse Grover's search problem. As for the relationship to the HSP, the groups under consideration are infinite and so a practical way to process them needs to be developed.

In [18], a practical cryptanalysis of WalnutDSA was proposed, a platform which was given in 2016 in [4] as a post-quantum cryptosystem using braid groups and conjugacy search problem, submitted to NIST competition in 2017.

There are other group-theoretic problems and classes of groups which have been proposed for post-quantum group-based cryptography, as we summarize here. The pioneers in this field were Wagner-Magyarik, who in [32] used a right-angled Artin group as a platform, relying on the word problem and the word choice problem; this approach was later improved by Levy-Perret in [25]. At the same time, Birget–Magliveras–Sramka [6] proposed a new protocol based on different groups that share some properties with Higman–Thompson groups. Later on, Flores–Kahrobaei and Flores–Kahrobaei–Koberda proposed right-angled Artin groups as a platform for various cryptographic protocols [13,14]. Eick and Kahrobaei proposed polycyclic groups as a platform, using the conjugacy search problem as a basis for security [11]. Gryak–Kahrobaei proposed other group-theoretic problems for consideration for polycyclic group platforms [15]. Kahrobaei–Koupparis [20] proposed a post-quantum digital signature using polycyclic groups. Kahrobaei–Khan [19] proposed a public-key cryptosystem using polycyclic groups [19]. Habeeb–Kahrobaei–Koupparis–Shpilrain proposed public key exchanges using semidirect products of semigroups in [16]. Thompson's groups have been considered by Shpilrain–Ushakov, with cryptoschemes based on the decomposition search problem [28]. Hyperbolic groups have been proposed by Chatterji–Kahrobaei–Lu, relying on properties of subgroup distortion and the geodesic length problem [9]. Cavallo–Habeeb–Kahrobaei–Shpilrain proposed using small cancellation groups for secret sharing scheme [8,17]. Free metabelian groups have been proposed as a platform by Shpilrain–Zapata, with the scheme based on the subgroup membership search problem [29]. Kahrobaei–Shpilrain proposed free nilpotent p-groups as a platform for a semidirect product public key [22]. Linear groups were proposed by Baumslag-Fine-Xu [5], and Grigorchuk's group have been proposed in [26]. Finally in [21], arithmetic groups were proposed as platform for a symmetric-key cryptographic scheme.

2. Hyperbolic 3-manifolds and the Thurston norm

We review some well-known background about hyperbolic 3-manifolds and the Thurston norm [30], concentrating on the case of fibred hyperbolic 3-manifolds.

2.1. Generalities about the Thurston norm

Let $M = M_\psi$ be a fibred hyperbolic 3-manifold. That is to say, there is an orientable surface S with negative Euler characteristic and a mapping class $\psi \in \mathrm{Mod}(S)$ such that M is the mapping torus of ψ. Observe that the rank of $H^1(M, \mathbb{R})$ is at least one, since $\pi_1(M)$ surjects to $\mathbb{Z}$. Rational cohomology classes of M which correspond to fibrations of M are called *fibred cohomology classes* of M. Precisely what is meant by this correspondence is the following: first, replace the given cohomology class by the smallest nonzero multiple which is integral. A cohomology class $\phi \in H^1(M, \mathbb{Z})$ is a homomorphism to $\mathbb{Z}$, which by standard arguments from algebraic topology is induced by a based map of spaces $\Phi\colon M \to S^1$. After modifying Φ by a homotopy, the generic preimage of a point will be a subsurface S of M which is Poincaré dual to ϕ. If Φ is chosen carefully enough, S will be a fibre of a fibration over S^1. The fibration can also be built by pulling the form $d\theta$ from S^1 back under Φ and integrating it. See [30] for more details.

A fibred 3-manifold M is called *atoroidal* if it does not contain a non-peripheral incompressible torus. Here, this means that if $T \subset M$ is a π_1-injective copy of the torus, then T can be pushed into a cusp of M. It is a famous result of Thurston that a fibred 3-manifold admits a finite volume hyperbolic metric if and only if it is atoroidal, which in turn will happen if and only if no power of the mapping

class ψ fixes the homotopy class of a simple closed loop on S. Here, a simple closed loop on S is an essential copy of S^1 which is not parallel to a puncture or boundary component of S. Such a mapping class ψ is called *pseudo-Anosov*.

It is a standard result from foliation theory that if the rank of $H^1(M,\mathbb{R})$ is at least two, then small perturbations of a fibred cohomology class $\phi \in H^1(M,\mathbb{Q}) \subset H^1(M,\mathbb{R})$ will give new fibrations of M over the circle which are inequivalent to ϕ. Thurston's work [30] organized the fibrations of M by defining a norm $\|\cdot\|_T$ on $H^1(M,\mathbb{R})$, called the *Thurston norm*. The norm of a cohomology class $\|\phi\|_T$ is given by $\min_{S_\phi} |\chi(S_\phi)|$, where this minimum is taken over surfaces which are Poincaré dual to ϕ. The following summarizes the relevant features of the Thurston norm:

Theorem 2.1: *Let M be a compact atoroidal 3-manifold with $\chi(M) = 0$, and let $\|\cdot\|_T$ be the Thurston norm.*

(1) *$\|\cdot\|_T$ is a nondegenerate norm on the vector space $H^1(M,\mathbb{R})$;*
(2) *The unit norm ball is a convex polytope, all of whose vertices lie at rational points in $H^1(M,\mathbb{R})$;*
(3) *Let $\phi \in H^1(M,\mathbb{Z})$ be a fibred cohomology class of M. Then there is a maximum dimensional face F of the unit ball of $\|\cdot\|_T$ such that $\phi \in \mathbb{R}\cdot F$. Moreover, every primitive integral cohomology class $\phi \in \mathbb{R}\cdot F$ is fibred. The face F is called a fibered face of the unit norm ball.*

Here, an integral cohomology class if called *primitive* if it is nonzero and if it is not an integer multiple of another integral cohomology class. Viewed as a tuple of vectors, an integral cohomology class is primitive if and only if the entries of the tuple are relatively prime and not all zero.

Let $\phi \in H^1(M,\mathbb{Z})$ be a fibred cohomology class. Then M fibres over the circle with fiber $S = S_\phi$, where $\pi_1(S) < \pi_1(M)$ is identified with $\ker\phi$. The following proposition is standard and we include its proof for the convenience of the reader.

Proposition 2.1: *Suppose M is hyperbolic, and let S be the fibre of a fibration of M over S^1. Then $\pi_1(S) < \pi_1(M)$ is exponentially distorted, and the membership problem for $\pi_1(S)$ is solvable in linear time.*

Proof: We have that $\pi_1(M)$ is a semidirect product of $\mathbb{Z}$ with $\pi_1(S)$, where the conjugation action of a generator t of $\mathbb{Z}$ is given by a pseudo-Anosov mapping class of $\pi_1(S)$. If $1 \neq \gamma \in \pi_1(S)$ and ψ is a pseudo-Anosov mapping class which has been lifted to an automorphism of $\pi_1(S)$, then the length of the shortest representative in the conjugacy class of $\psi^n(\gamma)$ grows like λ_ψ^n, where $\lambda_\psi > 1$ is a real number called the *stretch factor* of ψ. Since conjugation by t acts on $\pi_1(S)$ by ψ, we have that $\psi^n(\gamma) = t^{-n}\gamma t^n$, a word whose length is linear in n. It follows that $\pi_1(S) < \pi_1(M)$ is exponentially distorted. We refer the reader to Exposé 10 of [12] for details on word growth entropy and pseudo-Anosov mapping classes.

Now suppose that $g \in \pi_1(M)$ is a given element, and we wish to determine if $g \in \pi_1(S)$. The group $\pi_1(M)$ surjects to $\mathbb{Z}$ by a homomorphism ϕ, and the kernel of this map is exactly $\pi_1(S)$. If $\pi_1(M) = \langle g_1,\ldots,g_k\rangle$, then ϕ is determined by its values on the generators of $\pi_1(M)$. If $g \in \pi_1(M)$ is a product of N generators of $\pi_1(M)$, we compute the value of ϕ on the N generators needed to represent g and add them up, which requires computational resources bounded by a linear function in N. If the resulting sum is zero, then $g \in \pi_1(S)$. If the sum is nonzero then $g \notin \pi_1(S)$. ■

2.2. Examples

From the general description, the Thurston norm seems very difficult to compute and hence unwieldy for many practical applications. However, there are many situations in which the Thurston norm can be computed, at least in a cone over a fibred face.

In, McMullen defined the Teichmüller polynomial associated to a fibred face and gave a practically implementable algorithm for computing it. From the Teichmüller norm (computed from

the Teichmüller polynomial) and the Alexander norm (computed from the Alexander polynomial) on $H^1(M,\mathbb{R})$ for a fibred hyperbolic 3-manifold M, one can compute a fibred face of the unit Thurston norm ball, the cone over which contains the given fibred cohomology class. He indicates how to carry out these computations for certain pseudo-Anosov braids of the 4-times punctured sphere.

A very detailed computation of the Alexander and Teichmüller norm for a particular two-cusped hyperbolic 3-manifold, namely the sibling of the Whitehead link complement, was carried out by Aaber–Dunfield [1]. The authors of that paper explicitly computed the Alexander and Teichmüller polynomials of the sibling of the Whitehead link complement, as well as the whole Thurston norm ball, which is a square with unit side length centred at the origin. They show that all four faces of the square are fibred, and so that every primitive cohomology class of the manifold is fibred except the ones lying on the two lines passing through the corners of the square.

For other 3-manifolds presented as mapping tori of multiply punctured disks, an algorithm for computing the Teichmüller polynomial (as well as further topological data associated to other fibrations of the manifold) was proposed by Lanneau–Valdez [23]. Thus, the theory we apply in this paper is rich with computationally tractable examples.

3. An application to public-key cryptography

We now propose a cryptographic scheme which uses the Thurston norm. Alice and Bob are communicating over an insecure channel. The following information is public:

- A fibred hyperbolic 3-manifold M with $H^1(M,\mathbb{R})$ of rank at least two, a fixed finite presentation of $\pi_1(M)$, and a fibred face F of the Thurston norm ball. For instance, one could use Thurston's example of the simplest pseudo-Anosov braid, or alternatively Aaber–Dunfield's example, as described above.
- For every primitive integral cohomology class $\phi \in \mathbb{R}_+ \cdot F$, a standard presentation $\mathcal{P}_\phi$ of the corresponding fibre group $\pi_1(S_\phi)$, a stable letter $t_\phi \in \pi_1(M)$, and an automorphism ψ_ϕ of $\pi_1(S_\phi)$ such that $\pi_1(M)$ is the semidirect product of $\pi_1(S_\phi)$ with $\mathbb{Z}$ with the conjugation action of t_ϕ given by ψ_ϕ. An explicit isomorphism between $\pi_1(M)$ with its fixed presentation and this semidirect product presentation
$$\langle \mathcal{P}_\phi, t_\phi \mid t_\phi x t_\phi^{-1} = \psi_\phi(x)\rangle$$
corresponding to the fibred class ϕ is included in the data. We write $\mathrm{Prim}(\mathbb{R}_+ \cdot F)$ for the collection of such primitive integral cohomology classes. Here, the choice of the stable letter is not strictly necessary, but it precludes the need for an extra conjugacy decision later on in the cryptoscheme. Strictly speaking, $\mathrm{Prim}(\mathbb{R}_+ \cdot F)$ is an infinite collection of data, so it is necessary to define precisely what it means to share it. In practice, one would have a searchable database which is large enough to give Alice and Bob a rich collection of choices, and so that over a course of their communication, no repeats would be necessary. One could restrict the database to primitive rational cohomology classes in F whose denominators are at most some arbitrary large cut-off say 10^{12}.
- A finitely generated group G suitable for a public-key cryptographic scheme such as the Anshel–Anshel–Goldfeld protocol (see [3]) and an efficiently computable function
$$f\colon G \to \mathrm{Prim}(\mathbb{R}_+ \cdot F).$$

Here, a *standard presentation* for a fibre group is either a presentation of a free group with finitely many generators and no relations, or the standard presentation of a closed surface group of genus g:
$$\pi_1(S_g) = \langle a_1, b_1, \ldots, a_g, b_g \mid [a_1,b_1]\cdots[a_g,b_g] = 1\rangle.$$

The scheme is as follows:

(1) Alice and Bob use a public-key cryptographic scheme in order to produce a shared private key $g \in G$.
(2) Using the public function f, Alice and Bob agree on the fibred cohomology class $\phi = f(g)$ with corresponding fibre group $\pi_1(S)$ with presentation $\mathcal{P}$ and automorphism ψ.
(3) Alice chooses an arbitrary positive integer N and computes the length of $\psi^N(s)$ for every generator of $\pi_1(S)$ in the presentation $\mathcal{P}$. The key is the maximum length $\ell_{\max}$ obtained in this way, on the generator $s_{\max}$ in $\mathcal{P}$.
(4) Over a public channel, Alice sends a finite collection $\{x_1, \ldots, x_t\} \subset \pi_1(M)$, written in terms of the fixed generators for $\pi_1(M)$, and of length comparable to N. She chooses these elements in such a way that if X_ϕ is the generating set in the presentation $\mathcal{P}_\phi$, then $\psi^N(X_\phi) \subset \{x_1, \ldots, x_t\}$, but so that all but $|X_\phi|$ of the elements $\{x_1, \ldots, x_t\}$ do not belong to $\pi_1(S)$. We assume that $|X_\phi| \ll t$.
(5) Bob checks which of these elements lie in $\pi_1(S)$.
(6) Bob uses the fact that ψ is given by conjugation by an element of $\pi_1(M)$ to recover N.
(7) Bob computes the length of $\psi^N(s)$ for each generator of $\pi_1(S)$ and recovers $\ell_{\max}$.

We remark that the value of $\ell_{\max}$ is uniquely determined by Alice's initial choice of N.

4. An explicit example

We consider the example of a fibred 3-manifold coming from the simplest pseudo-Anosov braid, as worked out in [24].

4.1. The 3-manifold

The initial fibre is S_0, which is identified with the thrice punctured disk, and whose mapping class group is identified with the three-stranded braid group B_3. In the standard braid generating set $\{\sigma_1, \sigma_2\}$, the simplest pseudo-Anosov braid is given by $\beta = \sigma_1\sigma_2^{-1}$.

We have that $\pi_1(S_0) = \langle x, y, z\rangle \cong F_3$, where these generators are identified with small based loops about the three punctures of S_0. We have

$$\sigma_1 \colon (x, y, z) \mid (y, y^{-1}xy, z)$$

and

$$\sigma_2^{-1} \colon (x, y, z) \mapsto (x, yzy^{-1}, y).$$

Thus, we have

$$\beta \colon (x, y, z) \mapsto (yzy^{-1}, yz^{-1}y^{-1}xyzy^{-1}, y).$$

A presentation for the fundamental group of the fibred 3-manifold associated to β can be written as

$$\pi_1(M) = \langle t, x, y, z \mid t^{-1}xt = yzy^{-1}, t^{-1}yt = yz^{-1}y^{-1}xyzy^{-1}, t^{-1}zt = y\rangle.$$

It is easy to see that β acts transitively on the punctures of S_0, and so that $H_1(M, \mathbb{Z}) \cong \mathbb{Z}^2$. If $\phi \in H^1(M, \mathbb{Z})$, then ϕ is determined by its values on t and on x, so that we may write $\phi = (a, b) \in \mathbb{Z}^2$ for the cohomology class which satisfies $\phi(t) = a$ and $\phi(x) = b$. McMullen computes the Thurston norm on $H^1(M, \mathbb{R})$ and shows that it is given by

$$\|\phi\|_T = \max\{|2a|, |2b|\}.$$

Each face of the Thurston unit norm ball is fibred. The face F whose cone contains $(1, 0)$ is therefore given by $F = \{1/2\} \times [-1/2, 1/2]$.

4.2. From a public key to a new fibration

Let G be a finitely generated group suitable for the Anshel–Anshel–Goldfeld protocol, with a fixed normal form. Then we can construct a computable function which associates to elements of G various fibrations of M. If $g \in G$, we write g in a normal form and let $|g|$ denote the length of g in this normal form. Then, we may set

$$f(g) = D(g)\left(\{1/2\}, \left\{\frac{|g|}{|g|+1} - 1/2\right\}\right),$$

where here $D(g)$ is chosen to be the smallest positive integer so that $f(g) \in \mathbb{Z}^2$. Note that $D(g) \leq \operatorname{lcm}\{2, |g|+1\}$. Thus, we have associated to $g \in G$ a new cohomology class $f(g)$ which is defined by

$$f(g)(t) = D(g)/2$$

and

$$f(g)(x) = |g| \cdot D(g)/(|g|+1) - D(g)/2.$$

This cohomology class will represent a new fibration provided $|g| \neq 0$. We remark that the function f constructed here is just one possible example which would suit our purposes. There are many other suitable candidates for f.

4.3. New fibre subgroups

Given $\phi \in H^1(M, \mathbb{Z}^2)$. We have that the new fibre subgroup $\pi_1(S_\phi)$ is given by the kernel of ϕ, viewed as the composition

$$\pi_1(M) \to H_1(M, \mathbb{Z}) \to \mathbb{Z},$$

where the first map is the abelianization map and where the second map is ϕ. The group $\pi_1(S_\phi)$ will always be a finite rank free group, and its rank can be computed as $\|\phi\|_T + 1$, since $\|\phi\|_T$ denotes the absolute value of the Euler characteristic of the fibre. Finding a presentation for the fibre subgroup is sometimes possible [7,10], although in general it may be difficult. This is why we assume that free presentations for fibre subgroups are part of the public data.

4.4. Distortion of lengths

The advantage of the scheme we propose is that a very large integer is encoded by a relatively small one. The essential point is that both Alice and Bob do computations in $\pi_1(M)$, essentially just conjugation. The secrecy of the scheme is entirely in the choice of fibration, which in turn gives a mapping class and an exponentially distorted subgroup. Other than conjugation, which results in linear growth of words in $\pi_1(M)$, Proposition 2.1 shows that membership in the fibre subgroup is computable in linear time. Alice and Bob use their common knowledge of the fibre subgroup to extract an integer N, which is on the order of the logarithm of the shared key. It is in this last step, passing from N to $\ell_{\max}$ that the exponentially distorted subgroup comes into play.

Alice picks N, and her key is the maximal length of ψ_ϕ^N applied to elements of the free generating set of the fibre subgroup. To communicate N over the channel, she applies ψ_ϕ^N, viewed as conjugation by the element of $t_\phi \in \pi_1(M)$. The resulting elements of $\pi_1(M)$ will have lengths which are linear in N. When Alice sends information over the channel, Bob applies t_ϕ successively to generators of $\pi_1(S_\phi)$ and checks to see if the generating set lies in $\{x_1, \ldots, x_t\}$. This will require linearly many calculations in N and t, since the word problem in hyperbolic 3-manifold groups has linear complexity. Once Bob finds the first such N, this will be the same value of N as chosen by Alice, since ψ_ϕ is pseudo-Anosov and is therefore not periodic.

The key that Alice and Bob wish to share is instead $\ell_{\max}$, which is the maximal length of ψ_ϕ^N applied to a generator of $\pi_1(S_\phi)$, viewed as an element of $\pi_1(S_\phi)$. Alice and Bob now both know N, and thus can recover $\ell_{\max}$, since ψ_ϕ is a public automorphism of the free group $\pi_1(S_\phi)$. The size of $\ell_{\max}$ will be exponential in N. The precise distortion can be computed from the Teichmüller polynomial. McMullen computes the Teichmüller polynomial for that fibred face to be

$$\Theta(t,u) = 1 - t(1 + u + u^{-1}) + t^2.$$

Here, the polynomial $\Theta(t,u)$ is viewed as an element of the group ring $\mathbb{Z}[H, t^{\pm 1}]$, where here $H = \langle u \rangle$ denotes the ψ_ϕ–invariant homology of S_ϕ. In this case, the generator t can be identified with the stable letter t of the fibration defining M, and we can write the other generator as $u = [x] + [y] + [z]$, the sum of the homology classes of the three punctures. Then, we can write

$$\Theta(t,u) = \sum_{g \in H_1(M,\mathbb{Z})} a_g g,$$

with $a_g \in \mathbb{Z}$. If $\phi \in H^1(M,\mathbb{Z})$, then we view ϕ as an element of $\mathrm{Hom}(\pi_1(M),\mathbb{Z})$ and and we can write

$$\Theta(k) = \sum_{g \in H_1(M,\mathbb{Z})} a_g k^{\phi(g)}.$$

We set λ_ϕ to be the largest root of $\Theta(k)$, which will always be a real number which is greater than one. Then we have $\ell_{\max} \sim \lambda_\phi^N$.

For the specific Teichmüller polynomial

$$\Theta(t,u) = 1 - t(1 + u + u^{-1}) + t^2,$$

we work out two examples of stretch factors λ_ϕ for two different fibred cohomology classes. The canonical class $\phi = (1,0)$ is the one describing the original fibred 3-manifold. In this case, we compute $\phi(t) = 1$ and $\phi(u) = 0$. We thus obtain the polynomial $\Theta(k) = k^2 - 3k + 1$, whose largest root is one more than the Golden Ratio $(3 + \sqrt{5})/2$. This is well-known to be the stretch factor of β.

We also consider the class $\phi = (2,1)$. It is easy to check that this class lies in the cone over F. We obtain the polynomial $\Theta(k) = k^4 - k^3 - k^2 - k + 1$, which one discovers by numerical calculation to have a root at $k \approx 1.72208$.

4.5. Generalization to other pairs of groups

In principle, there is nothing special about the pair $(\pi_1(M), \pi_1(S))$ for a fibre subgroup of a hyperbolic 3-manifold. For the applications, one could use any pair of a finitely generated group and a finitely generated exponentially distorted subgroup (cf. [9]). The particular advantage of using the Thurston norm is that from a single hyperbolic group, we obtain infinitely many different exponentially distorted subgroups which are distorted in different ways. Moreover, the Teichmüller polynomial organizes the different fibre subgroups in a computationally convenient way. In general, such a framework does not exist for arbitrary such pairs of groups. A notable exception, on which one could also base a similar cryptoscheme, is the class of free-by-cyclic groups [2,10].

5. An application to symmetric-key cryptography

The scheme developed in Sections 3 and 4 can be simplified somewhat to yield a symmetric-key cryptographic scheme. Such a scheme would eschew the need for an initial private shared key. The setup for this scheme would be as follows.

Public information: The fibred hyperbolic manifold M, presented as a mapping torus, would be public as before. A presentation for $\pi_1(M)$ would also be public.

Private information: Alice and Bob would agree beforehand on a fibred cohomology class ϕ of M. This would yield a private fibred subgroup $\pi_1(S_\phi)$ with a preferred presentation, and a private automorphism ψ_ϕ of $\pi_1(S_\phi)$.

The implementation of the cryptoscheme would be as follows:

(1) Alice chooses an arbitrary integer N.
(2) Alice communicates the integer N to Bob over a public channel.
(3) Alice and Bob both compute ψ_ϕ^N on the generators of $\pi_1(S_\phi)$ in the preferred presentation and compute the lengths of the resulting words.
(4) The shared key is $\ell_{\max}$, the longest length of a word obtained by applying ψ_ϕ^N to the generators.

6. Remarks on security

There are several layers of security which are built into the schemes we propose. In the public-key scheme, the first layer of security lies in similar security assumptions of the public key-exchange scheme à la Anshel–Anshel–Goldfeld (AAG). We recall that this is used by Alice and Bob to agree on a fibred cohomology class. We note that there have been several proposals for the platform group for the AAG protocol, such as braid groups, polycyclic groups, Grigorchuk groups, certain classes of right-angled Artin groups and their subgroups, in which the simultaneous conjugacy search problem is difficult. Apart from a few proposed attacks (see [27,31] for attacks adapted to braid group and linear group platforms as well as potential ripostes), the AAG scheme remains secure for suitable choices of parameters. In the symmetric-key scheme, the use of AAG is unnecessary, thus removing any vulnerabilities to attacks on that protocol.

In both schemes, the key that Alice and Bob share will be much larger than any of the public data over the channel. Thus, even if the eavesdropper is able to guess N, the key $\ell_{\max}$ is exponentially longer than N and would therefore be much more difficult to guess, short of knowing which cohomology class Alice and Bob are using.

For Alice and Bob, computations inside the group $\pi_1(S)$ are easy since this group is either free or a surface group, and hence computing word lengths and solving the word problem is relatively easy (using small cancellation theory, for instance) from the standard presentations given in the public data.

Finally, since the public data of the fibred classes is public and since for practical purposes it must be truncated to be a finite list, it is conceivable that an eavesdropper would simply use the database of fibrations and an efficient solution to the conjugacy problem to discover the key without knowing the secret fibre. The eavesdropper could conceivably check each fixed presentation in the database and look for words sent by Alice in which the stable letter appears with exponent sum zero. This vulnerability can be overcome by making the database very large compared to the size of the key, so that processing the whole database would be prohibitive. Thus, the key shared by Alice and Bob would be obsolete by the time the eavesdropper could compute it.

Acknowledgments

The authors thank the anonymous referees for their careful reading of the manuscript and for their helpful comments.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

Ramón Flores is partially supported by FEDER-MINECO (Ministerio de Economia y Competitividad) [grant number MTM2016-76453-C2-1-P]; Delaram Kahrobaei was supported by the ONR (Office of Naval Research) [grant number N000141512164]; Thomas Koberda is partially supported by an Alfred P. Sloan Foundation Research Fellowship and by NSF-Center for Hierarchical Manufacturing, National Science Foundation [grant number DMS-1711488].

References

[1] J.W. Aaber and N. Dunfield, *Closed surface bundles of least volume*, Algebr. Geom. Topol. 10(4) (2010), pp. 2315–2342.
[2] Y. Algom-Kfir, E. Hironaka and K. Rafi, *Digraphs and cycle polynomials for free-by-cyclic groups*, Geom. Topol. 19(2) (2015), pp. 1111–1154.
[3] I. Anshel, M. Anshel and D. Goldfeld, *An algebraic method for public-key cryptography*, Math. Res. Let. 6 (1999), pp. 287–291.
[4] I. Anshel, D. Atkins, D. Goldfeld and P. Gunnells, *WalnutDSATM: A quantum resistant group theoretic digital signature algorithm*, 2016. Available at https://www.nist.gov/sites/default/files/documents/2016/10/19/atkins-paper-lwc2016.pdf.
[5] G. Baumslag, B. Fine and X. Xu, *Cryptosystems using linear groups*, Appl. Algebra Eng. Comm. Comput. 17 (2006), pp. 205–2017.
[6] J.C. Birget, S.S. Magliveras and M. Sramka, *On public-key cryptosystems based on combinatorial group theory*, Tatra Mt. Math. Publ. 33 (2006), pp. 137–148.
[7] K. Brown, *Trees, valuations, and the Bieri-Neumann-Strebel invariant*, Inv. Math. 90 (1987), pp. 479–504.
[8] B. Cavallo and D. Kahrobaei, *Secret sharing using the shortlex order and non-commutative groups*, Contemp. Math. 633 (2015), pp. 1–8. AMS.
[9] I. Chatterji, D. Kahrobaei and N.Y. Lu, *Cryptosystems using subgroup distortion*, Theor. Appl. Inform. 29 (2017), pp. 14–24.
[10] S. Dowdall, I. Kapovich and C. Leininger, *McMullen polynomials and Lipschitz flows for free-by-cyclic groups*, J. Eur. Math. Soc. 19(11) (2017), pp. 3253–3353.
[11] B. Eick and D. Kahrobaei, *Polycyclic groups: A new platform for cryptography*, Technical report (60 citations), 2004. Available at http://math.gr/0411077.
[12] A. Fathi, F. Laudenbach, V. Poenaru, Travaux de Thurston sur les surfaces, Séminaire Orsay. Astérisque, pp. 66–67. Société Mathématique de France, Paris, 1979.
[13] R. Flores and D. Kahrobaei, *Cryptography with right-angled Artin groups*, Theor. Appl. Inform. 28(3) (2016), pp. 8–16.
[14] R. Flores, D. Kahrobaei and T. Koberda, *Algorithmic problems in right-angled Artin groups: complexity and applications*, J. Algebra 519 (2019), pp. 111–129.
[15] J. Gryak and D. Kahrobaei, *The status of the polycyclic group-based cryptography: A survey and open problems*, Groups Complex. Cryptol. 8 (2016), pp. 171–186.
[16] M. Habeeb, D. Kahrobaei, C. Koupparis and V. Shpilrain, *Public key exchange using semidirect product of (SEMI) groups*, ACNS 2013, Applied Cryptography and Network Security, LNCS Vol. 7954, 2013, pp. 475–486.
[17] M. Habeeb, D. Kahrobaei and V. Shpilrain, *A secret sharing scheme based on group-presentation and word problem*, Contemp. Math. AMS 582 (2012), pp. 143–150.
[18] D. Hart, D.H. Kim, G. Micheli, *A Practical Cryptanalysis of WalnutDSA*, LNCS, PKC, Rio de Janeiro, 2018.
[19] D. Kahrobaei and B. Khan, *A Non-Commutative Generalization of the El Gamal Key Exchange using Polycyclic Groups*, Proceeding of IEEE, GLOBECOM, 2006, pp. 1–5.
[20] D. Kahrobaei and C. Koupparis, *Non-commutative digital signatures using non-commutative groups*, Groups Complex. Cryptol. 4 (2012), pp. 377–384.
[21] D. Kahrobaei and K. Mallahi-Karai, *Some applications of arithmetic groups in cryptography*, Groups Complex. Cryptol. 11(1) (2019), pp. 1–9.
[22] D. Kahrobaei and V. Shpilrain, *Using semidirect product of (semi)groups in public key cryptography*, Computability in Europe 2016, LNCS 9709, 2016, pp. 132–141.
[23] E. Lanneau and F. Valdez, *Computing the Teichmüller polynomial*, J. Eur. Math. Soc. (JEMS) 19(12) (2017), pp. 3867–3910.
[24] C. T. McMullen, *Polynomial invariants for fibered 3-manifolds and Teichmüller geodesics for foliations*, Ann. Sci. Ecole Norm. Sup. 33(4) (2000), pp. 519–560.
[25] F. Levy-dit-Vehel, L. Perret, On the Wagner-Magyarik cryptosystem, in Coding and Cryptography, Ø. Ytrehus, ed., LNCS, Vol. 3969, pp. 316–329, Springer, Berlin, 2006.
[26] G. Petrides, *Cryptanalysis of the public key cryptosystem based on the word problem on the Grigorchuk groups*, Cryptography and Coding, 2003, pp. 234–244.

[27] V. Roman'kov, *An improved version of the AAG cryptographic protocol*, Groups Complex. Cryptol. 11 (2019), pp. 35–42.
[28] V. Shpilrain, A. Ushakov, *Thompson's Group and Public Key Cryptography*, ACNS, New York, 2005.
[29] V. Shpilrain and G. Zapata, *Combinatorial group theory and public key cryptography*, Appl. Algebra Engin. 17 (2006), pp. 291–302.
[30] W.P. Thurston, *A norm for the homology of 3-manifolds*, Mem. Am. Math. Soc. 59(339) (1986), pp. 99–130. i–vi.
[31] B. Tsaban, *Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography*, J. Cryptology 28(3) (2015), pp. 601–622.
[32] N.R. Wagner and M.R. Magyarik, *A Public-Key Cryptosystem Based on the Word Problem*, in *Advances in Cryptology. CRYPTO 1984*, G.R. Blakley, D. Chaum, eds., Lecture Notes in Computer Science, Vol. 196, Springer, Berlin, 1985.