A topological approach to secure key exchange

Filippo Cerocchi[1], Ph.D., Gabriele Rizzo[2], Ph.D.

[1]*Leonardo S.p.A., Cybersecurity Division, Grants & Collaborations & Prototypes*
[2]*Leonardo S.p.A., Cybersecurity Division, Grants & Collaborations & Prototypes*

Abstract

Quantum algorithms providing an exponential boost to the solutions of Decision and Search Problems on infinite, non-commutative groups have not been found yet. Despite this apparent robustness, only one candidate of the NIST Post-quantum standardization based its security on these problems (WalnutDSA). In this brief note we look at some general aspects of Lattice based and Isogeny based cryptoschemes (with particular reference to the idea of *Hard Homogeneous Space* by Couveignes —[1]) and we show how these ideas can be adapted to the context of non-commutative Group based cryptography. We identify the Mapping Class Group of a closed surface and its action on the Curve Graph as an ideal candidate to construct a new quantum resistant key exchange protocol built on this group action based approach.

Keywords

Post-Quantum Cryptography, Mapping Class Group, Curve Graph, Dehn Twist, Conjugacy Search Problem

1. Introduction

Since the breakthrough of Shor ([2], [3]) in the mid nineties, who provided a polynomial time quantum algorithm for integer factorization and discrete logarithm —virtually breaking every currently used cryptosystem—, the advent of a scalable, universal quantum computer inspire mixed feeling into academics, institutions and in the tech industry.

Two main questions were raised:

- Assume quantum computers become available. How can we protect classified informations stored and encrypted with classical methods?
- Will the quantum key distribution (QKD) and quantum mechanics based cryptographic protocols completely replace classic cryptography?

Over twenty years after Shor's discovery, it is widely believed that quantum computers will not entirely replace classical computers ([4]), with the former employed to execute specific tasks which are classically intractable, and that classical cryptography is likely to serve us also in the next technological revolution, though renewed to face threat posed by a malevolent use of quantum technologies.

ITASEC'21: Italian Conference on Cybersecurity, April 07–09 2021, Online

filippo.cerocchi@leonardocompany.com (F. Cerocchi); gabriele.rizzo@leonardocompany.com (G. Rizzo)

The necessity of classical methods to secure informations from quantum attacks is certainly driven by the efforts that Tech Giants are putting in place to realize more and more powerful and refined quantum computers. This rush is one of the reasons why NIST proposed a selection for Post-Quantum standardization ([5]) in 2017, looking for new quantum resistant cryptographic primitives which could guarantee certain functionalities (Public-key Encryption and Key-establishment algorithms, Digital Signatures algorithms). We are currently at the final round of evaluation with 4 candidates considered for Public-key Encryption and Key-establishment algorithms and 3 candidates for Digital Signatures (other candidates has been considered as alternate candidates). The 4 candidates for Public-key Encryption and Key-establishment algorithms are ClassicMcEliece (code based cryptosystem), CRYSTALS-KYBER, NTRU and SABER (lattice based cryptosystems).

It did not go unnoticed the absence of candidates exploiting techniques of non-commutative group based cryptography, among the proposals (with the exception of WalnutDSA for Digital Signatures, based on Braid Groups). This note aims to provide some motivations to why it still makes sense to look at non-commutative group based cryptography as fertile ground for quantum resistant public-key cryptoschemes. We shall thus try to highlight the links existing between group-based cryptography and low-dimensional geometry and topology, and see how their interaction mirrors into abstract paradigms preparing the ground for Isogeny based cyrptography and Lattice based cryptography.

Our eventual aim, which will not be pursued in this short note, is to provide a new quantum resistant key-exchange protocol, based on the action of the Mapping Class Group onto the Curve Graph (see §3.2 for an heuristic description of these mathematical objects). To this end we remark that some specific operations involving these mathematical objects have become computationally tractable only recently (see §2.2). The techniques adopted to develop these ideas have a minimal overlap with the techniques used by the NIST candidates, hence it is a research direction which is new. Nevertheless, we are working within the general framework of exploiting a group action to provide an additional layer of complexity. This should be understood as an attempt to bring Geometric Topology into play in quantum resistant Public-Key Cryptography.

2. Non commutative group based cryptography and computational topology

2.1. Non commutative group based cryptography and quantum resistance

It is customary to date back the origin of non-commutative group based cryptography to the work of Magyarik-Wagner ([6]) though it was the successive work of Anshel-Anshel-Goldfeld ([7]) that attracted attention of group theorist and cryptographers. In [7] the authors proposed the protocol described below whose major advantage is the fact that it does not rely on any commutativity property of the groups (or subgroups) involved.

Anshel-Anshel-Goldfeld Protocol

0. A trusted authority provides Alice and Bob with a group G and two subsets $\{a_1, ..., a_n\}$, $\{b_1, ..., b_m\}$ of elements of G;

1. Alice chooses a secret word $w_A = w_A(a_1, .., a_n)$; Bob chooses a secret word $w_B = w_B(b_1, ..., b_m)$;

2. Alice sends to Bob the conjugates $\{b_i^{w_A}\}_{i=1,...,m}$; Bob sends to Alice the conjugates $\{a_i^{w_B}\}_{i=1,...,n}$;

3. Bob computes $w_B^{-1} w_A^{-1} w_B w_A = w_B^{-1} \cdot w_B(b_1^{w_A}, ..., b_m^{w_A})$;
Alice computes $(w_B^{-1} w_A w_B)^{-1} w_A = (w_A(a_1^{w_B}, .., a_n^{w_B}))^{-1} w_A$;

4. The shared secret $[w_B^{-1}, w_A^{-1}]$ is established.

The introduction of this protocol raised the attention of researchers on possible application of infinite, non-abelian group theory to cryptography. One year later a protocol by Ko-Lee et al. ([8]) was proposed on Braid Groups. Since then, a lot of effort have been made in order to identify a good *platform group* (see [9] chapter 4 for the definition) for AAG-protocol, bringing more and more attention on Braid groups, a rather peculiar and well understood family of groups, whose characteristics match with the requests defining a *platform group*. Braid groups on one hand show sufficient complexity and on the other hand they come with a handful of algebraic tools which make them computationally tractable. Several other protocols have been conceived in this area, we refer to [9] and references therein.
The general idea for protocols *à la* Anshel-Anshel-Goldfeld is to choose among decisional problems on non-abelian infinite groups (Word Problem, Conjugacy Problem, Membership Problem, Decomposition Problem, Factorization Problem, Isomorphism Problem etc.) and define a protocol exploiting the corresponding “search problem". There have also been attempts to define protocols for infinite non-abelian groups using decisional problems. As it can be read in [9], some of these protocols exhibit security against computationally unbounded adversaries, the trade-off of these techniques being that their use only allows a legitimate party to decrypt messages correctly with a probability which can be made arbitrarily close but not equal to 1.

It is worth to remark that no quantum algorithm at the moment is known to provide an exponential computational boost to the solution of problems over finitely generated, infinite, non-abelian groups ([10], [11] the second providing an updated list of quantum tools to solve hard computational problems). This could be due to the fact quantum algorithms are usually based on the possibility of creating an entangled state exhausting the elements of a finite set, which hopefully encodes enough information to solve a certain problem. This is not the case when we work on infinite, non-abelian groups, which do not have any preferred or “canonical" finite set of elements to rely upon. It is possible that the lack of efficient quantum algorithms to speed up solutions of certain computational problems over non-commutative group based cryptography is due to a minor interest of the quantum computing community towards this kind of cryptoschemes. Nevertheless, the absence of efficient algorithms for treating problems on infinite, finitely generated, non-abelian groups is factual.

2.2. Non commutative group based cryptography and topology

Non commutative group based cryptography investigates the hardness of certain computational problems over non-abelian, infinite, finitely generated groups and tries to produce effective and secure cryptographic protocols based on these problems. Infinite groups have been originally studied using tools coming from combinatorics and algebra. During the eighties of the 20th century a new approach to the study of infinite group, mostly fueled by ground-breaking works of M. Gromov ([12],[13], [14], [15]), led to the rise of Geometric Group Theory as an established research field. Generally speaking the idea behind Geometric Group Theory is to derive properties of infinite groups not just looking at their presentations[1] and their algebraic aspects but instead looking at the way these groups “act" on suitably constructed spaces. These provided mathematicians with a bunch of new tools, which led to unforeseeable developments in the last 30 years.

It is thus safe to say that there is a strong interaction between the study of infinite, discrete groups and the fields of Topology and Geometry. This link is particularly significant when we look at the Topology and Geometry of manifolds of dimension 2 and 3: here the *fundamental group* — a group obtained by looking at loops based at a given point of the manifold (up to *homotopy*) with “multiplication" given by the concatenation of paths — of a 2- or 3-manifold encodes (almost) all of the topological information of the manifold, and conversely several properties of the group can be investigated by studying suitably chosen geometric structures on the manifold. In particular several geometric problems have group-theoretic translations and *viceversa.*

On the other hand, the techniques used to study manifolds of dimension 2 and 3 have strongly combinatorial aspects: several proofs concerning surfaces and 3-manifolds are actual algorithms. The study of these combinatorial and algorithmic aspects of surfaces and 3-manifolds have been one of the motivations for the development of an area which is known as Computational Topology. If we restrict our attention to surfaces, several works throughout the last twenty years enable us to efficiently perform several topological and geometric operations on them (for example [16], [17], [18]). Our belief is that we can exploit these algorithms and the connection existing within surfaces and groups for cryptographic purposes.

[1] A presentation of a group G is a pair $\langle S \mid R \rangle$ where S is a set of symbols and R is a subset of (reduced) words in $S \cup S^{-1}$ such that $\mathbb{F}(S)/\langle\langle R \rangle\rangle \cong G$, where $\mathbb{F}(S)$ denotes the free group over the set S and $\langle\langle R \rangle\rangle$ denotes the smallest normal subgroup containing all elements of the collection R.

3. The Mapping Class Group

3.1. An unexpected help

In the attempt of applying geometric and topological techniques to group-based cryptography, we first studied one of the most interesting protocols of the NIST Post-quantum standardization: the candidate SIKE (Supersingular Isogeny Key Encapsulation), the unique candidate using Isogeny-based Cryptography. SIKE can be thought as the Post-quantum evolution of Elliptic Curve Cryptography. A description of the protocol SIKE is beyond the scope of this note (the webpage [19] contains an exhaustive repository of research papers as well as expository papers concerning SIKE and more generally Isogeny-based cryptography). That being said we want to focus on one foundational aspect: the notion of *Hard Homogeneous Space*.

Hard Homogeneous Spaces were introduced by Couveignes in [1]. His (unpublished) paper contains also a first Isogeny-based protocol. The intuition of Couveignes is the abstract paradigm on which SIKE have been built. Let us consider a group G acting on a space X, transitively and freely; we give some preliminary definitions:

Vectorization Problem: Given two points $x_1, x_2 \in X$ find the unique element $g \in G$ such that $g.x_1 = x_2$.

Parallelization Problem: Given three points $x_1, x_2, x_3 \in X$ find the unique point x_4 such that $g.x_1 = x_2$ and $g.x_3 = x_4$, for some $g \in G$.

We are thus ready to explain what a Hard Homogeneous Space is:

Hard Homogeneous Space (HHS): a *Hard Homogeneous Space* or *HHS* fis a pair (G, X) where G is a finite commutative group, and X is a space on which G acts transitively and freely, where there exist efficient algorithms for the following operations:

- Compute inverses and products of elements of G and equality testing in G;
- Random sampling from G with uniform probability;
- Decide whether a given string represents an element in X;
- Test equality in X;
- Compute the action $G \curvearrowright X$;

but the Vectorization Problem and the Parallelization Problem are computationally infeasible.

The original idea of Couveignes (later, though independently, rediscovered by Rostovtsev and Stolbunov — [20], [21]—) was to look at the action of isogenies onto Ordinary Elliptic Curves, with a set of isogenous ordinary elliptic curves to play the role of the HHS for the group of isogenies. The work of Childs-Jao-Soukharev [24] pointed out that Isogeny-based schemes on Ordinary Elliptic Curve are susceptible to quantum attacks. A different key exchange involving Supersingular Elliptic Curves had successively been proposed by De Feo-Jao-Plût [22] (see also the corresponding extended version [23]) and eventually led to SIKE. The work of

Childs-Jao-Soukharev [24] pointed out that Isogeny-based schemes on Ordinary Elliptic Curve are susceptible to quantum attacks, a problem which is circumvented by the deployment of Supersingular Elliptic Curves.

At this level of abstraction there are several remarks to make:

1. While the transitivity of the action of the group G on X can be seen as a *minimality* assumption (otherwise we could just restrict ourselves to a G-orbit in X), the freedom of the action is useful if our objective is to produce a "non-algebraic copy" of the group G. If we drop the assumption we are in a situation where we have some redundancy in the group action $G \curvearrowright X$ (for example several solution to the parallelization equation $g.x_1 = x_2$, *i.e.* non-trivial stabilizers). Can we benefit from the presence of non-trivial stabilizers?
2. Commutativity does not play any role in the definition of HHS. Though abelian groups are certainly more studied than their non-abelian siblings from the computational point of view, the assumption can be dropped.
3. The finiteness assumption on G (and thus on X) interact with the requirement of the existence of efficient algorithms for random sampling with uniform probability. If we want to drop the finiteness assumption we should replace the uniform probability with some different condition.

Taking into account these comments, it is clear that the framework provided by HHS is extremely general and it seems that it could be well adapted to infinite, possibly non-abelian, finitely generated groups. This provides an additional motivation to construct cryptoschemes involving group actions. It is therefore legitimate to ask ourselves whether there exists a concrete example of non-commutative, infinite group action onto a suitable space which could represent a sort of HHS in the generalized sense suggested by the previous remarks.

3.1.1. Group actions and lattice-based cryptography

Though not directly linked or even inspired by Couveignes' notion of HHS, protocols arising in Lattice based Cryptography do not make exception from the paradigm of hiding the algebra via a "group action". Here we briefly describe GGH algorithm ([25]) as it is presented in [26], pg. 167. In such a protocol each legitimate party possesses a secret key which is represented by a good basis $\mathcal{B}$ (composed by almost orthogonal vectors) for a lattice $\mathscr{L}(\mathcal{B}) < \mathbb{R}^n$, and a public key which is represented by a "bad basis" $\mathcal{B}_{bad}$ of the same lattice. Suppose that Alice wants to construct a shared key with Bob. Then she chooses a short noise vector $\mathbf{r}$; she takes the bad basis $\mathcal{B}_{bad}$, she chooses a point $\mathbf{v}$ in the lattice $\mathscr{L}(\mathcal{B}_{bad})$ and she publishes $\mathbf{w} = \mathbf{v} + \mathbf{r}$. As the bad basis chosen by Bob is particularly inconvenient and the information published by Alice is "noisy", the instance of the Closest Vector Problem that a potential eavesdropper is forced to solve is computationally infeasible. Viceversa as Bob possesses the good basis, he is able to efficiently solve the Closest Vector Problem, which allows him to find the vector $\mathbf{v}$, as the closest point to $\mathbf{w}$ in $\mathscr{L}(\mathcal{B})$. Once found $\mathbf{v}$ Bob is able to retrieve the original noise vector chosen by Alice $\mathbf{r} = \mathbf{w} - \mathbf{v}$. This naïve description of a Lattice-based protocol, is to highlight that Lattice based cryptography is built on the idea of exploiting a group action (the action of the abstract group given by the integer lattice $\mathbb{Z}^n$) on a suitable space (the Euclidean space $\mathbb{R}^n$). In particular for what concerns the protocol we just described, the idea is to hide the shared key using a perturbation of the shared key together with a choice of a vector obtained from a public basis (a generating system for the group $\mathscr{L}(\mathcal{B})$ which has be chosen to be different from the secret basis of the other legitimate party) which makes computations for the recovery of the secret noise vector infeasible. We observe that this is a rather general and flexible schema which can be adapted to many other interesting group actions.

3.2. Homeomorphisms of surfaces

A natural candidate to provide a link between Group-based cryptography and the Geometry and Topology of low-dimensional manifolds is the Mapping Class Group of a closed surface S of genus $g \geq 2$. The Mapping Class Group of S (usually denoted $Mod(S)$ or $\mathrm{MCG}(S)$) is the group of orientation preserving homeomorphisms of S considered up to homeomorphisms isotopic to the identity of S. It is one of the most studied groups in Geometric Topology and Geometric Group Theory. The more direct introduction to subject, to our knowledge, is the book by Farb and Margalit ([27]). Due to lack of space we shall only try to give an heuristic idea of certain basic concepts, and briefly recall some of the properties which are relevant to our purposes. The group $Mod(S)$ is a finitely presented group; we shall not give the presentation (see [27]), but we shall exhibit a finite generating set. A *Dehn twist* about the isotopy class of a simple, essential closed curve $[\alpha]$ in the surface S (an embedded curve in S which is not homotopic to a point in S) is the mapping class $T_{[\alpha]}$ corresponding to the following homeomorphism of S: the map is the identity map outside an annulus $A(\alpha)$ whose core is a representative of α, and it is isotopic to the following map inside $A(\alpha)$:

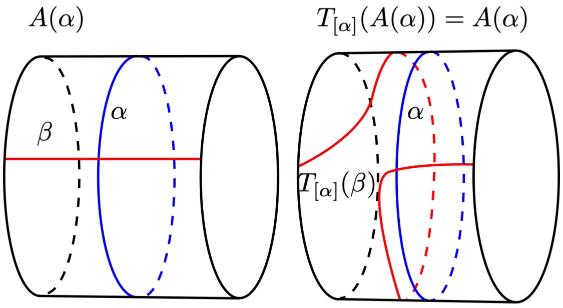

Figure 1: The action of the Dehn twist $T_{[\alpha]}$ about α on a curve β crossing α inside the annulus $A(\alpha)$.

It was proven in 1964 by Lickorish ([28]) that the Dehn twists corresponding to the homotopy classes of curves in Figure 2 generate the Mapping Class Group:

The Mapping Class Group has several interesting properties. First of all it is a group of exponential-growth, meaning that, for any choice of a finite generating set Σ the number of elements of $Mod(S)$ in the ball of radius n (with respect to the word metric[2] induced by Σ)

[2] Let Σ be a finitely generating set for a group $G = \mathbb{F}(\Sigma)/\langle\langle R\rangle\rangle$. The word metric on G relative to Σ measures

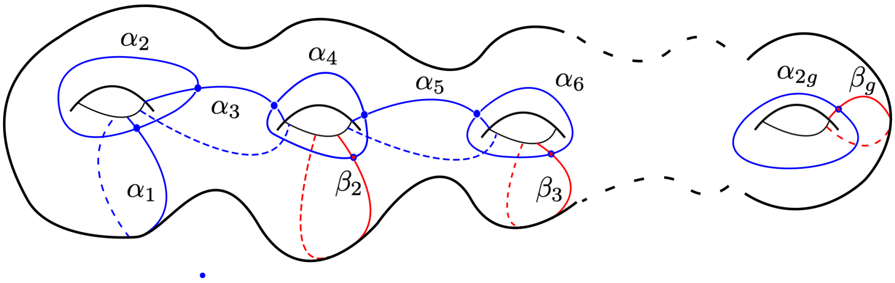

Figure 2: The Dehn-Lickorish generating system for $Mod(S)$.

is an exponential function of n. The group contains many interesting subgroups: free groups, braid groups and $\mathbb{Z}^k$ for every $k \leq 3g - 3$. There exist efficient algorithms to compute inverses as well as products of mapping classes and a linear time algorithm for the Word Problem, *i.e.* the problem of recognizing whether a given mapping class represents the identity element or not, which means that there exists an efficient algorithm to check equality between mapping classes. For what concerns measures on finitely generated, infinite, non abelian groups and suitable notions of complexity in this context they are extensively discussed in [9]. The Mapping Class Group possesses several interesting actions, two of them are particularly significant and played a central role in the understanding of the group itself:

1. the action of $Mod(S)$ on S;
2. the action of $Mod(S)$ on the Curve Graph.

The action of $Mod(S)$ on S shows us that certain mapping classes called “pseudo-Anosov" have a highly mixing behaviour: they possess a dense orbit, the number of periodic point of S with respect to a given transformation is dense in S and they have relevant measure-theoretic mixing properties. On the other hand, it is possible to show that random walking on the Cayley graph of $Mod(S)$ we stop at a pseudo-Anosov mapping class (see [27], Ch. 14) with asymptotic probability 1. As randomness lies at the very core of cryptography, this partially justify the idea to look at $Mod(S)$ for cryptographic purposes.

The Curve Graph $\mathscr{C}(S)$ is a simplicial graph whose vertices are given by isotopy classes of essential, simple closed curves. We put an edge of length 1 between two (distinct) isotopy classes $[\alpha]$, $[\beta]$ if they possess disjoint representatives. It turns out that $\mathscr{C}(S)$ is an infinite graph, having infinite diameter and where each vertex has infinite valence, *i.e.* there are infinitely many edges based at every vertex. The action of $Mod(S)$ onto $\mathscr{C}(S)$ is a simplicial action. There is an interesting correspondence between the Vectorization Problem on the pair $(Mod(S), \mathscr{C}(S))$ and the Conjugacy Search Problem on $Mod(S)$, for which the fastest known algorithms run in exponential time. On the other hand computational aspects of the Mapping Class Group and of its action on simple closed curves have been investigated over the last 15 years by

the distance between two elements $g_1, g_2 \in G$ as equal to the shortest length in terms of letters in $\Sigma \cup \Sigma^{-1}$ of a word in $\mathbb{F}(\Sigma)$ representing $g_1^{-1}g_2$.

several authors ([16], [17], [29], [30], [18], [31], [32]), so there is a set of linear/polynomial time algorithms at our disposal to perform elementary operations on the Curve Graph.

Among all the mentioned characteristics of the Mapping Class Group and the properties of its action of the Curve Graph, the existing link between the CSP on the Mapping Class Group and the Vectorization Problem for the action $Mod(S) \curvearrowright \mathscr{C}(S)$ is certainly the most inspiring. We are currently investigating the possibility to exploit this correspondence.

4. Conclusions

Decisional and Search problems on non-commutative (infinite) groups is one of the areas where quantum algorithms have not provided yet computational advantage. Despite difficulties of non-commutative group based cryptography to present efficient and secure concrete protocols, it seems that some of the abstract ideas underlying other areas such as Isogeny based and Lattice based cryptography could be a source of inspiration for new research directions and possibly concrete implementations. In particolar, non-commutative, infinite group actions protocols could present some advantage in comparison with to the pure group theoretic approach to cryptography. On the other hand, if we look at non-commutative group actions it is natural to look at topology and geometry as a source of those action. We thus identified the Mapping Class Group as one promising candidate in view of its complexity as a group, of its extremely involved actions on both surfaces and on the Curve Graph, and on the fact that we have reasonably efficient algorithms at our disposal. One of the activities we are carrying on at Leonardo Cybersecurity is the development of non-commutative group action based cryptoschemes, with particular reference to the Mapping Class Group.

References

[1] J. M. Couveignes, Hard homogeneous spaces (2006). URL: http://eprint.iacr.org/2006/291, preprint, Cryptology ePrint Archive, Report 2006/291.

[2] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proc. 35th Annual Symp. on Foundations of Computer Science, Santa Fe, IEEE Computer Society Press,, 1994, pp. 124–134.

[3] P. Shor, Polynomial time algorithms for discrete logarithms and factorization on a quantum computer, SIAM Journal of Computing 26 (1997) 1484–1509.

[4] K. Hartnett, Quantum supremacy is coming: here's what you should know, Blog post, 2019. URL: https://www.quantamagazine.org/quantum-supremacy-is-coming-heres-what-you-should-know-20190718/, quanta Magazine.

[5] NIST, Post-quantum cryptography standardization, 2017.

[6] M. R. Magyarik, N. R. Wagner, A public key cryptosystem based on the word problem, in: Advances in Cryptology – CRYPTO 1984, volume 196 of *Lecture Notes in Computer Science*, Springer-Verlag, London, 1985, pp. 19–36.

[7] I. Anshel, M. Anshel, D. Goldfeld, An algebraic method for public key cryptography, Math. Research Letters 6 (1999) 1–5.

[8] K. H. Ko, S. J. Lee, J. H. Cheon, J. W. Han, J. Kang, C. Park, New public-key cryptosystem using braid groups, in: Advances in Cryptology – CRYPTO 2000, volume 1880 of *Lecture Notes in Computer Science*, Springer-Verlag, London, 2000, pp. 166–183.

[9] A. Myasnikov, V. Shpilrain, A. Ushakov, Group-based Cryptography, Adv. Courses in Math. CRM Barcelona, Birkhauser, 2008. Pp. XV+ 183.

[10] J. Gryak, D. Kahrobaei, The status of polycyclic group-based cryptography: A survey and open problems, Groups Complexity Cryptology 8 (2016) 171–186.

[11] S. Y. W. Z. J. Suo, L. Wang, J. Zhang, Quantum algorithms for typical hard problems: a perspective of cryptanalysis, Quantum Information Processing 19 (2020). 26pp.

[12] M. Gromov, Structure métriques pour les variétés riemanniennes, volume 1 of *Textes Mathématiques*, CEDIC, 1981. Edited by J. Lafontaine and P. Pansu.

[13] M. Gromov, Groups of polynomial growth and expanding maps, Publications Math. IHES 53 (1981) 53–78.

[14] M. Gromov, Hyperbolic groups, volume 8 of *Essays in Group Theory*, Springer, New York, NY, 1987.

[15] M. Gromov, Geometric group theory. asymptotic invariants of infinite groups. volume 2, volume 182 of *London Mathematical Society Lecture Notes Series*, Cambridge University Press, 1993.

[16] M. Schaefer, E. Sedgwick, D. Stefankovic, Algorithms for normal curves and surfaces, in: O. H. Ibarra, L. Zhang (Eds.), COCOON, volume 2387 of *Lecture Notes in Computer Science*, Springer-Verlag, London, 2002, pp. 370–380.

[17] M. Schaefer, E. Sedgwick, D. Stefankovic, Computing dehn twists and geometric intersection numbers in polynomial time, in: Proc. 20th Annual Canadian Conference on Computational Geometry, 2008, pp. 111–114. Full version: Technical Report 05–009, Computer Science Department, DePaul University. April 2005. http://facweb.cs.depaul.edu/research/techreports/abstract05009.htm.

[18] M. C. Bell, Simplifying triangulations (2016). ArXiv:1604.04314v2.

[19] Supersingular isogeny key encapsulation (sike), website, 2017. URL: https://sike.org.

[20] A. Stolbunov, Public-key ecnryption based on cycles of isogenous elliptic curves, Master's thesis, Saint-Petersburg State Polytechnical University, St. Petersburg, RU, 2004. In russian.

[21] A. Rostovstev, A. Stolbunov, Public-key cryptosystem based on isogenies (2006).

[22] L. D. Feo, D. Jao, Towards quantum-resistant cryptosystems from supersingular elliptic curves isogenies, in: PQCrypto, volume 7071 of *Lecture Notes in Computer Science*, Springer-Verlag, London, 2011, pp. 19–34.

[23] L. D. Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curves isogenies (2011). URL: htttps://eprint.iacr.org/2011/506.

[24] A. Childs, D. Jao, V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, J. Math. Cryptology 8 (2014) 1–29.

[25] O. Goldreich, S. Goldwasser, S. Halevi, Public-key cryptosystems from lattice reduction problems, in: Advances in Cyrptology, volume 1294 of *Lecture Notes in Computer Science*, Springer-Verlag, London, 1997, pp. 112–131.

[26] D. J. Bernstein, J. Buchmann, E. D. (eds.), Post-Quantum Cryptography, 2nd. ed., Springer, 2009. IX+245 pages.

[27] B. Farb, D. Margalit, A Primer on The Mapping Class Group, volume 39 of *Princeton Mathematical Series*, Princeton University Press, 2012.

[28] W. B. R. Lickorish, A finite set of generators for the homeotopy group of a 2-manifold, Proc. Cambridge Philos. Soc. 60 (1964) 769–778.

[29] J. Erickson, A. Nayyeri, Tracing compressed curves in triangulated surfaces, Discrete Comput. Geom. 49 (2013) 823–863.

[30] M. C. Bell, The pseudo-anosov and conjugacy problems are in $\mathbf{NP} \cap co{-}\mathbf{NP}$ (2014). ArXiv:1410.1358.

[31] M. C. Bell, R. C. H. Webb, Applications of fast triangulation simplification (2016). ArXiv:1605.03514.

[32] M. C. Bell, R. C. H. Webb, Polynomial-time algorithms for the curve graph (2016). ArXiv:1609.09392.