Post Quantum Cryptography from Mutant Prime Knots

Annalisa Marzuoli[(1)] and *Giandomenico Palumbo*[(2)]

Dipartimento di Fisica Nucleare e Teorica, Università degli Studi di Pavia
and Istituto Nazionale di Fisica Nucleare, Sezione di Pavia
via A. Bassi 6, 27100 Pavia (Italy)
[(1)] E-mail: annalisa.marzuoli@pv.infn.it
[(2)] E-mail: giandomenico.palumbo@pv.infn.it

Abstract

By resorting to basic features of topological knot theory we propose a (classical) cryptographic protocol based on the 'difficulty' of decomposing complex knots generated as connected sums of prime knots and their mutants. The scheme combines an asymmetric public key protocol with symmetric private ones and is intrinsecally secure against quantum eavesdropper attacks.

PACS2008:
89.70.-a (Information and communication theory)
02.10.kn (Knot theory)
03.67Dd (Quantum Cryptography and communication security)

MSC2010:
68QXX (Theory of computing)
57M27 (Invariants of knots and 3-manifolds)
68Q17 (Computational difficulty of problems)

1 Introduction

Knots and links (collections of knotted circles), beside being fascinating mathematical objects, are encoded in the modeling of a number of physical, chemical and biological systems. In particular it was in the late 1980 that knot theory was recognized to have a deep, unexpected interaction with quantum field theory [1]. In earlier periods of the history of science, geometry and physics interacted very strongly at the 'classical' level (as in Einstein's General Relativity theory), but the main feature of this new, 'quantum' connection is the fact that geometry is involved in a global and not purely local way, *i.e.* only 'topological' features do matter. Over the years mathematicians have proposed a number of 'knot invariants' aimed to classify systematically all possible knots. Most of these invariants are polynomial expressions (in one or two variables) with coefficients in the relative integers. It was Vaughan Jones in [2] who discovered the most famous polynomial invariant, the Jones invariant, and solved the Tait's conjectures for alternating knots. In the seminal paper by Edward Witten [1], the Jones polynomial was actually recognized to be associated with the vacuum expectation value of a 'Wilson loop operator' in a quantum Chern–Simons theory (see the rewiews [3], [4] for comprehensive accounts on these topics).

Seemly far from the above remarks, the search for new algorithmic problems and techniques which should improve 'quantum' with respect to classical computation is getting more and more challenging in the last decade. Most quantum algorithms are based on the standard quantum circuit model [5], and are designed to solve problems which are essentially number theoretic such as the Shor's algorithm [6] (see [7] for a general review on the basics of quantum algorithms). However, other types of problems, typically classified in the field of enumerative combinatorics and ubiquitous in many areas of mathematics and physics, share the feature to be 'intractable' in the framework of classical information theory. In particular the evaluation of the Jones polynomial has been shown to be #**P**–hard, namely computationally intractable in a very strong sense [8]. In this perspective, efficient quantum algorithms for computing approximately knot invariants (of the Jones' type or extensions of it) have been successfully addressed in the last few years [9], [10, 11, 12], [13] and indeed such problem has been recognized to be 'universal' in the quantum complexity class **BQP** (**B**ounded error **Q**uantum **P**olynomial), namely the hardest problem that a quantum computer can efficiently handle [14].

Notwithstanding the improvements outlined above both in field–theoretic settings and in quantum complexity theory, the basic unsolved problem in topological knot theory still remains the 'recognition problem'. Namely, given two knots, how can we check if they are 'equivalent' (in the sense to be formalized in the next section). Invariants of (oriented) knots might be useful to this task, but there exist particular classes of knots –the 'mutants' of a given knot– that cannot be distinguished *in principle* since by definition all of them possess the same Jones' type invariants, a result derived by resorting to standard tools in combinatorial topology (see *e.g.* [15]) but recognizable also in the field–theoretic framework as a property of expectation values of Wilson loop operators [16].

As is well known, group–based cryptography has became in the last few years a very fruitful branch of cryptoanalysis [17], [18]. In particular, the key–agreement protocol proposed in [19] can be implemented using the braid group $\mathbf{B}_n$ (a non–Abelian group on (n-1) generators that can be associated to geometric configurations of n interlaced strands whose endpoints are fixed on two parallel straight lines in the plane). Knots and braids are indeed closely interconnected since we can get a (multi–component) knot by 'closing' up an open braid, and a number of interesting algorithmic problems related to this group can be addressed [20]. Roughly speaking, a braid–group–based cryptographic protocol relies on the existence of an 'easy' problem (recognize whether two braids W and W', expressed algebraically in terms of generators of the braid group, are the same element) and an 'intractable' one (recognize whether two words W_1 and W_2 are conjugate to each other, namely if there exists a W' for which $W_2 = W'W_1(W')^{-1}$). As reviewed in [17], basic ingredients for implementing secure cryptosystem are the computational time required to execute the protocol, the number of bits that are to be exchanged between Alice and Bob, the number of passes (exchange of information), the sizes of keys and the sizes of system parameters. However modern security is often much more demanding, so that at present braid–group–based protocols [19, 21] do not seem safe from eavesdropper attacks.

The theoretically secure protocol we propose in this paper is framed within topological knot theory and the basic ingredients are 'prime' knots depicted in a standardized manner in Knot Tables currently available on the web. The scheme relies on the 'easy' problem of associating with prime knots in Knot Tables their Dowker–Thistlethwaite codes, numerical sequences which

are different for inequivalent knots. Then we resort to the 'difficulty' of factorizing, so to speak, complex knots generated by composing prime knots and their mutants. The scheme resorts to purely classical cryptographic tools, combining an asymmetric public key protocol with symmetric private ones.

The adjective 'post quantum' in the title comes about *a posteriori* in light of the fact that most currently popular public–key cryptosystems rely on the integer factorization problem or discrete logarithm problem (arising *e.g.* in the framework of cyclic group–based protocols), both of which would be easily solvable on large enough quantum computers using Shor's algorithm. Our protocol is not based on the quoted two problems, neither seems reducible to them, and thus the standard meaning of post–quantum –secure against 'quantum' attacks– can be taken for granted until someone will be able to prove the converse. In a somehow extended sense, and according to the remarks made above on quantum algorithms for computing knot invariants, an attack based on (quantum) calculations of such polynomials would fail in view of the presence of mutants, not detectable even by a quantum computer.

In section 2 we review in brief some basic notions in topological knot theory, while in section 3 the cryptographic protocol is presented. A few more comments and conclusions are collected in section 4.

2 Overview of Topological Knot Theory and coding of knot diagrams

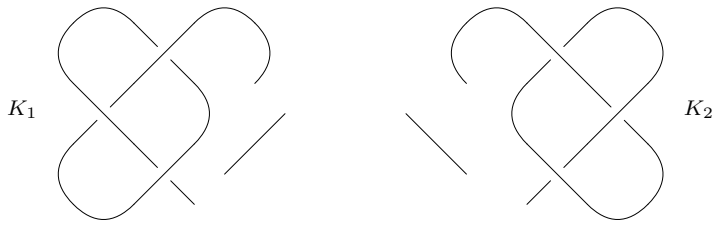
A *knot* K is defined as a continuous embedding of the circle S^1 (the 1–dimensional sphere) into the Euclidean 3–space $\mathbb{R}^3$ or, equivalently, into the 3–sphere $S^3 \doteq \mathbb{R}^3 \cup \{\infty\}$. A *link* L is the embedding of the disjoint union of M circles, $\cup_{m=1}^{M} (S^1)_m$ into $\mathbb{R}^3$ or S^3, namely a finite collection of knots. Since each circle can be naturally endowed with an orientation, we can introduce naturally *oriented* knots (links).

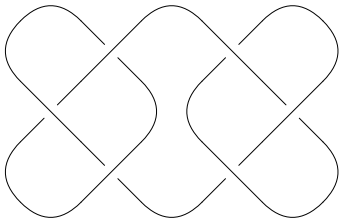
Referring for simplicity to the unoriented case, two knots K_1 and K_2 are said to be *equivalent*, $K_1 \sim K_2$, if and only if they are (ambient) isotopic. An isotopy can be thought of as a continuous deformation of the shape of, say, $K_2 \subset \mathbb{R}^3$ which makes K_2 identical to K_1 without cutting and gluing back the 'closed string' K_2.

The *planar diagram*, or simply the *diagram*, of a knot K is the projection

of K on a plane $\mathbb{R}^2 \subset \mathbb{R}^3$, in such a way that no point belongs to the projection of three segments, namely the singular points in the diagram are only transverse double points. Such a projection, together with 'over' and 'under' information at the crossing points –depicted in figures by breaks in the under–passing segments– is denoted by $D(K)$. In what follows we shall identify the symbols K with $D(K)$, although we can obviously associate with a same knot an infinity of planar diagrams.

The number of crossings of a knot (diagram) is clearly a good indicator of the 'complexity' of the knot and indeed Tait in late 1800 initiated a program aimed to classifying systematically knots in terms of the number of crossings. In Knots Tables (see [22] and the *Knot Atlas* on Wikipedia) there appear diagrams of unoriented 'prime' knots listed by increasing crossing numbers as $\digamma_N$, where $\digamma$ is the number of crossings and $N = 1, 2, \ldots$ enumerates in a conventional way the (standard projections of) knots with the same $\digamma$. The (unique) 'unknot' or trivial knot $K_\bigcirc$ has standard projection given by the circle, *i.e.* $\digamma_N(K_\bigcirc) = 0$ with $N = 1$. A prime knot is defined as a non–trivial knot which cannot be decomposed into two (or more) non–trivial knots. Decomposition is in turn the inverse of the topological operation of composition of knot diagrams. More precisely, given two knot diagrams K_1 and K_2, it is possible to draw a new knot by removing a small segment from each knot and then joining the four endpoints by two new arcs. The resulting diagram is the *connected sum* of K_1, K_2, denoted by $K_1 \# K_2$. As shown below, starting for instance from the diagrams of the trefoil knot K_1 (configuration 3_1 in Knot Tables) and its mirror image K_2, their connected sum turns out to be the so–called 'square' knot, the six–crossings configuration listed as 6_2.

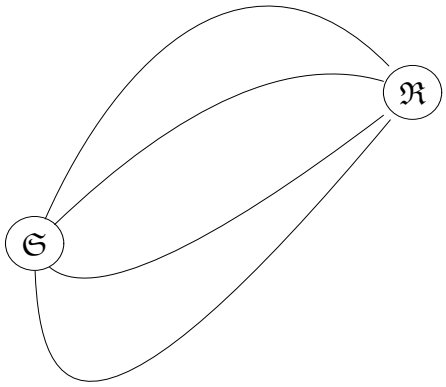




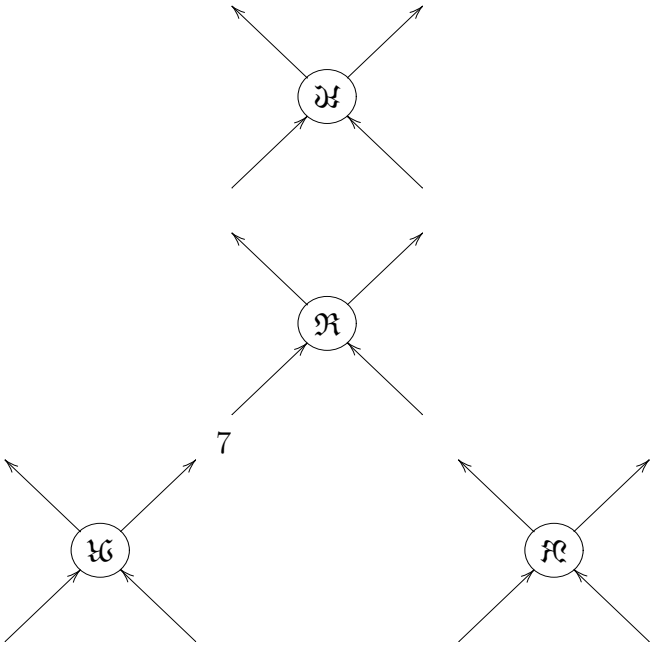
The connected sum of knot diagrams (well defined for oriented knots) is commutative and associative and has an identity element given by the trivial knot $K_{\bigcirc}$, namely $K_{\bigcirc} \# K = K$ for each K. Remarkably, to each diagram representing a composite knot it is possible to associate a decomposition into prime knots which is unique [23] –up to ordering of summands. The (minimal) crossing number used for building up Knot Tables is the first example of a numerical knot 'invariant' since it depends only on the ambient isotopy class of the knot. Switching to knot (link) diagrams, it can be proved that a knot invariant is a quantity (a number or a polynomial, see below) which does not change under applications to the diagrams of finite sequences of the so–called Reidemeister moves (we leave aside this issue and refer to the classic books [24, 15, 25, 26] also as general references on knot invariants). It is not difficult to recognize that polynomial invariants can take the same value on inequivalent knots, and it is the biggest open problem in knot theory to establish a 'complete' set of invariants able to distinguish (and thus classify) all equivalence classes of knots. Most famous polynomial invariants of knots, such as Alexander polynomial, Jones polynomial [2] and its extensions [27] (in one formal variable) as well as HOMFLY [28] and Kauffman [25] polynomials (in two variables) are able to distinguish particular sub–classes or types of knots. Actually, even resorting to all of them, there exists quite a large number of examples (with relatively small crossing numbers) in which indistinguishable diagrams still remain. In particular, neither Jones, Kauffman and HOMFLY polynomials, nor more general invariants such as Reshetikhin–Turaev ones, are sufficient to distinguish *any* knot K from its mutations K' [15, 16].

To explain what is a 'mutant' knot we introduce first a 'tangle' notation for dealing with knot diagrams. A tangle is defined as a region of the planar diagram of an oriented or unoriented knot bounded by a circle (not belonging to the diagram) such that the knot strands cross the circle exactly four times. Thus any knot can be always presented by resorting to (at least) two tangles,

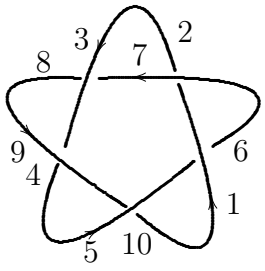
say $\mathfrak{S}$ and $\mathfrak{R}$, joined by 2+2 strands (this shorthand graphical notation for a single knot should not be confused with the operation of connected sum on knot diagrams).



Starting from a tangle presentation of an *oriented* knot K, a mutant K' arises by removing, *e.g.*, the tangle labeled by $\mathfrak{R}$ (two strands ingoing and two outgoing) and replacing it with a tangle $\mathfrak{R}'$ obtained by rotating $\mathfrak{R}$ (and reversing orientation of some strands if necessary). Admissible rotations are depicted below: the inner content of the tangle undergos π–rotations with respect to three mutually orthogonal axes which can be thought as pointing from the central configuration toward the other three embedded in a reference 3–space. Note that only two of these rotations are independent, but of course the process of mutation can be carried out at will on different subsets of a same knot diagram including at least one crossing.



In view of applications in cryptography we conclude this section by introducing Dowker–Thistlethwaite (DT) notation (or code) for oriented knots. This allows us to associated to each planar diagram its (minimal) DT sequence (actually a string of relative integers) from which it is possible to reconstruct (almost) uniquely the knot. Consider as an example an oriented alternating knot with n crossings (namely a diagram with an alternating sequence of over and under–crossings) and start labeling an arbitrary crossing with 1. Once fixed an orientation, go down the strand to the next crossing and denote it by 2. Continue around the knot until each crossing has been numbered twice. Then each crossing is decorated with a pair of even/odd positive numbers, running from 1 to 2n, as shown below for the knot 5_1.



For prime alternating knots the notation uniquely defines a single knot in case of amphichiral knots or corresponds to a single knot or its mirror image in case of chiral ones. (Recall that a chiral knot is a knot that is not equivalent to its mirror image while an oriented knot that is equivalent to its mirror image is an amphichiral knot). For generic, non–alternating prime knots (which actually appear in tables for crossing numbers greater than 7), the Dowker–Thistlethwaite coding is slightly modified by making the sign of the even numbers positive if the crossing is on the top strand, and negative if it is on the bottom strand. Since any Dowker sequence is dependent on both a minimal projection and the choice of a starting point, the mapping between knots and their DT sequences is one–to–many, so it would be necessary to find a minimal DT sequence for each (composite) knot. Hence DT codes are to be interpreted as minimal permutations of strings of relative integers representing certain knot diagrams, not carrying significant topological information about knots (so that they are useless in any attempt of knot classification).

Summing up, the assignment of Dowker–Thistlethwaite codes to prime knots enumerated in currently available Knot Tables (up to 17 crossings) is

essentially unique and the length of these numerical strings (plus possibly $\pm$ signs) grows linearly with the crossing number.

3 Cryptography using knots

Let us remind some basics facts about RSA cryptosystem, the most famous protocol of all times invented by Rivest, Shamir and Adleman [29] and based on the concept of 'asymmetric' public key. Imagine that A (Alice) must send a secret message to B (Bob). It would take the following steps:

1. B generates a public key χ by resorting to a certain set of 'generators'.
2. B sends the public key to A. Anyone can see it.
3. A uses the key to encrypt the message $\mathcal{M}$;
4. A sends the encrypted message $\mathcal{M}^{\chi}$ to B, but none can decrypt it.
5. B receives the message $\mathcal{M}^{\chi}$ and, knowing the generators, is able to decrypt it.

Actually most RSA–type protocols are based on the computational complexity of factorization of prime numbers, because the generators are two large prime numbers (p and q) and the public key is the product of them (N = pq). Once given N, decrypting the message needs the knowledge of its prime factors, and this is of course a computationally hard problem. Note however that public key algorithms are very costly in terms of computational resources. The time it takes the message to be encoded and decoded is relatively high and this is actually the main drawback of (any) asymmetric decoding. This problem can be overcome or even solved by using a symmetric key together with the asymmetric one, as we are going to illustrate in the following statements defining our knot–based cryptosystem.

A must send a secret message to B and they share the same finite list of prime knots K's. The message $\mathcal{M}$ will be built by resorting to a finite sequence of (not necessarily prime) knots $L_1, ..., L_N$ as described below

step I) Through a standard RSA protocol, B sends to A an ordered sublist of N prime knots (taken from current available Knot Tables) $K_1, ..., K_N$,

together with mutation instructions to be applied to each K_i (also no mutation on some of them is allowed). Then a second list $K'_1, ..., K'_N$ is generated by picking up definite mutations of the original sequence.

step II) A takes $K'_1, ..., K'_N$ and performs a series of ordered connected sums

$$L_1 \# K'_1,\ L_2 \# K'_2,\ \ldots,\ L_N \# K'_N$$

with the knots $L_1, ..., L_N$ associated with the message to be sent. These composite knots are now translated (efficiently) into Dowker–Thistlethwaite sequences and sent to B. Obviously at this stage everyone has access to these strings of relative integers.

step III) B receives the (string of) composite knots. Since he knows the DT sub–codes for the prime knots of the shared list, he can decompose the composite knots, thus obtaining the DT code for every L_i. Then the planar diagrams of $L_1, ..., L_N$ can be uniquely recovered.

Basically we are using in the protocol both a public key (step I) and a private key (step II). In fact the message is encrypted (by A) and decrypted (by B) using the same key, the sequence of prime knots that they share (secretly) thanks to step I.

4 Discussion and conclusions

There are a number of advantages in basing a cryptosystem on complex geometric structures such as knots, where the selected prime knots could be looked at as providing an encryption alphabet. Note first that the coding procedure that provides the Dowker–Thistlethwaite string (*e.g.* written in the standard binary notation) is efficiently implementable since it grows linearly with the crossing number. As noted above, decomposing a composite knot in its prime components is at least as difficult as finding the prime factors of a large number, while of course the composition (corresponding to multiplying integers) is an easy task. In order to attack such kind of protocol, one might resort to two strategies.

• The first approach is based on the use of topological invariants which provide, at least in case of low crossing numbers, quite a lot of information.

Looking at Knot Tables we note that, up to seven crossings, all knots are alternating, so that, in particular, the crossing number of a knot built as a connected sum of alternating knots is the sum of the individual crossing numbers (but this is not true for non–alternating knots). On the other hand, most powerful knot polynomials (quoted in section 2) are multiplicative with respect to connected sums. So, for instance, we can evaluate [25] the Jones invariant $J_K(t)$ of a given composite knot K getting a (Laurent) polynomial in the formal variable t, but still it is a hard task to extract the polynomials associated with the prime factors of K. As a matter of fact, such a strategy based on knot invariants is effectively unfeasible because topological invariants of polynomial type are not able to distinguish a (generic) knot from one of its mutations.

• Another way is to try to decompose the knot diagram containing the message by resorting to iterated combinatorial operations aimed to recognize in the encrypted message $L_1\#K'_1,\ L_2\#K'_2,\ \ldots, L_N\#K'_N$ at least some of the prime knots in the public list. But there exists no known algorithm to address the decomposition problem of a generic knot into its prime components. Finally, as pointed out in section 2, it is certainly true that the recognition problem can be associated with combinatorially recursive procedures, but Haken [30] was able to prove only the existence of an algorithm running in exponential time. On the other hand, the unknotting problem [31] –a particular case of the recognition problem stated in term of comparison of a given knot K with the unknot $K_{\bigcirc}$– is shown to belong to the complexity class **NP** [32, 33].

The new knot–based cryptographic protocol proposed in this paper relies on quite simple mathematical notions and needs of course to be further specified and checked against different types of attacks. Note however that techniques developed within the framework of braid group–based cryptography (see [17], section 4) do not seem to be implementable in such a purely topological setting[1].

[1] It is worth recalling that the set of (prime) knots equipped with connected sum # is an Abelian semigroup (actually a monoid, the unknot being the identity element). On the other hand, closed braids representative of a given knot diagram exist, but they are certainly not unique. Actually the problem of finding out the 'minimal' braid index for a knot K –namely the minimum number n such that there exists a braid $W \in \mathbf{B}_n$ whose closure reproduces K– is again a hard problem, *cfr.* section 4 of [20]. Then the knot–based protocol is not effectively reducible to the group–based approach to classical cryptography.

In conclusion, it seems quite promising that, besides brute force attacks which would be exponential resources consuming as the topological complexity of the knots grows, more sophisticated attacks based on (exact or approximate, classical or quantum) calculations of polynomial invariants of knots are intrinsically unreliable.

Acknowledgments

A special debt of gratitude goes to Chiara Macchiavello and Claudio Dappiaggi for useful conversations.

References

[1] Witten E 1989 *Commun. Math. Phys.* **121** 351

[2] Jones V F R 1985 *Bull. Amer. Math. Soc.***12** 103

[3] Kaul R K, Govindarajan T R and Ramadevi P 2005 Schwarz type topological quantum field theories *Encycl. Math. Phys.* (Amsterdam: Elsevier) *eprint* arXiv: hep-th/0504100

[4] Boi L 2009 *Int. J. Geom. Meth. in Mod. Phys.* **6** 1

[5] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge University Press)

[6] Shor P 1994 Algorithms for Quantum Computation: Discrete Logarithms and Factoring in *Proc. 35th Ann. Symp. Found. Comp. Sci.* 124.

[7] Cleve R, Ekert A, Henderson L, Macchiavello C, Mosca M 1998 *Complexity* **4** 33

[8] Jaeger F, Vertigan and Welsh D J A 1990 *Math. Proc. Camb. Phil. Soc.* **108** 35

[9] Aharonov D, Jones V and Landau Z 2006 A polynomial quantum algorithm for approximating the Jones polynomial, in Proc. STOC2006 427

[10] Garnerone S, Marzuoli A and Rasetti M 2006 *Op. Sys. Inf. Dyn.* **13** 373

[11] Garnerone S, Marzuoli A and Rasetti M 2007 *Quant. Inf. Comp.* **7** 479

[12] Garnerone S, Marzuoli A and Rasetti M 2007 *J. Phys A: Math. Theor.* **40** 3047

[13] Wocjan P and Yard J 2008 *Quant. Inf. Comp.* **8** 147

[14] Bordewich M, Freedman M, Lovasz L and Welsh D 2005 *Combinat. Prob. Comp.* **14** 737

[15] Lickorish W 1997 *An Introduction to Knot Theory* (Springer–Verlag, New York).

[16] Ramadevi P, Govindarajan T R, Kaul R K 1995 *Mod. Phys. Lett.* **A10** 1635

[17] Blackburn S R, Cid C and Mullan C 2009 Group theory in cryptography *eprint* arXiv:0906.5545v2

[18] González Vasco M I, Magliveras S and Steinwandt R 2010 *Group–theoretic cryptography* (Chapman & Hall / CRC Press)

[19] Anshel I, Anshel M and D. Goldfeld 1999 *Math. Res. Lett.* **6** 1

[20] Birman J S and Brendle T E 2004 *Braids: a survey* in *Handbook of Knot Theory* Menasco W and Thistlethwaite M eds (Amsterdam: Elsevier) *eprint* arXiv: mathGT/0409205

[21] Dehornoy P 2004 *Contemp. Math.* **360** 5

[22] Hoste J, Thistlethwaite M and Weeks J 1998 The first 1,701,935 knots *Math. Intelligencer* **20** 33

[23] Schubert H 1949 *S.-B Heidel. Akad. Wiss. Math.-Nat. Kl.* **3** 57

[24] Rolfsen D 1976 *Knots and Links* (Publish or Perish, Berkeley, CA).

[25] Kauffman L 2001 *Knots and Physics* (World Scientific, Singapore)

[26] Adams C 2004 *The Knot Book: An Elementary Introduction to the Mathematical Theory of Knots* (Amer. Math. Soc., Providence, RI)

[27] Reshetikhin N and Turaev V G 1991 *Invent. Math.* **103** 547

[28] Freyd P, Yetter D, Hoste J, Lickorish W, Millett K and Ocneanu A 1985 *Bull. Amer. Math. Soc.* **12** 183

[29] Rivest R, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120

[30] Haken W 1961 *Acta Math.* **105** 245

[31] Birman J and Hirsch M 1998 *Geom. Topol.* **2** 175

[32] Hass J, Lagarias J and Pippenger 1999 *J of the ACM* **46** 185

[33] Hass J 1998 *Cha. Sol. Fra.* **9** 569