Knot-based Key Exchange protocol

Silvia Sconza* and Arno Wildi†

University of Zurich, Zurich, Switzerland

Abstract

We propose a new key exchange protocol based on the Generalised Diffie-Hellman Key Exchange. In the latter, instead of using a group-action, we consider a semigroup action. In our proposal, the semigroup is the set of oriented knots in $\mathbb{S}^3$ with the operation of connected sum. As a semigroup action, we choose the action of the semigroup on itself through the connected sum. For the protocol to work, we need to use knot invariants, which allow us to create the shared secret key starting from the same knot represented in two different ways. In particular, we use finite type invariants. The security of the protocol is guaranteed by the hardness of decomposing knots in the semigroup.

Keywords: Generalised Diffie-Hellman Key Exchange, Public Key Cryptography, Knot Theory, Connected Sum, Finite Type Invariants, Semigroup Action, Semigroup-based Cryptography.

1 Introduction

Knots, which are ambient isotopy types of embeddings $\mathbb{S}^1 \hookrightarrow \mathbb{S}^3$ (see Figure 2 and Definition 2.1), were used by humankind since ancient times, at the latest since the invention of the shoelace. The mathematical study of knots however started with Lord Kelvin, hypothesizing that atoms are actually knots and molecules are links flowing in the aether. His collaborator Peter Tait then initiated the field of knot theory. The basic problem being: Given two knots, are they the same or not? Following the development of topology in the early 20th century, numerous knot invariants like the Alexander polynomial [39] were developed to give answers to this problem. The interest in knot theory rose when deep connections were found to the study of 3- and 4-manifolds. For example, knots were used to prove that there are exotic $\mathbb{R}^4$, i.e. manifolds that are homeomorphic but not diffeomorphic to $\mathbb{R}^4$ [15]. Jones and Witten revolutionized the field with the discovery of the Jones polynomial [20] and its relation to Quantum field theory [41] from which quantum topology emerged. These breakthroughs were followed by the discovery of Khovanov homology [22] and knot Floer homology [35], which vastly generalize the Jones and the Alexander polynomial and provide active fields of research.

In this paper we are mainly interested in two aspects of knot theory. The first is an operation called the connected sum (see Figure 5) that takes two oriented knots, cuts them open and glues

*silvia.sconza@math.uzh.ch
†arno.wildi@math.uzh.ch

them together, respecting the orientation, to produce a new oriented knot. It turns out that, with this operation, oriented knots form the abelian semigroup **Knots**. The second is a class of knot invariants (see Section 2.1.3) called finite type invariants. They have many interesting features, one of them being that they are efficiently computable.

In the last 30 years, applications of knot theory to other scientific disciplines were found. In chemistry, we can decide whether a molecule is chiral or not. Molecules can have very different properties depending on their chirality. In biology, one can study the knottedness of the DNA in a cell. And in quantum computing, one studies anyons which give naturally a braid that can be studied in knot-theoretic terms.

In the paper, we propose an application of knot theory in cryptography, in particular we propose a Key Exchange Protocol. We know of three instances where knots were considered in cryptography. After getting the Fields Medal, Jones was asked whether knotted antennas would help sending messages securely. Together with Przytycki they investigated the problem. More promising attempts were the protocol of Marzuoli and Palumbo in [28] and the secret-key agreement proposed by Zucker in [42]. In the first one, they are proposing a symmetric protocol, the weakness of which is that they have to agree in secret on as much information as is used to describe the message. The second one is more close to our proposal since it is also a Key Exchange Protocol, but the author is using knots in braid form (see Subsection 4.1.2). Moreover, the use of the Jones Polynomial allows us to break it, since it is multiplicative. We will discuss in Section 4 why it is necessary to avoid such invariants.

In cryptography, we are concerned with exchanging messages securely, i.e. in such a way that an eavesdropper outside the conversation cannot obtain the original message. To do this, the message is "reformed" using a cryptographic key and only the designated recipient can retrieve the original message again using a key (not necessarily the same one). One of the main problems facing cryptography is how to generate and exchange these keys (Key Exchange Problem). One of the most widely used ways is the Diffie-Hellman Key Exchange, proposed in [13] and described below in Protocol 2.20. The original protocol works for a finite cyclic group G (in the first proposal $G = \mathbb{F}_q^\times$), but it can be generalised using a group action or a semigroup action, obtaining the Generalised Diffie-Hellman Key Exchange, described below in Protocol 2.24. In our case, the semigroup that we consider is **Knots**. The semigroup action is the action of the semigroup on itself, through the connected sum.

In the past, several cryptosystems based on group-actions have been proposed. The most famous are the one proposed by Anshel, Anshel and Goldfeld [2] and Ko et al. [23], where the groups considered are the braid groups and the action is the conjugation, and the one proposed by Castryck et al. [11], known as CSIDH (Commutative Supersingular Isogeny Diffie-Hellman). The latter is part of Isogeny-based Cryptography; the set considered is that of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_p$, characterised by the fact that the ring of endomorphisms is an order $\mathcal{O}$ in an imaginary quadratic field. The acting group is the ideal-class group $\mathrm{cl}(\mathcal{O})$ which acts through the application of isogenies.

As we will see also in our case, the use of semigroup actions instead of group actions brings certain advantages. First of all, given the poorer algebraic structure, many attacks cannot be applied or generalised. Generic algorithms for the group case like Pollard's rho [37], Pollard's lambda [37] and Shank's baby-step-giant-step [40] require at some point the existence of inverses, which is not ensured in the case of semigroups.

The choice of considering **Knots** and the semigroup action on itself brings certain advantages. First of all, referring to the aforementioned attacks, no knot admits an inverse except for the trivial

one, i.e. the unknot $\mathcal{U}$, as stated in Proposition 2.6. Furthermore, in order to propose a well-defined cryptosystem, one must find a mathematical problem which is supposed to be computationally hard. Our cryptosystem is based on the difficulty of factoring a connected sum of knots while knowing one of the two knots used (Problem 2.14). The particularity of this problem is that it admits a unique solution, thanks to Proposition 2.7.

The paper is organised as follows. In Section 2 we give all the necessary preliminaries. It is divided in two subsections: in the first one, we give the preliminaries of Knot Theory and in the second one, there are the preliminaries related to Public-Key Cryptography. In Section 3, we describe our proposed new cryptosystem, with an indication of the size of the keys. Section 4 is dedicated to the cryptoanalysis; there we analyse both generic attacks for the semigroup action problem and knot theoretic attacks. Moreover, we briefly discuss the efficiency. Finally, we give a possible choice of parameters for a 128-bit security level and we conclude with some open questions.

Acknowledgement The authors would like to thank their respective advisors Joachim Rosenthal and Anna Beliakova for their generous support and their helpful suggestions. We would like to thank Léo Ducas for useful comments on a first draft of the paper. We are also extremely grateful to Chris Monico, who is working on an implementation of our cryptosystem and for useful comments that allowed us to obtain the final version of the paper, highlighting some problems with the first proposed obfuscation algorithm. It is also his idea to use a hash function and to compute not just one, but several finite type invariants of small degree. The second author would like to thank Peter Feller, Józef Przytycki and Daniel Tubbenhauer for interesting conversations on the use of knot invariants in cryptography.

2 Preliminaries

In this section we introduce the required topics for understanding the proposed cryptosystem. A reader coming from the knot-theory-side may skip the part on knots (although one might want to refresh the memory on finite type invariants from Section 2.1.3), while a reader coming from the cryptography-side may skip the part on cryptography.

2.1 Crash course on knots

We discuss the relevant notions and results from knot theory, but leave out most of the proofs. For a general introduction to knot theory we refer to [39].

2.1.1 Basic notions and problems from knot theory

Intuitively, knots are exactly what one expects them to be. We think of them as tied ropes where we glue the ends together and allow the rope to "wiggle". Let us start by giving a mathematically precise definition.

Definition 2.1. A *knot* is described by either of the following (equivalent) definitions.

1. Knots are smooth embeddings $\mathbb{S}^1 \hookrightarrow \mathbb{R}^3$, considered up to ambient isotopy. [1]

2. Knots are (finite) polygonal closed lines in $\mathbb{R}^3$, considered up to the Δ-move seen in Figure 1.

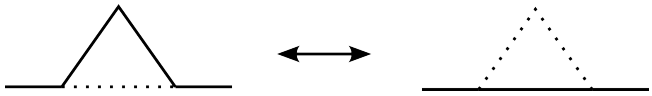


Figure 1: A local picture of the Δ-move.

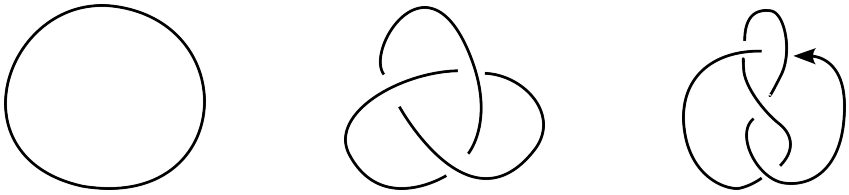


Figure 2: Some examples of knots (diagrams). The unknot $\mathcal{U}$, the (right-handed) Trefoil knot and the oriented Figure-Eight knot.

If one allows several components, one speaks of a link. Usually, we picture knots by *knot diagrams*. Some examples can be seen in Figure 2. They are generic projections of the knot to a plane allowing only singularities of a certain kind, called *crossings*. The complexity of a knot diagram can be measured by its number of crossings. Of course, a knot has many different diagrams, depending on its position in $\mathbb{R}^3$ and the chosen projection. The *Reidemeister theorem* allows us to handle this problem.

Theorem 2.2 (Reidemeister)**.** *Two knot diagrams represent the same knot if and only if they are related by planar isotopies and a finite sequence of the Reidemeister moves, represented in Figure 3.*

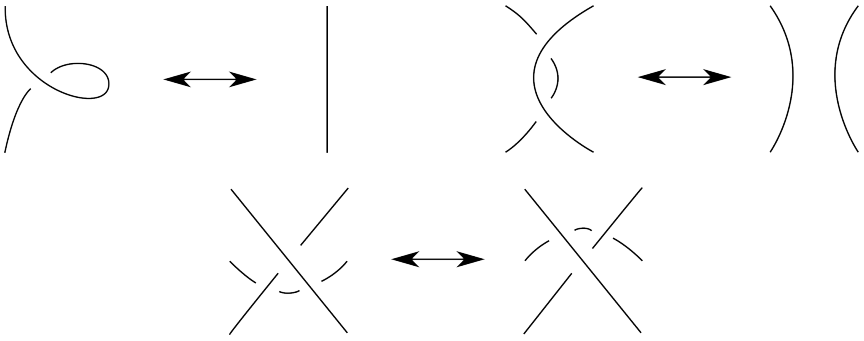


Figure 3: The three Reidemeister moves for knot diagrams.

[1] Two embeddings $g, h\colon N \hookrightarrow M$ are called ambient isotopic, if there is a continuous map (called ambient isotopy) $F\colon M \times [0,1] \to M$ such that $F_0 = id_M$ and $F_1 \circ g = h$.

Definition 2.3. When a knot is endowed with an orientation, it is called an *oriented knot*. There is a corresponding Reidemeister theorem for oriented knots. We distinguish two types of crossings called the positive and the negative crossing seen in Figure 4. The set of oriented knots is denoted by **Knots**.

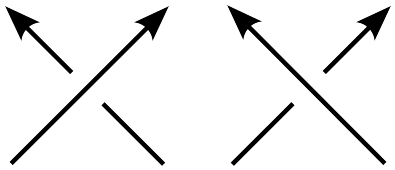


Figure 4: The positive and the negative crossing.

We consider the following operation on oriented knots.

Definition 2.4. Given two oriented knots K and K' we define the *connected sum* $K\#K'$ by cutting open the two knots and glueing the corresponding ends (given by the orientation) together as in Figure 5 to get a new knot.

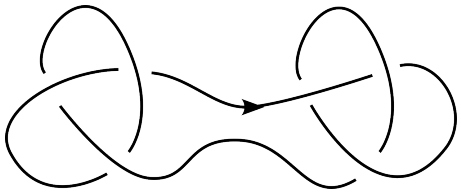


Figure 5: The connected sum of two Trefoil knots.

The connected sum of two knots is well defined, because cutting the knots at different spots results in isotopic knots. Note that it is not well defined for unoriented knots, since we have a choice, i.e. which arcs we glue together in the unoriented case. It is obvious that taking the connected sum with the unknot $\mathcal{U}$ yields an isotopic knot. The following Proposition is immediate.

Proposition 2.5. $(\mathbf{Knots}, \#, \mathcal{U})$ *form an abelian semigroup.*

We call a knot that cannot be written in a non-trivial way as the connected sum of two other knots *prime*. The semigroup of oriented knots has the following properties proven in [39].

Proposition 2.6. *Apart from the unknot, no knot has an inverse with respect to the connected sum.*

Proposition 2.7. *For any knot there is a unique (up to reordering) decomposition into prime knots.*

In general, it is hard to tell whether a knot is prime or not. But for a certain subset of knots, it is straightforward.

Definition 2.8. A knot diagram is called *alternating*, if the crossings alternate between under- and overpasses when travelling along the knot. A knot is called *alternating*, if it has an alternating diagram.

Not all knots are alternating. There are even prime knots which are not alternating. There are the following useful fact about alternating knots proven in [31] and [33].

Proposition 2.9. *An alternating knot diagram represents a prime knot if and only if the diagram "looks prime", which means that there is no circle that intersects the diagram in two points such that both, in the interior and the exterior of the circle there are crossings. Moreover, such an alternating prime diagram is minimal. i.e. there is no diagram of the knot with less crossings.*

This gives a method to generate random prime knots. With Schaeffer's algorithm, one can generate a random planar graph with n vertices in $\mathcal{O}(n)$ time. This will give a graph representing a link in general, but one can take the biggest component which is a knot. There is a unique (up to mirroring) way of making the diagram alternating. Then, one can take the biggest prime summand and this will give in practice a prime knot with $\frac{n}{2}$ to n crossings. This is implemented in the "SnapPy" program. An example of a randomly produced knot is seen in Figure 6.

A question to ask is, whether one gets enough knots this way, or if the set of alternating prime knots is comparably small. While Table 1 provides the number of small (alternating) prime knots, the following estimate, proven in [1], answers the previous question in our favour.

n	1	2	3	4	5	6	7	8	9	10	11	12
# n crossings prime knots	0	0	1	1	2	3	7	21	49	165	552	2176
# n crossings alternating prime knots	0	0	1	1	2	3	7	18	41	123	367	1288

13	14	15	16	17	18	19	20	21
9988	46972	253293	1388705	8053393	48266466	294130458	unknown	unknown
4878	19536	85263	379799	1769979	8400285	40619385	199631989	990623857

Table 1: The list of the number of (alternating) prime knots with n crossings.

Proposition 2.10. *Let* $\mathrm{K}(n)$ *be the number of knots with at most* n *crossings,* $\mathrm{PK}(n)$ *be the number of prime knots with at most* n *crossings, and* $\mathrm{APK}(n)$ *be the number of alternating prime knots with at most* n *crossings. We have the following estimate.*

$$4.45 \leq \liminf \mathrm{APK}(n)^{\frac{1}{n}} \leq \liminf \mathrm{PK}(n)^{\frac{1}{n}} \leq \liminf \mathrm{K}(n)^{\frac{1}{n}} \leq 10.40.$$

In cryptography, one is usually interested in problems that are hard to solve. Topology is full of such problems and, in particular, we have examples in knot theory.

Problem 2.11 (Unknotting Problem)**.** Given a diagram D, does it represent the unknot?

Problem 2.12 (Recognition Problem)**.** Given two knot diagrams D and D', do they represent the same knot?

Problem 2.13. Given a knot diagram D of a knot K, are there non-trivial knots K_1 and K_2 such that $K_1 \# K_2 = K$? Can you find (diagrams of) K_1 and K_2?

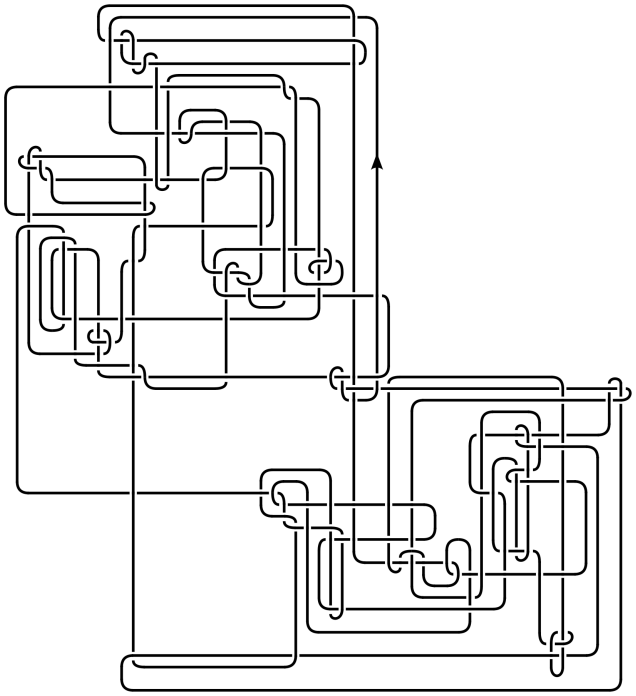


Figure 6: A randomly produced alternating prime knot with 151 crossings.

Problem 2.14. Let D be a knot diagram of a knot $K = K_1 \# K_2$ and assume you know (a diagram of) K_1. Find (a diagram of) K_2.

It was shown in [18] that Problem 2.11 is in *NP* (which stands for Nondeterministic Polynomial time). It is the set of decision problems verifiable in polynomial time by a deterministic Turing machine. So far the best unknotting algorithms are exponential ([9], [10], [25], [14]). In [14], it was shown that Problem 2.13 and Problem 2.14 are in *NP*. However, the presented algorithm is very ineffective for knots with many crossings. The hardness of Problem 2.14 is what we use to our advantage in the construction of the cryptosystem.

2.1.2 Encoding knots

The following part is dedicated to transferring the cryptosystem into the world of computers. Since we are using knots, we need to have some way of encoding these topological objects. We will introduce the so called *PD* (planar diagram) *notation*.

PD notation. Consider a knot diagram D. We can see it as a 4-regular graph with the additional information about which strand goes over which one at every vertex. The goal now is to encode this information efficiently. Choose a starting point on an arc of the knot and the direction along the knot, given by the orientation. Start by labelling this arc with 1. The next will get labelled with 2 and so on until every arc has a number associated to it. Now, we associate to each crossing a quatern with the labels of the four arcs attached to it: we start with the label of the unique incoming

undergoing arc and we conclude with the other three in counter-clockwise order. At the end, form a list with all these quaterns. This holds the information about the underlying 4-regular graph. An example is seen in Figure 7.

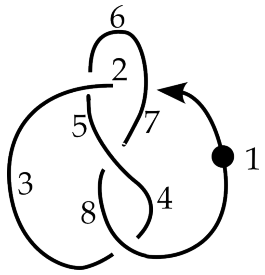


Figure 7: The PD notation of the Figure Eight knot pictured above is the following list: $[(1, 6, 2, 7), (5, 2, 6, 3), (3, 1, 4, 8), (7, 5, 8, 4)]$.

PD notation and connected sum. Notice that the PD notation in Figure 8 for the connected sum of twice the Figure Eight knot splits into two sublists where in the first one there are all the numbers between 1 and 9 and in the second one there are the the remaining ones from 9 over 16 to 1. This fact is true in general for the code of the connected sum, if the starting point for the code lies on one of the connecting arcs. If the starting point lies somewhere else, we can get it to lie on the connecting arc by shifting every number by a fixed shift modulo twice the number of crossings.

To perform the connected sum of two knots we can use the previous observation to split the first arc of the two knots and combine the list of tuples, shifting the numbers of the second list.

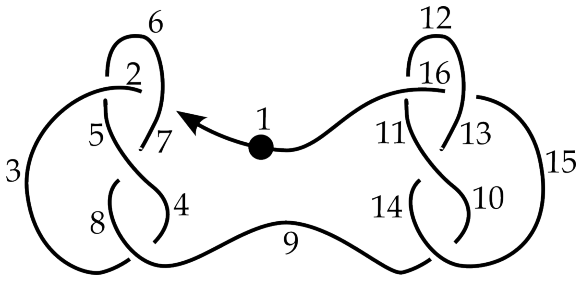


Figure 8: The PD notation for the connected sum of two Figure Eight knots is $[(1, 6, 2, 7), (5, 2, 6, 3), (3, 9, 4, 8), (7, 5, 8, 4), (9, 15, 10, 14), (13, 11, 14, 10), (11, 16, 12, 1), (15, 12, 16, 13)]$.

PD notation and Reidemeister moves. We analyze how Reidemeister moves performed on the diagram change the PD notation. A visualization is seen in Figure 9. There are several possibilities for each move, depending on the orientation of the arcs and the signs of the crossings. In the following we will show one case per move.

- Reidemeister 1+ (R1p): It adds a crossing with tuple $(i, i + 1, i + 1, i + 2)$.
- Reidemeister 1- (R1m): It deletes a crossing with tuple $(i, i + 1, i + 1, i + 2)$.

– Reidemeister 2+ (R2p): It adds two crossings between arcs belonging to the same region. The crossings are of the form $(i, j, i+1, j+1)$ and $(i+1, j+2, i+2, j+1)$.
– Reidemeister 2- (R2m): It deletes two crossings of the form $(i, j, i+1, j+1)$ and $(i+1, j+2, i+2, j+1)$.
– Reidemeister 3 (R3): This move changes three crossings $(j, i, j+1, i+1), (j+1, k+2, j+2, k+1), (i+1, k+1, i+2, k)$ to $(i, k+2, i+1, k+1), (j+1, i+1, j+2, i+2), (j, k+1, j+1, k)$ (see Figure 9).

This gives us the tools to apply random Reidemeister moves to a knot diagram using the PD notation, because we can see from the code where we can do which move. For this, we use a weight system that assigns weights to (R1p,R1m,R2p,R2m,R3) according to which we randomly decide which kind of move to perform.

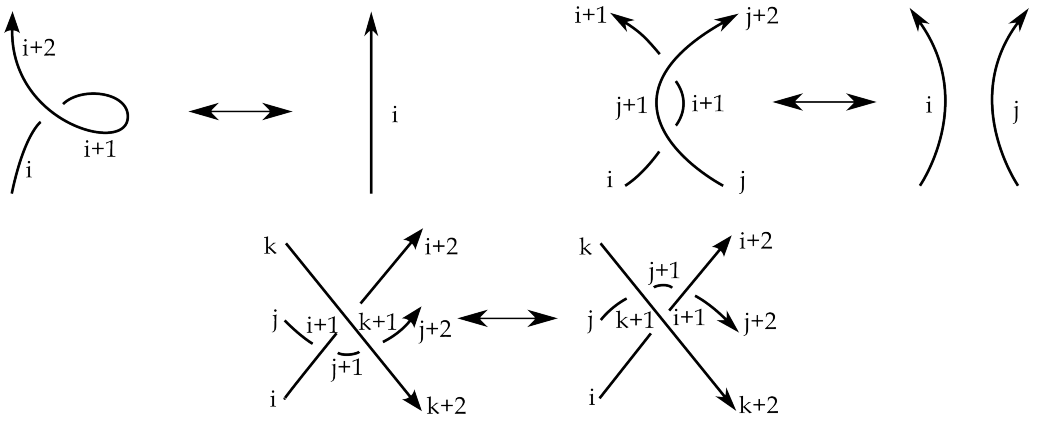


Figure 9: A visualization of how the PD notation transforms under the Reidemeister moves.

PD notation and coding. It is important to note that PD notation is supported by "SnapPy" and the Mathematica package "KnotTheory" from Bar Natan and Morrison [5].

Complexifying knots. We want to investigate means of bringing a knot into a general, i.e. unrecognisable, position. Usually, one is interested in the converse problem, so our ideas here (except Move I) are, at least to our knowledge, new. To complexify knots, one can do a combination of the following four moves.

– **Move I**: Apply random Reidemeister moves.
– **Move II**: Take a knot diagram and map it into $\mathbb{R}^3$ by taking a random piecewise linear height function, respecting the height order at the crossings. Turn the knot in $\mathbb{R}^3$ by a random element in SO(3) and project to a diagram. This is visualised in Figure 10.
– **Move III**: Take an arc in the diagram and move it around the whole knot such that it passes once underneath the knot. This is visualised in Figure 11.
– **Move IV**: Take an arc in the diagram and move it in an alternating fashion through regions of the diagram. This is visualised in Figure 12.

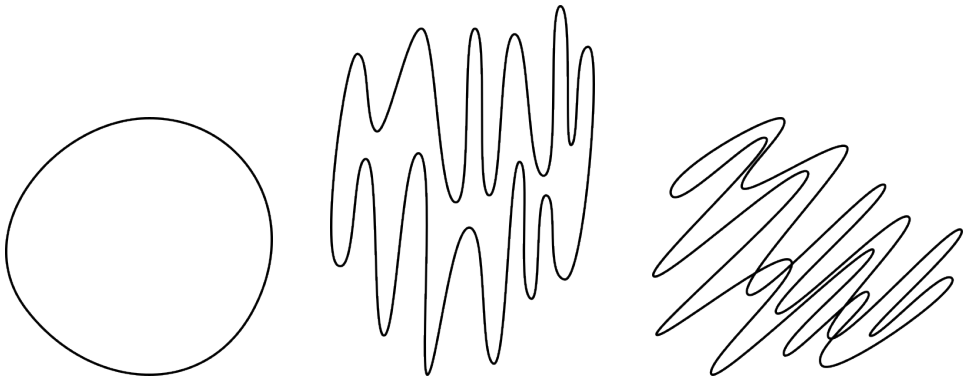


Figure 10: A sketch of the complexification move II. A diagram followed by its corresponding knot with a random height function. The turned knots is visualised at last.

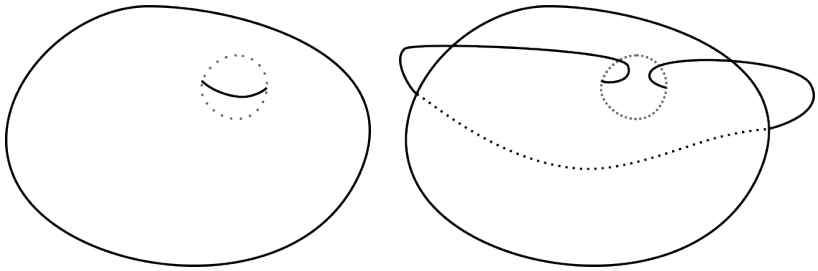


Figure 11: A visualisation of the complexification move III.

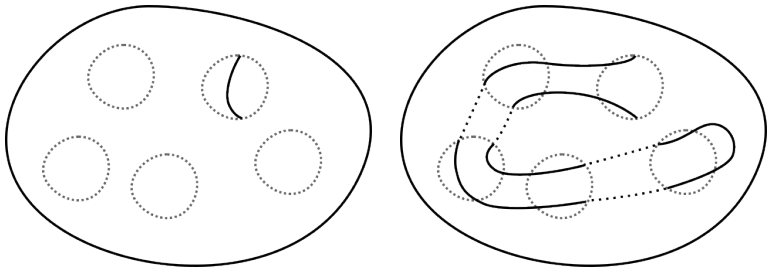


Figure 12: A visualisation of the complexification move IV.

2.1.3 Finite type invariants

To classify knots we use functions defined on diagrams that do not change under planar isotopies and Reidemeister moves. These functions are called knot invariants. Prominent examples include the knot signature, the Jones polynomial, the Alexander polynomial and the finite type invariants studied in this section. Note that these invariants usually do not distinguish all knots and it is common to trade calculability of the invariant for its power to detect knots.

We now consider finite type invariants. An introduction can be found in [3]. Let V (for Vassiliev invariant) be an invariant of knots with values in $\mathbb{Z}$, i.e. a function

$$V\colon \{\text{Knot Diagrams}\} \to \mathbb{Z}$$

that does not change under Reidemeister moves. Extend V to an invariant of oriented 1-singular knots, which are knots that have a singularity locally looking like  , using the (local) formula

$$V\left(\text{  }\right) = V\left(\text{}\right) - V\left(\text{  }\right). \tag{1}$$

Further extend V to the set of oriented m-singular knots by using (1) repeatedly.

Definition 2.15. We say that V is a *finite type invariant* (of degree m), if its extension to oriented $(m+1)$-singular knots vanishes.

Example 2.16 (Conway polynomial)**.** The (Alexander-)Conway polynomial Δ provides a source of finite type invariants. It is a polynomial (in the formal variable z) knot invariant, with value 1 on the unknot, satisfying the following local (skein) relation

$$\Delta\left(\text{  }\right) - \Delta\left(\text{  }\right) = z \cdot \Delta\left(\text{  }\right)$$

It is immediate from the definition that the coefficient of z^m in the Conway polynomial is a finite type invariant of degree m.

In some sense, finite type invariants forget a lot of data. They carry a "finite" amount of information in the sense of Theorem A.3. Nevertheless there is the following conjecture.

Conjecture 2.17. The set of all finite type invariants distinguishes knots.

The following property of finite type invariants is crucial for the purpose of our paper. We postpone the proof to Appendix A.

Corollary 2.18. *A finite type invariant of degree m can be computed in polynomial time $\mathcal{O}(c^m)$, depending on the number of crossings c.*

The proof will give an explicit way of constructing any finite type invariant. Parts of this are already encoded in Bar-Natan's, Amir-Khosravi's, and Sankarans Program "VasCalc". In Table 2, we see the list of the number of linearly independent finite type invariants.

Recently, it was shown in [4] that one can compute finite type invariants significantly faster, as stated in the Theorem below.

Theorem 2.19. *A finite type invariant of degree m can be computed in polynomial time $\mathcal{O}(c^{\frac{m}{2}})$, depending on the number of crossings c.*

Note that finite type invariants are supported in the "KnotTheory" package of Mathematica [5].

m	0	1	2	3	4	5	6	7	8	9	10	11	12
#Degree m finite type invariants	1	1	2	3	6	10	19	33	60	104	184	316	548

Table 2: The list of the number of linearly independent finite type invariants of a given degree m.

2.2 Crash course on cryptography

The aim of this section is to introduce the notions of cryptography, particularly relating to key exchanges, which we will use in the main part of the article.

The purpose of cryptography is to find ways (protocols) to communicate securely, assuming the presence of eavesdroppers. In particular, we want to transform our messages (*encryption phase*) in such a way that opponents will find it to be unintelligible text and only the predestined receiver will be able to trace the original message (*decryption phase*).

In order to carry out encryption and decryption, we need so-called *cryptographic keys*. This brings us to the *Key Exchange Problem*: how can two parties exchange keys in such a way as to establish a secure communication channel? This process is called the *key exchange protocol* and, in the next section, we will propose one based on knots.

There are two main types of cryptography: *symmetric-key* cryptography (or *single-key* cryptography) and *asymmetrical* cryptography (or *public-key* cryptography). In the first one, the two parties (Alice and Bob) use the same secret key to encrypt and decrypt the message. The main problem in this case is that they need to communicate this key to each other via a secure channel. The commonly used symmetric cryptosystem is the Advanced Encryption Standard (AES) [12, 19].

In public-key crytography, there are two keys involved: a public one known to everybody and a private one known only to the owner; depending on the algorithm, one will be used to encrypt and the other to decrypt. One of the earliest and most famous examples of Public-Key Exchange (PKE) is the *Diffie-Hellman Key Exchange* [13], proposed by Diffie and Hellman in 1976 and described below in Protocol 2.20. It allows the two parties to establish a shared secret key over an insecure channel, i.e. even in the presence of eavesdroppers who can monitor the channel.

Protocol 2.20 (Diffie-Hellman Key Exchange)**.**

1. Alice and Bob publicly agree on a cyclic finite group G and a generator g.
2. Alice chooses $a \in \{1, \dots, \mathrm{ord}(G)\}$, computes g^a and sends it to Bob. Her secret key is a.
3. Bob chooses $b \in \{1, \dots, \mathrm{ord}(G)\}$, computes g^b and sends it to Alice. His secret key is b.
4. Alice computes $(g^b)^a = g^{ba}$.
5. Bob computes $(g^a)^b = g^{ab}$.

The secret common key is $g^{ba} = g^{ab}$.

The security of the system is based on the following hard problem:

Problem 2.21 (Diffie-Hellman Problem (DHP))**.** Let G be a finite cyclic group and let g be a generator. Given g^a and g^b, find g^{ab}.

We will say that a mathematical problem is *easy* if there exists a polynomial-time algorithm which can solve it. If there are no deterministic or probabilistic polynomial-time algorithms that can solve it, we will call it *hard*.

Actually, if someone is able to solve the Discrete Logarithm Problem (DLP): *given G an abelian group and $a, b \in G$ such that $b = a^m$ for some $m \in \mathbb{Z}$, find $0 \leq n < \mathrm{ord}(G)$ such that $a^n = b$*, they can also solve the DHP.

Remark 2.22. In a cryptosystem, we need the computations required for implementation to be feasible, and those needed to break it to be not. In the Diffie-Hellman Key Exchange 2.20, we have that g^a can be computed in $\mathcal{O}(\log a)$ group multiplications, while the best algorithm to solve the DLP requires $\mathcal{O}(\sqrt{\text{ord}(G)})$.

Notice that we define the Diffie-Hellman protocol using the group action of $\mathbb{Z}^\times_{\text{ord}(G)}$ over G given by

$$\begin{aligned} \mathbb{Z}^\times_{\text{ord}(G)} \times G &\to G \\ (n, g) &\mapsto g^n. \end{aligned}$$

Therefore it is possible to naturally extend the Diffie-Hellman protocol from a generic group action and even from a semigroup action, as shown in [32].

Definition 2.23. Let G be a semigroup and let S be a set. The semigroup G *acts on* S if there exists a map

$$\begin{aligned} G \times S &\to S \\ (g, s) &\mapsto g \cdot s, \end{aligned}$$

satisfying $(gh) \cdot s = g \cdot (h \cdot s)$ for all $g, h \in G$ and all $s \in S$.

If the semigroup is abelian, the map is called a *G-action* on the set S.

We can then define the *Generalised Diffie-Hellman Key Exchange*.

Protocol 2.24 (Generalised Diffie-Hellman Key Exchange)**.**

1. Alice and Bob publicly agree on a G-action on a finite set S and an element $s \in S$.
2. Alice chooses $a \in G$, computes $a \cdot s$ and sends it to Bob. Her secret key is a.
3. Bob chooses $b \in G$, computes $b \cdot s$ and sends it to Alice. His secret key is b.
4. Alice computes $a \cdot (b \cdot s)$.
5. Bob computes $b \cdot (a \cdot s)$.

The secret common key is $a \cdot (b \cdot s) = (ab) \cdot s = (ba) \cdot s = b \cdot (a \cdot s)$.

In order to obtain a secure cryptosystem, we need to choose an action that makes the following mathematical problem hard.

Problem 2.25 (Diffie-Hellman Semigroup Action Problem (DHSAP))**.** Let G be an abelian semigroup, S a finite set and $\cdot$ a G-action on S. Given $x, y, z \in S$ such that $y = g \cdot x$ and $z = h \cdot x$ for some $g, h \in G$, find $(gh) \cdot x$.

Notice that, on the other hand, in order to be able to calculate the key, we need the action to be computationally feasible, i.e. we need to be able to easily calculate every $g \cdot s$ and also every multiplication in G.

There is a generalised version of the DLP which use a generic semigroup action, the so-called Semigroup Action Problem.

Problem 2.26. (Semigroup Action Problem (SAP)) Let G be an abelian semigroup, S a finite set and $\cdot$ a G-action on S. Given $x, y \in S$ such that $y = g \cdot x$ for some $g \in G$, find $h \in G$ such that $y = h \cdot x$.

As with the DLP and the DHP, if one is able to solve the SAP, then he can automatically solve the DHSAP; indeed, let $\tilde{g} \in G$ such that $g \cdot x = \tilde{g} \cdot x$, therefore we could solve the DHSAP computing

$$\tilde{g} \cdot (h \cdot x) = (\tilde{g}h) \cdot x = (h\tilde{g}) \cdot x = h \cdot (\tilde{g} \cdot x) = h \cdot (g \cdot x) = (hg) \cdot x = (gh) \cdot x.$$

It is still an open question if the DHSAP and the SAP are equivalent, therefore all the attacks considered attempt to solve the Semigroup Action Problem.

Remark 2.27. If we are considering a semigroup G, we can always take $S = G$ and consider as a semigroup action just the semigroup operation. This is actually what we will do in the next section with $S = G =$ **Knots**.

3 Cryptosystem

The proposed cryptosystem is built by using the semigroup of oriented knots in the (Generalised Diffie-Hellman Key Exchange) Protocol 2.24 with the choices as in Remark 2.27. The security of the protocol is ensured by the fact that the general Problem 2.26 in our case translates to Problem 2.14, which is believed to be hard.

Protocol 3.1 (Knot-based Diffie-Hellman)**.** All knots in this protocol are presented in PD notation, as described in Subsection 2.1.2.

1. Alice and Bob publicly agree on a (randomly generated) alternating prime knot K, a positive integer n and a finite type invariant V taking values in $\mathbb{Z}$.

2. Alice chooses a (randomly generated) alternating prime knot A with at most n crossings, computes $A\#K$, complexifies the obtained knot by applying a combination of the four complexification moves described in Subsection 2.1.2 and sends it to Bob. Her secret key is A.

3. Bob chooses a (randomly generated) alternating prime knot B with at most n crossings, computes $B\#K$, complexifies the obtained knot by applying a combination of the four complexification moves described in Subsection 2.1.2 and sends it to Alice. His secret key is B.

4. Alice computes $V(A\#(B\#K))$.

5. Bob computes $V(B\#(A\#K))$.

The secret common key is $V(A\#B\#K) = V(B\#A\#K) \in \mathbb{Z}$.

There are two things about this protocol that are worth dwelling on. At first, there is the fact that we complexify the knot $A\#K$ (respectively $B\#K$). The reason is that otherwise, it is very easy to see where the connected sum was made and we can decompose the knot by looking at its PD notation. The other thing that makes our protocol not quite a standard Diffie-Hellman protocol is that, in the end, we compute a knot invariant. The reason is that even though we know that

Alice and Bob share the same knot $A\#B\#K = B\#A\#K$, they have very different presentations of that knot. Thus, the presentations themself are useless for doing encryption, so we compute a knot invariant to get an integer, which is the same for both Alice and Bob.

Notice that the bottleneck of the protocol is the computation of the finite type invariant, which requires $\mathcal{O}(c^{\frac{m}{2}})$ operations, where c is the number of crossings of the final knots $A\#B\#K$ and $B\#A\#K$ (recall that in their description these two knots can have a different number of crossings) and m is the degree of the chosen finite type invariant V.

Key size. Assume that in the complexification phase of the knot, both Alice and Bob apply complexification moves until they obtain an equivalent knot with at most $2n$ crossings.

In order to describe a knot with n crossings, we need all the positive integers from 1 to $2n$, just to enumerate all the edges. Following the encoding procedure, we have to write each integer between 1 and $2n$ twice in the string of integers, since each edge is related to two crossings. Recall that we need at most (up to a constant)

$$\sum_{i=1}^{\lfloor \log_2(n) \rfloor} i2^{(i-1)} - 1 = 2^{\lfloor \log_2(n) \rfloor} \lfloor \log_2(n) \rfloor - 2^{\lfloor \log_2(n) \rfloor} \simeq n(\log_2(n) - 1) \text{ bits}$$

to describe all the integers from 1 to n.

Summing up, given a knot with n crossings, we need roughly $2n(\log_2(2n) - 1)$ bits to describe all the integers from 1 to $2n$ that represent the edges and, since we need to use each of them twice, we need roughly $4n(\log_2(2n) - 1)$ bits to describe Alice's private key and Bob's private key respectively.

About the private common key, recall that it is an integer number that we obtain computing a finite type invariant of a knot with at most $3n$ crossings, since K as at most n crossings and both Alice and Bob complexify their secret knots to obtain an equivalent knot with at most $2n$ crossings. Therefore, thanks to Corollary A.4, we need at most $\lfloor 3n \log_2(M) \rfloor$ bits to describe the common secret key.

Remark 3.2. Since the bottleneck of the protocol is the computation of the finite type invariant, we would like to choose an invariant of degree as small as possible. But we need it to be of degree large enough to ensure that a brute force attack is not possible. In fact, one can decide to compute not just one finite type invariant, but several different ones, all of small degree, since the complexity is essentially the same.

4 Cryptanalysis

In the following, we analyse the security and the efficiency of the proposed protocol. We explain how other invariants than the ones of finite type fail and give a suitable choice of parameters.

4.1 Security analysis

We discuss several possible attacks on the proposed protocol and either explain why they fail or give our opinion on how likely they would work to break the protocol.

Notice that the underlying mathematical problem is the following one.

Problem 4.1. Given V a finite type invariant and the knots K, $A\#K$ and $B\#K$, find $V(A\#B\#K)$.

Notice that if, for example, we would have chosen the Jones polynomial [20] as our knot invariant the protocol would break. This is because the Jones polynomial J is multiplicative with respect to the connected sum, so one can compute $J(A) = \frac{J(A\#K)}{J(K)}$ or $J(B) = \frac{J(B\#K)}{J(K)}$, which leads to $J(A\#B\#K) = J(A)J(B\#K)$ or $J(A\#B\#K) = J(B)J(A\#K)$. Thus, we want to avoid knot invariants which have a connected sum formula. We don't know of any such general formula for finite type invariants. But it may be (and we actually know it for some of them as discussed in Section 4.3) that the specific finite type invariant we choose has such a formula. The strength of the proposed protocol however then lies in the fact that we are free to choose another finite type invariant for which we know no connected sum formula.

The study of an attack for a given finite type invariant is far from exhaustive. It is possible that some of them allow ad hoc attacks and should therefore be excluded.

There is a related mathematical problem, which is the SAP 2.26 on **Knots**.

Problem 4.2. Given two knots K and K', construct a knot A (if it exists) such that $K' = A\#K$.

Notice that, solving the previous problem allows an attacker to solve the underlying problem 4.1. Indeed, given K and $A\#K$ as in the protocol, if he finds A, since he also knows $B\#K$, he can compute $A\#B\#K$; at this point, he only has to calculate the finite type invariant of $A\#B\#K$ in order to get the secret shared key.

In the following, we discuss several possible attacks on the SAP on **Knots**. We divide them into two families: those related to the generic SAP and those that explicitly use Knot Theory.

4.1.1 Generic attacks for the semigroup action problem

Here we analyse the generic attacks on the SAP described in [30] and [29].

Feasibility of the SAP. In general, when we try to solve the SAP, we are looking for an $h \in G$ such that $g \cdot x = h \cdot x$, not necessarily for the specific g. For this reason, we are interested in the following set

$$G_{x,g} = \{h \in G \mid h \cdot x = g \cdot x\}.$$

The parameters G, S and x need to be chosen in such a way that $|G_{x,g}|$ is small with respect to $|G|$. In our case we have $G = S =$ **Knots**, $x = K \in S$ and the action is just the connected sum. Thanks to Proposition 2.7, we know that, given K and $K'\#K$, the knot K' is unique, therefore $G_{K,K'} = \{K'\}$ and $|G_{K,K'}| = 1$ for all $K, K' \in$ **Knots**.

Structure of the semigroup. Various attacks on DH realised through a group action are known and it is therefore legitimate to ask whether some of them can also be applied or generalised to semigroup actions. First, notice that we can partition the semigroup G, following the notation in [29], as $G = G_0 \cup G_1$, where

$$G_1 = \{g \in G \mid g^{-1} \text{ exists}\} \quad \text{and} \quad G_0 = G \setminus G_1.$$

Practically, if G has a large subgroup, it can be a problem. Indeed, we can try to solve the SAP in G_0 by brute force, with an exhaustive search. If we found no solutions, then we can restrict the SAP to G_1, which is a group. Now all the attacks that we know for groups are applicable. In our case, this strategy does not apply, because $G_1 = \{\mathcal{U}\}$, thanks to Proposition 2.6.

4.1.2 Knot theoretic attacks

Attacking the basic structure and the complexification phase. In our proposed protocol there are three steps which need our attention. Taking the connected sum, complexifying the diagram, and the evaluation via a knot invariant. We have already discussed above, at the begginning of the section, the choice of the finite type invariant. The connected sum poses no problems for security. Provided that the knot is in a general position, it is commonly accepted that decomposition as in Problem 2.14 is very hard. However, if you just take the connected sum and leave the knot as it is, it is easy to decompose it by looking at its PD notation. So the question becomes, whether the algorithm using a combination of the four complexification moves achieves a position for the knot which is random enough that one cannot decompose the knot easily. This is still an open question. What has been invastigated is that using only random Reidemeister moves is not enough as in all examples, the knot was easily recognizable.

Brute force attack. Of course, the first attack that one can always try is the brute force attack, which means that the attacker has to compute $A'\#K$, for all $A' \in \mathbf{Knots}$ with at most n crossings, until he finds the correct one, which is $A\#K$. But recall that he doesn't have a way to compare directly $A'\#K$ with $A\#K$, since the second one is complexified in the protocol and Problem 2.12 is hard. The best thing that he could do is computing a fixed invariant of $A'\#K$ and $A\#K$ and check if it is the same. In general, in order to avoid brute force attacks, it is sufficient to set the parameters of the cryptosystem appropriately. We will give an example of a possible choice of parameters in Subsection 4.4. But recall that we don't have a computable complete invariant, so it could happen that more than one knot A' satisfy that $A'\#K$ and $A\#K$ have the same fixed invariant. In that case, the attacker could change the invariant and compute it only for previously acceptable candidates or for each of them (if they are few) he can compute the finite type invariant of $A'\#B\#K$ and check which one works as the cryptographic key.

Actually, since the cryptographic key is an integer given by the finite type invariant of the final knot, an attacker can also apply a brute force attack to this value. The unique upper bound that we have in general is given in Corollary A.4. However, we do not expect a finite type invariant to have a uniform distribution, therefore it is possible that some integers are more likely than others. Some experiments showed that some of them, at least of small degree, look more distributed close to 0. A solution to this problem is to apply an Hash-function to the secret shared key.

Problem with small knots. One thing to keep in mind is that knots with up to around 15 crossings can be taken apart with knot invariants. This forces us to use bigger knots. Otherwise one could compare the invariants of the public knots to a table of knots with their invariants and try the corresponding knot. The number of (alternating prime) knots however increases very fast as seen in Proposition 2.10, which means that this procedure is not possible for bigger knots.

Attack using invariants with a connected sum formula. If the knots chosen by Alice and Bob in the protocol are sums of smaller knots, there is the following attack. In Subsection 4.3.2 we will see that a lot of knot invariants have a connected sum formula. Take for example the Alexander polynomial Δ. It satisfies $\frac{\Delta(A\#K)}{\Delta(K)} = \Delta(A)$. Hence, one can get the invariant of the secret knot. If this knot is composed of small knots, one can factor $\Delta(A)$ and only consider prime knots with Alexander polynomial equal to one of the factors (including the constant polynomial 1). This will

lead to a combinatorial problem that is more approachable, given that one can compute the Alexander polynomial on all prime knots with a given crossing number. This attack also generalizes to other knot invariants with a connected sum formula. This attack is the reason why we work with prime knots in the protocol.

Attack for braid group cryptography. Knots and braids (see Figure 13) are intimately related by the Alexander and Markov Theorem proven in [8]. The basic idea is that closing up a braid yields a knot (or a link). But the group structure on braids is not related to the semigroup structure on knots. There are cryptographic protocols involving braid groups (see [23, 16]) which are now broken. They were successfully attacked by using the faithful Lawrence representation of the braid group, where one could transfer the underlying problem into the world of matrices (compare [26], [7], and [24]). Contrary to braid groups, we know no reasonable representation of the semigroup of knots, so attacks of this form are not available.

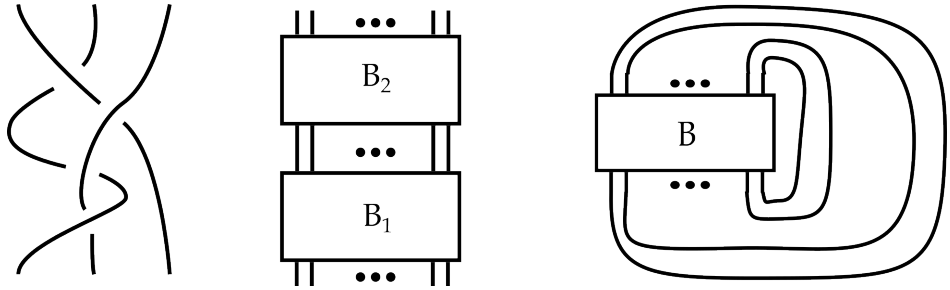


Figure 13: An example of a braid with three strands, the group structure of the braid group given by stacking and the closure of a braid.

Knots seen as graphs. In general, a linear representation of the problem could be a weakness; indeed, if we can represent the action as a matrix action on a vector space, then the SAP may be solved easily. One can think of a knot as a graph (keeping track of over- or undercrossing) and to a graph we can associate the adjacency matrix. However, we can't represent the connected sum as a matrix action. Moreover, if we consider a complicated knot and the adjacency matrix associated to it, we can't obtain enough information to understand which knot it is.

We are therefore unable to represent the action as a linear one, or at least we are unable to do so by exploiting the one related to braid groups nor the point of view of graphs. This obviously does not represent an exhaustive study of all possible ways in which one can try to represent the connected sum as a linear action.

4.2 Efficiency analysis

We show here that our proposed protocol can be ran in polynomial time, depending on the crossing number. We have three knots involved K, A, and B with the number of crossings c_K, c_A, and c_B. Taking the connected sum is an easy operation. We trust that complicating the diagram is not very costly as well, since all the moves are easy 3D-moves and the application of Reidemeister moves in terms of the PD notation is efficient. This leaves the computation of the finite type invariant

which uses $\sim (c_K + 2c_A + 2c_B)^{\frac{m}{2}}$ steps for a finite type invariant of degree m, thanks to Theorem 2.19.

4.3 Other invariants

In principal, one can choose any knot invariant for the protocol to work. Maybe, there is a knot invariant that we do not know and that fits the protocol better then the finite type ones. However there are some features of certain knot invariants that make the protocol very slow or even attackable. We discuss them here.

4.3.1 Computability

First, there is the problem of computability. Low-dimensional topology is notorious for having complicated (and powerful) constructions which are hard to calculate. This rules out basically all knot homologies like the Khovanov homology [22] and the knot Floer homology [35], as well as any invariant coming from them, like the Rassmussen invariant [38], the Υ [36] and the τ invariant [34]. Even the Jones polynomial is too costly to calculate, since its computation time grows exponentially in the number of crossings [21]. The genus, braid index and similar invariants have no algorithms to calculate them at all [39].

4.3.2 Connected sum formula

As already explained before, the protocol is attackable when the used invariant has a reasonably nice connected sum formula. Then the attacker does not have to decompose the knot itself, but rather has to find the invariant of the individual knots. We show here which invariants this excludes. The HOMFLY, Jones, and Alexander knot polynomials [27] are all multiplicative with respect to the connected sum and are therefore immediately excluded. Even the "Polynomial time knot polynomial" of Bar Natan [6] has a nice enough connected sum formula that it can be attacked. The signature is additive [39] and the number of 3-colorings is multiplicative [39].

We show here how even some finite type invariants fail. Let us consider f_m the m-th coefficient of the Conway polynomial C considered in Example 2.16, i.e. $C(K) = \sum_{m\in\mathbb{N}} f_m z^m$. The polynomial itself is multiplicative, i.e. $C(K\#A) = C(K)C(A)$. While the finite type invariant f_m is not multiplicative, it has the following formula

$$f_m(K\#A) = \sum_{i=0}^{m} f_i(K) f_{m-i}(A).$$

Thus, knowing $f_i(K)$ and $f_i(K\#A)$ for $0 \leq i \leq m$ (which are computable in not much more time than $f_m(K\#A)$) allows an attacker to solve for $f_i(A)$ (and similarly $f_i(B)$), which is enough to compute $f_m(K\#A\#B)$.

With exactly the same reasoning, one can also exclude the finite type invariants given by the m-th coefficient of $J(e^x)$ (where J is the Jones polynomial) seen as a formal power series in x. This tells us that we have to choose our finite type invariant carefully enough to avoid these specific ones. But there are plenty of other finite type invariants.

4.4 Choice of Parameters

Here we will give a possible choice of parameters in order to reach a 128-bit security level, which means that the attacker would have to perform at least 2^{128} operations to break the protocol. The unique parameter that we have to choose is the number of crossings n. As far as we know, the best attack is the brute force attack described above in this chapter, since the knots chosen by Alice and Bob are prime.

So we need to look at the number of alternating prime knots with at most n crossings. For this we look at Table 1 and Proposition 2.10. From Table 1, we know APK(21), the number of alternating prime knots with crossing number 21. Assuming exponential growth after that as in Proposition 2.10, we have that $n = 67$ is a suitable parameter in order to reach 128-bit security level, since

$$2^{128} < \mathrm{APK}(21) \cdot 4.45^{46}.$$

5 Conclusion and further development

In the paper, we propose a new Key-Exchange Protocol based on the Generalised Diffie-Hellman Key Exchange Protocol. We use the semigroup action given by

$$\begin{aligned} \#\colon \mathbf{Knots} \times \mathbf{Knots} &\to \mathbf{Knots} \\ (K_1, K_2) &\mapsto K_1 \# K_2, \end{aligned}$$

where $\#$ represents the connected sum of two knots.

Since in our protocol Alice and Bob get the same connected sum of three knots, but represented in two different ways, in the last step we need to compute an invariant of this knot in order to obtain the same shared secret key. We studied the different possibilities and concluded that the best choice are finite type invariants, since they give us a bounded positive integer, they can be computed in polynomial type and they do not admit a connected sum formula.

Furthermore, after the cryptanalysis, the best attack is the brute force attack and, based on this, we propose a possible choice of parameters for a 128-bit security level.

Open problems. The following problems are still open and are interesting for a future work:

- A much deeper study of finite type invariants is needed. We should study each of them for degree $m \geq 3$, to understand which is the most suitable one. It could be that some of them admit a connected sum formula, which means that we have to exclude them. We must also exclude those that only admit too few integer values. This research also is needed to understand which degree m is most suitable. This choice is fundamental, since the computational complexity of a finite type invariant of degree m is exactly $\mathcal{O}(c^{\frac{m}{2}})$, where c is the number of crossings of the knot. This computation is the bottleneck of the protocol.
- As already mentioned, the weak point in our protocol is the use of the knot invariant. Even though finite type invariants seem to work in principal, probably they make the protocol too slow. So the main goal would be to replace them with a better invariant, i.e. an invariant with the same good properties as the finite type ones (no connected sum formula), but that could

be computed in less time. Otherwise, another solution can be to find a more efficient way to compute at least finite type invariant of small degree.

– Another unanswered question is: how many times do we have to apply the four moves to get an equivalent knot that looks as random as possible?

– The choice of creating random alternating prime knots requires further investigation: does it weaken the protocol, if one works with alternating knots?

– Finally, no attempt has yet been made to implement our protocol.

A Finite type invariants are computable in polynomial time

The aim of this appendix is to show how one can compute finite type invariants in polynomial time. Additionally, we will see a way to construct any finite type invariant.

A.1 Gauss diagrams

We first consider Gauss diagrams. They are closely related to PD notation in the sense that the former are a visualization of the latter.

Start with a knot diagram with n crossings. Label its crossings starting at a basepoint on the knot, following the orientation, with the numbers 1 to $2n$ such that every crossing has two numbers assigned to it. To construct the Gauss diagram, we draw a circle with $2n$ dots with labels from 1 to $2n$ and connect the points belonging to the same crossing with a line and decorate it using the sign of the crossing. In addition, we give an orientation to the line to indicate which strand passed over the other one. See an example in Figure 14.

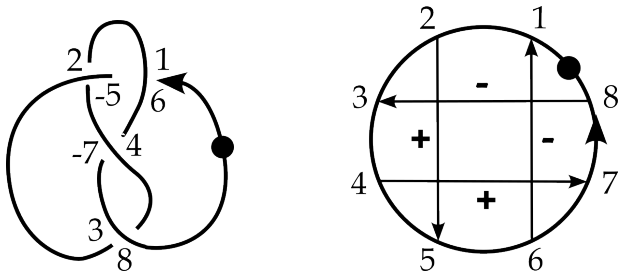


Figure 14: The Gauss diagram for the Figure Eight knot.

We can consider arbitrary Gauss diagrams which do not need to come from knots. In fact, there are examples of Gauss diagrams that cannot be realised as knot in $\mathbb{R}^3$ without introducing singularities.

Definition A.1. The *space of Gauss diagrams* $\mathcal{D}$ is the $\mathbb{Q}$ vector space spanned by all Gauss diagrams.

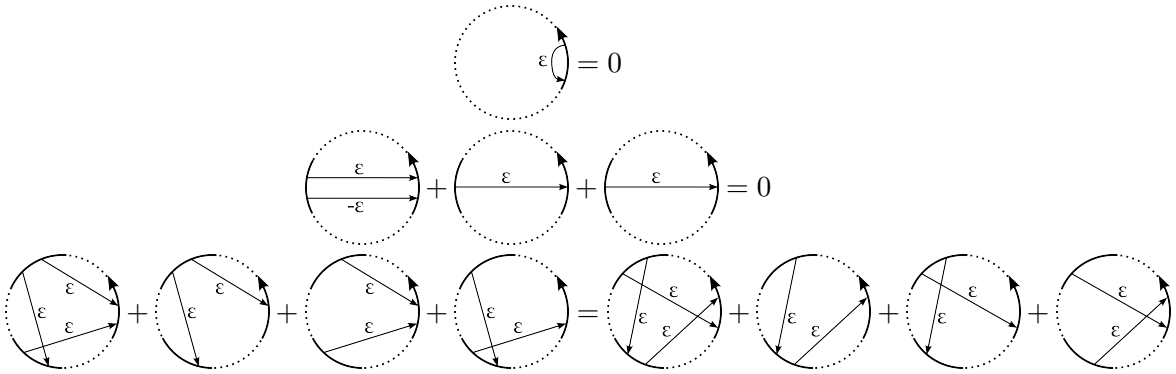
A *Gauss subdiagram* D' of D is a diagram in which some arcs of D have been deleted and we say $D' \subset D$. We can define the following endomorphism:

$$\begin{aligned}\phi\colon \mathcal{D} &\to \mathcal{D}\\ D &\mapsto \sum_{D_i \subset D} D_i\ .\end{aligned}$$

A.2 The Polyak space and the proof

Clearly, ϕ doesn't yield a knot invariant. Just introducing more crossings in a diagram changes its image under ϕ. To make ϕ an invariant, we need to introduce relations in the space of Gauss diagrams $\mathcal{D}$.

Definition A.2. The *Polyak space* $\mathcal{P}$ is defined to be $\mathcal{A}$ with the following relations:



The space $\mathcal{P}_m$ is obtained by setting all diagrams with more than m arcs to zero. It yields a finite dimensional vector space. The restriction of ϕ to $\mathcal{P}_m$ is denoted by ϕ_m. It is a universal finite type invariant in the sense of the next theorem.

Theorem A.3 ([17]). *V is a finite type invariant of degree m (with values in $\mathbb{Q}$) if and only if $V = f \circ \phi_m$, where $f\colon \mathcal{P}_m \to \mathbb{Q}$ is a linear functional.*

From this we can prove Corollary 2.18.

Proof of Corollary 2.18. To compute the map ϕ_m one needs to compute all $\sum_{i=1}^{m} \binom{c}{i}$ Gauss subdiagrams, which requires the stated polynomial amount of operations of Gauss diagrams:

$$\sum_{i=1}^{m} \binom{c}{i} \sim \sum_{i=1}^{m} c^i \sim c^m.$$

The evaluation of these subdiagrams via f doesn't add computational cost. □

Note that the previous proof allows us to construct any finite type invariant and thus, can be seen as a blueprint to construct finite type invariants. One can calculate a basis of the finite dimensional vector space $\mathcal{P}_m$ and then choose any linear functional on this basis. Note that the finite type invariant in principle takes values in $\mathbb{Q}$. It is more convenient to have an invariant that takes values

in $\mathbb{Z}$, which is easily obtained by scaling the invariant by the least common multiple of the divisors of the values on the basis of Gauss subdiagrams, such that they evaluate to integers. The following corollary is immediate.

Corollary A.4. *Let the knot K have a diagram with c crossings and let V be a finite type invariant of degree m. Define $M \coloneqq \max_{D \text{ Gauss diagram}} V(D)$. We have the following bound:*

$$|V(K)| \leq M \cdot 2^c.$$

References

[1] Ilya Alekseev, Anatolii Moiseevich Vershik, and Andrei Valer'evich Malyutin. On the growth of the number of prime knots. *Algebra i Analiz*, 36(1):17–39, 2024.

[2] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6(3):287–291, 1999.

[3] Dror Bar-Natan. On the Vassiliev knot invariants. *Topology*, 34(2):423–472, 1995.

[4] Dror Bar-Natan, Itai Bar-Natan, Iva Halacheva, and Nancy Scherich. Computing finite type invariants efficiently. *arXiv preprint arXiv:2408.15942*, 2024.

[5] Dror Bar-Natan, Scott Morrison, and et al. The Knot Atlas. http://katlas.org.

[6] Dror Bar-Natan and Roland van der Veen. A polynomial time knot polynomial. *Proceedings of the American Mathematical Society*, 147(1):377–397, 2019.

[7] Stephen Bigelow. Braid groups are linear. *Journal of the American Mathematical Society*, 14(2):471–486, 2001.

[8] Joan S. Birman and Tara E. Brendle. Braids: a survey. *Handbook of knot theory*, pages 19–103, 2005.

[9] Benjamin A Burton. Maximal admissible faces and asymptotic bounds for the normal surface solution space. *Journal of Combinatorial Theory, Series A*, 118(4):1410–1435, 2011.

[10] Benjamin A Burton. The Pachner graph and the simplification of 3-sphere triangulations. In *Proceedings of the twenty-seventh annual symposium on Computational geometry*, pages 153–162, 2011.

[11] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: an efficient post-quantum commutative group action. In *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*, pages 395–427. Springer, 2018.

[12] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael. 1999.

[13] Whitfield Diffie and Martin Hellman. New directions in cryptography (1976). *IEEE Trans. Inform. Theory*, 22:644–654, 1976.

[14] Ivan Dynnikov. Arc-presentations of links: monotonic simplification. *Fundamenta Mathematicae*, 1(190):29–76, 2006.

[15] Michael H Freedman and Frank Quinn. Topology of 4-manifolds (pms-39), volume 39. 49, 2014.

[16] David Garber. Braid group cryptography. *Braids: Introductory lectures on braids, configurations and their applications*, pages 329–403, 2010.

[17] Mikhail Goussarov, Michael Polyak, and Oleg Viro. Finite-type invariants of classical and virtual knots. *Topology*, 39(5):1045–1068, 2000.

[18] Joel Hass, Jeffrey C Lagarias, and Nicholas Pippenger. The computational complexity of knot and link problems. *Journal of the ACM (JACM)*, 46(2):185–211, 1999.

[19] Daemen Joan and Rijmen Vincent. The design of rijndael: AES-the advanced encryption standard. *Information Security and Cryptography*, 2002.

[20] Vaughan FR Jones. A polynomial invariant for knots via von Neumann algebras. 1985.

[21] Louis H Kauffman. State models and the Jones polynomial. *Topology*, 26(3):395–407, 1987.

[22] Mikhail Khovanov. A categorification of the Jones polynomial. 2000.

[23] Ki Hyoung Ko, Sang Jin Lee, Jung Hee Cheon, Jae Woo Han, Ju-sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In *Advances in Cryptology—CRYPTO 2000: 20th Annual International Cryptology Conference Santa Barbara, California, USA, August 20–24, 2000 Proceedings 20*, pages 166–183. Springer, 2000.

[24] Daan Krammer. Braid groups are linear. *Annals of Mathematics*, pages 131–156, 2002.

[25] Marc Lackenby. A polynomial upper bound on Reidemeister moves. *Annals of Mathematics*, pages 491–564, 2015.

[26] Ruth J Lawrence. Homological representations of the Hecke algebra. *Communications in mathematical physics*, 135:141–191, 1990.

[27] William BR Lickorish and Kenneth C Millett. The new polynomial invariants of knots and links. *Mathematics Magazine*, 61(1):3–23, 1988.

[28] Annalisa Marzuoli and Giandomenico Palumbo. Post quantum cryptography from mutant prime knots. *International Journal of Geometric Methods in Modern Physics*, 8(07):1571–1581, 2011.

[29] Gérard Maze. *Algebraic Methods for constructing One-Way Trapdoor Functions*. University of Notre Dame, 2003.

[30] Gérard Maze, Chris Monico, and Joachim Rosenthal. Public key cryptography based on semigroup actions. *Adv. in Math. of Communications 1.4*, pages 489–507, 2007.

[31] William Menasco. Closed incompressible surfaces in alternating knot and link complements. *Topology*, 23(1):37–44, 1984.

[32] Christopher Monico. *Semirings and semigroup actions in public-key cryptography.* University of Notre Dame, 2002.

[33] Kunio Murasugi. Jones polynomials and classical conjectures in knot theory. *Topology*, 26(2):187–194, 1987.

[34] Peter Ozsváth and Zoltán Szabó. Knot Floer homology and the four-ball genus. *Geometry & Topology*, 7(2):615–639, 2003.

[35] Peter Ozsváth and Zoltán Szabó. An overview of knot Floer homology. *arXiv preprint arXiv:1706.07729*, 2017.

[36] Peter S Ozsváth, András I Stipsicz, and Zoltán Szabó. Concordance homomorphisms from knot Floer homology. *Advances in Mathematics*, 315:366–426, 2017.

[37] John M Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of computation*, 32(143):918–924, 1978.

[38] Jacob Rasmussen. Khovanov homology and the slice genus. *Inventiones mathematicae*, 182(2):419–447, 2010.

[39] Justin Roberts. Knots knotes. *Lectures from Edinburgh Course Maths*, 415, 1999.

[40] Daniel Shanks. Class number, a theory of factorization, and genera. In *Proc. Symp. Math. Soc., 1971*, volume 20, pages 415–440, 1971.

[41] Edward Witten. Quantum field theory and the Jones polynomial. *Communications in Mathematical Physics*, 121(3):351–399, 1989.

[42] Marc Zucker. *Studies in cryptological combinatorics.* City University of New York, 2005.