Abstract

Cryptography nowadays plays a fundamental role within society, as it forms the basis of all the security related to the informatic world. This obviously includes private chats, banking, wireless communications, wi-fi connections, login operations or any other computer authentication process, and much more. All these processes hide within them the use of a particular *cryptographic protocol* (or *cryptosystem*) and, as a result, all their security lies in the security of the cryptographic protocols themselves. Each cryptosystem is in turn usable effectively as it is based on mathematical problems considered unassailable because they are too computationally difficult to solve in a reasonable time.

Classical cryptography, in its dual guise (*private key cryptography* and *public key cryptography*), is based on three unresolved mathematical problems that guarantee its usability:

- *Integer Factorization Problem*
- *Discrete Logarithm Problem*
- *Elliptic Curves Discrete Logarithm Problem*

It is therefore immediate to observe that, if the underlying mathematical problem could be solved in a short time, the cryptosystem would lose all its security and therefore could no longer be used in any context. In fact, the cryptosystems still used in practice today are only those that, over time, have managed to prove resistant to all the attacks presented.

When Feynman observed in 1982 that, in accordance with Moore's law, technology would gradually move closer and closer to atomic dimensions, a fundamental problem ached: since physical laws have quantum nature, in order to represent them appropriately through a computer, it is necessary that the latter be based on quantum principles too.

It was from these considerations that the concept of quantum computers, as it is known today, was initiated, even if only theoretically. It should be pointed out that a quantum computer is not a simple evolution of a classical computer, but is governed by completely different physical laws and its elementary components are *quantum bits*, or *qubits*, which are able to represent simultaneously and with some probability more classical bits at the same time.

This remarkable property that distinguishes them involves the possibility of making calculations, through quantum computers, with a marked speed: if one considers a *quantum register*, that is a system of numerous qubits that interact with each other, it is able to simultaneously represent 2^n classical configurations.

The high computational speed of a quantum computer is crucial for the future of cryptography as it can help to speed up the resolution of those mathematical problems that were discussed earlier. It is therefore clear that when a quantum computer is materially created, cryptography as it is known today will be undermined in the foundation of its security. The concern that comes directly is that the birth of a quantum computer marks the definitive death of the cryptographic age.

This question became relevant as early as 1994 when computer scientist Peter Williston Shor [16] created what is now known as *Shor factorization algorithm* which, as the name suggests, is able to factor an integer. In more detail, given an entire N the algorithm returns a factorization of N in prime integers by calculating the period of a function. This calculation requires the use of a quantum computer because it originates from an overlap of all possible values of the function itself in a single qubit and then ends with the evaluation of the *Fourier quantum transform*. Although not deterministic, the algorithm, which has an order execution complexity of $(\log N)^2 \cdot \log(\log N) \cdot \log(\log(\log N))$, can be repeated iteratively to most likely achieve the desired result.

Shor's work was of considerable concern to cryptographers, as some of the most important cryptographic protocols still used today, such as RSA, DSA, and more generally most public key cryptosystems, base their effectiveness and security precisely on the integer factorization problem. Shor's algorithm thus allows the complete rupture of such protocols.

An additional quantum algorithm capable of threatening modern cryptography, though much less powerful than Shor's, was introduced in 1996 by Lov Kumar Grover [8]. Known as the *Grover search algorithm*, while not completely breaking cryptographic protocols such as Shor's algorithm, it halves the computational time of almost all private key cryptosystems still used. The security of this cryptosystem lies, as know, in the relationship between the encryption function and the decryption function which, although one is the inverse of the other, has a very different calculation time: while the evaluation of the former can be seen as a *structured problem*, evaluating the second is equivalent to solving an *un-structured problem*. Grover, taking advantage of the remarkable speed of a quantum computer and the peculiar superposition characteristic of a qubit, created an algorithm based on the *Hadamard transform* and able to greatly decrease the resolution time for an un-structed problem.

What has been said so far would lead anyone to claim that, on the day when a quantum computer is physically available, it will have to be said definitively goodbye to cryptography. Fortunately, many researchers have become increasingly interested in the subject in recent decades in order to research cryptosystems resistant to any type of attack, even quantum ones: they have thus given rise to *post-quantum cryptography*.

Post-quantum cryptography is divided into several branches, depending on the mathematical approach adopted as a starting point for the in-depth study of the cryptographic processes that derive from it. The areas of development are:

- *Lattice-based cryptography*;
- *Multivariate cryptography*;
- *Hash-based cryptography*;
- *Code-based cryptography*;
- *Isogeny-based cryptography*.

The thesis will deal with the latter type of post-quantum cryptography. It is divided into three sections, corresponding respectively to Chapters 2, 3 and 4.

The second chapter is focused on the necessary bases to deal with the proposed study, zoom in particular on elliptic curves, being the environment in which one will subsequently work and also remembering notions related to quaternion algebras and useful orders for subsequent results.

An *elliptic curve* E is a projective curve, described by a cubic equation and defined on an arbitrary field. Curves of this type are of interest to many of their properties, the first of which is that the set of all elliptic curves on a field can be treated as a group, following the definition of an addition law within it. It is thanks to the use of this law that it is possible to define a very important map, called *multiplication by-m map*, with peculiar properties that make it widely used within many protocols defined starting from elliptic curves. In fact, it is linked to the notion of *m-torsion group* of curve E which, in finite fields, determines the crucial distinction between *ordinary curves* and *supersingular curve*s. These two classes of curves remain distinct even under the action of maps between elliptic curves, in particular by *isogenies*, i.e. group surjective morphisms.

Isogenies are extensively studied, analyzing their *degree* in order to distinguish them between *separable, inseparable* and *purely inseparable isogenies* and focusing on significant properties inherent in *dual isogenies*.

A particular role is played by the isogenies from the curve to itself that make up the *endomorphism ring* of E, which proves to be isomorphic at $\mathbb{Z}$, to an order in an imaginary quadratic field or to an order in a quaternion algebra.

After examining elliptic curves extensively in the more general case, instead one will move on to dealing with elliptic curves defined on a finite field $E/\mathbb{F}_q$ for which, as already mentioned, the distinction between ordinary curves and supersingular curves is crucial, which can be carried out not only through the study of the m-torsion group but also through considerations on the endormorphism ring. In the case of curves on finite fields, the ring is isomorphic to an order in a quaternion algebra (supersingular case) or to an order in a quadratic imaginary extension of $\mathbb{Q}$ (ordinary case).

The most important arithmetic quantity associated with elliptic curves on finite fields is the number of rational points $\#E(\mathbb{F}_q)$: there is a close relationship, provided by a result known as the *Sato-Tate Theorem*, between that number and the isogenies from the curve.

The most important result related to $\#E(\mathbb{F}_q)$ is the theorem enunciated in 1936 by Helmut Hasse [9] which provides a fairly accurate bound for the number of points of an elliptic curve defined on a finite field, dependent on the trace of *Frobeniuos endomorphism* characteristic of the curve itself π_E.

Although this bound is the best starting point for the study of the number of rational points, Hasse's theorem gives no indication of how this number can be calculated. A significant step forward in this direction was provided in 1949 by Andrè Weil [22] who formulated a conjecture, known precisely as the *Weil conjecture*, concerning the number of points in a variety (in particular an elliptic curve) defined on a finite field.

However, it was not until 1995, thanks to the mathematician Renè Schoof [15], that the first algorithm really capable of calculating the Frobenious trace and consequently, taking advantage of Hasse's theorem, also the number of points on the curve. This algorithm is based on two other auxiliaries algorithms that make extensive use of what are called *division polynomials*, thanks to which it is possible to rewrite multiplication by-m map in another form.

The working environment for all steps to be taken is a quotient ring related to one particular division polinomial. For this reason this algorithm can be covered within a wider set of algorithms, known as SEA (Schoof-Elkies-Atkin Algorithms) that differ slightly from one another only for the working environment: in particular, the polynomials that provide the quotient ring for the Elkies [5] and Atkin [1] algorithms have lower degrees and this ensures a higher rate of calculation.

To conclude the study of elliptic curves defined on finite fields, it is appropriate to focus on a further crucial result that allows, given a curve E and its subgroup Φ, to explicitly describe not only a new curve $E' = E/\Phi$ but also the isogeny between E and E'.

This 1978 result is due to Jacques Vélu [21], and represents a very important step for the study of the supersingular elliptic curves isogeny cryptography as it allows, as it will be seen, to move within particular graphs (isogeny graph) used for the creation of post-quantum cryptographic protocols.

The chapter on elliptic curves ends with the study of elliptic curves defined in the field of complex numbers $E/\mathbb{C}$. After defining a *complex lattice* Λ, the respective quotient $\mathbb{C}/\Lambda$, called *torus*, and the set of classes representing $\mathbb{C}/\Lambda$, said the *fundamental parallelogram*, one focuses on demonstrating a two-way correspondence between elliptic curves and tori.

In order to achieve this objective, it is worth analyzing first in more detail some aspects of lattice. So they are defined the *weight-k Eisenstein series* for Λ and an equivalence relationship between two of them Λ_1, Λ_2 (*omotetia*); one than moves on to *elliptic functions* and their properties, focusing in particular on the most important of them, capable of generating all the others: the *Weierstrass $\wp$-function*.

The Weierstrass $\wp$- function and its derivative satisfy a differential equation which, by simple substitutions, is easily seen to be the equation of an elliptic curve. In particular it is possible to define an isomorphism between this elliptic curve and the torus corresponding to the lattice in which $\wp$ is defined.

This leads to the central result in finite field elliptic curves: the *(Uniformization Theorem* induces the two-way correspondence that was initially talked about. Such a correspondence plays an essential role since, being the study of lattices much simpler than that of elliptic curves, choosing an appropriate lattice, an elliptic curve can be constructed with a fixed ring of endomorphisms.

Within the third chapter, the main object of study is a particular type of graphs, called *isogeny graphs*, the classification of which is due to Mestre [13], Pizer and Kohel.

Before going into the careful analysis of this type of graph, it is obviously advisable to pay attention to the basic notions in the most general sense.

A *graph* G is a set of points called *nodes* or *vertices* that can be connected to each other by lines called *arcs* or *sides* or *edges*. Depending on how the edges connect vertices to each other, a distinction is made between *directed graphs* and *undirected graphs*. Moreover, after defining the *neighbors set* of a vertex, that is the set of all the vertices adjacent to it, one can speak of *degree* and consequently classify *k-regular graphs*. These types of graphs turn out to be really very important in the cryptographic field as you will see later.

One of the basic notions of graph theory is that of walking: A $(v_0; v_k)$-*walk in* G is a sequence of vertices and edges from G that starts on v_0 and ends on v_k and

such that the end vertex of one edge is the start vertex of the next one. Starting from this simple and intuitive definition, it can then be made specifications, such as the concept of *trail* or *path*, from which derive quantities that characterize the graph itself, such as *distance*, *diameter* and *connection*.

One of the most effective methods of representing a graph without resorting to a graphical-geometric scheme is through its *adjacency matrix*: A is such that entry $A_{i;j}$ denotes the number of edges joining vertex v_i and v_j. The *eigenvalues* (and their respective *eigenvectors*) of G, which make up the *spectrum*, are defined to be those of A. Thanks to the analysis of the adjacency matrix and its eigenvalues, the characteristic properties of graph G can be understood.

An *isogeny graph* is a particular type of graph in which vertices consist of elliptic curves defined on a field and edges represent l-isogenies between curves, i.e. isogenies of degree l. This graphs are undirected graphs whose adjacency matrix is symmetric.

The notable distinction between ordinary elliptic curves and supersingolar elliptic curves is also reflected in the graphs that these two classes form: there are significant differences (both in the structure of the isogeny graph and the way it is used in applications) between the ordinary and supersingular cases.

For the study of ordinary case isogeny graphs, a further subdivision into horizontal and vertical isogenes (ascending or descending) is applicable; analyzing these three possibilities one immediately observes that ordinary case graphs possess a rigid structure, known as *volcano*. Algorithms allowing to travel on these graphs were developed by Kohel in his thesis [10]. Within his thesis, Kohel demonstrated that elliptic curves placed at the same "level" in the volcano have similar structures, in particular, satisfy a very important property: they possess the same endomorphism ring.

The possible applications of volcanoes are really numerous and some of them remarkable: by identifying the level at which the curve is located one can calculate the endomorphism ring and, also, through the search for paths between a summit of the volcano and the floor supersingolar curves can be identified.

The part of isogeny graphs for supersingular case is related to *expander graphs*, which are a type of sparse but pseudorandom graphs of importance in the theory of random walks, geometric group theory, and in number theory. The expansion can be defined by two different modes known as *Spectral expansion*, obtained by the eigenvalues of the graph's adjacency matrix, and *Edge expansion*, obtained by considering apposite subsets of vertices related to their *edge boundaries*, i.e. the set of all arcs from the set itself to its complement. These two different expansions are related to each other through *Cheeger's inequality*.

Finally, it is analyzed the most important concept related to isogney graphs, which constitutes the real way in which they are used within post-quantum cryptographic processes, namely random walk.

A *random walk* is obtained starting from a graph vertex and then proceeding following a path in which the edges (and therefore the vertices reached from time to time) are determined by some probability distributions. It is easy to see that a random walk defined on an isogeny graph is a Markov Chain and therefore converges to a stationary distribution. The number of steps required for the random walk to be close to stationary distribution characterizes *mixing time*, which is a fundamental parameter especially for expander graphs for which this time is extremely fast.

The last chapter of the thesis finally focuses on the in-depth study of cryptographic protocols based on isogenies of elliptic curves and on isogeny graphs for which to date no attacks are known that can threaten their total or partial security (for example drastically decreasing the resolution time) even through the use of an efficient quantum computer.

Why can elliptic curve isogenies be used as a basis for ensuring the security of hash functions? The answer to this question lies in the existence of some mathematical problems, known as *isogeny problems*, which are still unresolved or for which a solution method is known but which does not appear to be entirely computationally optimal:

1. Given an elliptic curve E with Frobenius endomorphism π, and a subgroup $G \subset E$ such that $\pi(G) = G$, compute the image curve of the separable isogeny ϕ of kernel G.

   This problem can be solved using Vélu's formula, although this algorithm is not optimal.

2. Given two elliptic curves E, E' over a finite field, isogenous of known degree d, find an isogeny $\phi : E \to E'$ of degree d.

   The first to present this problem, and a related resolution algorithm, with complexity $O(d^3)$ was Elkies [5], followed by Couveignes [2] who managed to slightly lower the execution time by presenting a complexity algorithm of $O(d^2)$.

3. Given two elliptic curves E, E' over a finite field K, such that $\#E = \#E'$, find an isogeny $\phi : E ß E'$ of smooth degree.

   This third and final problem is the most difficult to solve and therefore the one that occurs most in isogeny-based cryptography. The only known attacks, such as the *meet in the middle*, have exponential complexity in $\log \#E$.

The first post-quantum protocol studied in this chapter was introduced by mathematicians Luca De Feo, David Jao and Jérôme Plût [11] and consists of a zero-knowledge identification scheme.

A *zero-knowledge protocol* is an interactive method used by one subject to prove to another subject that a statement is true, without revealing anything other than its veracity. In this case, given two isogenous curves E and $E' = E/\langle S \rangle$, Alice proves that she knows a generator for $\langle S \rangle$. To do this, she uses a process based on Vélu's formula.

One of the biggest players in cryptography, since 1976 when Diffie and Hellman first proposed it, is the *key exchange*.

In its original version, two users, Alice and Bob, publicly choose a $g \in \mathbb{F}_p^*$ and privately integers, respectively, a and b and then they share the values g^b and g^a respectively. In this way both are able to calculate a secret key g^{ab}. The security of this procedure, i.e. the actual secrecy of the key, lies in the difficulty of calculating g^{ab} knowing only g, g^a and g^b and therefore depends on the impossibility of solving the discrete logarithm problem.

A similar version of the key exchange procedure has been defined on elliptic curves, the safety of which is provided by the curves discrete logarithm problem.

There are two versions of post-quantum key exchange presented in the thesis, both based on isogeny graphs and resistant to quantum attacks.

The first key exchange, presented by Rostovtsev and Stolbunov [14] in 2006, uses random walks in *Schreier graph*, which are graphs of ordinary curves with horizontal isogenies: Alice and Bob start at the same vertex g and arrive at the same vertex $g_{A,B}$ but following different paths.

As one would expect, this key exchange scheme based on ordinary graphs is contrasted with a respective key exchange based on supersingular graphs.

Presented by Luca De Feo, David Jao and Jérôme Plût in [11], the *Supersingular Isogeny Diffie-Hellman protocol (SIDH)* is more complicated than the one described in the previous case, although the basic idea is slightly similar: given a set of vertices (consisting of supersingular elliptic curves defined on a finite field $\mathbb{F}_{p^2}$ with p very large) Alice works on an l_A- isogeny graph while Bob works on a l_B- isogeny graph.

Hash functions are particular functions that play a central role within cryptography, used in principle only to secure certification procedures such as digital signature and message authentication, appear today in a wide range of cryptographic protocols and even represent the basis on which an entire line of research for post-quantum cryptography is based.

They are so important because they have three particular properties that characterize them, such as *collision resistance*, *first preimage resistance* and *second preimage resistance*: it must be computationally really difficult to reverse a hash function or find two inputs with the same output.

The hitherto known and secure algorithms inherent in hash functions are unfortunately subject to attack by Grover's algorithm that halves its computational security. For this reason, in the goal of searching for protocols that can withstand quantum attacks, it is also necessary to focus on the definition of new hash functions.

The idea of using graphs to define hash functions originated in 1991, when researcher Gilles Zemor proposed to build a hash function from a *Cayley graph*. Unfortunately, this first structure was quickly broken by an attack.

The method by which, starting from a graph, it is possible to define a function is very simple and intuitive. For example, if one is supposed to be working with cubic graphs, that is a 3-regular graphs, the input is a binary string. At each step one bit is read from the string, and its value is used to choose an edge from the current vertex to the next one, avoiding the one edge that goes back. The arrival point is the output of the function.

More than fifteen years after Zemor's proposal, researchers Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren [4] took up this idea using hash functions from supersingular isogenic graphs: they proposed the use of LPS and Pizer graphs.

Pizer graphs are Ramanujan $\mathrm{l} + 1$-regular graph: the set of vertices consists of the supersingular curves defined on $\mathbb{F}_{p^2}$. The resistance to collision and preimage of the resulting hash function is guaranteed by the difficulty of solving isogenic problems for supersingular curves. The best algorithm known to date has a complexity of $O(p \log p)$.

LPS graphs are not bipartite Ramanujan graphs but also Cayley graphs. Although the definition of hash functions through the use of these graphs is much simpler and faster, they are then easily subject to both collision attacks and preimage attacks.

The chapter, and the thesis itself, ends with the post-quantum study of a last procedure of fundamental importance in cryptography for authentication procedures: the *digital signature scheme*. It is used, as the name suggests, to affix a (digital) signature to a message in order to simultaneously testify to its *authenticity*, ensuring that the sender is real, and *integrity*, ensuring that the message has not been altered.

The first digital signature scheme based on isogenies, which is strongly unforgeable under chosen message attack in the quantum random oracle model, was proposed by Youngho Yoo, Reza Azarderakhsh, Amir Jalali ,David Jao and Vladimir Soukharev and it is based on the zero-knowledge protocol already described.

Bibliography

[1] Arthur O. L. Atkin. The number of points on an elliptic curve modulo a prime, 1991. URL http://www.lix.polytechnique.fr/Labo/Francois.Morain/AtkinEmails/19910614.txt.

[2] J.-M. Couveignes. *Quelques calculs en théorie des nombres*. Thèse, Université de Bordeaux I, July 1994.

[3] Jean-Marc Couveignes. Hard homogeneous spaces, aug 2006.

[4] Eyal Z. Goren Denis X. Charles and Kristin E. Lauter. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, 2009.

[5] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In AMS International Press, editor, *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7, page Studies in Advanced Mathematics, 1998.

[6] De Feo. Isogeny graphs in cryptography, mar 2018. URL http://defeo.lu/docet/.

[7] Luca De Feo. Mathematics of isogeny based cryptography. Thiès, Senegal, may 2017. École mathématique africaine.

[8] Lov K. Grover. A fast quantum mechanical algorithm for database search.

[9] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper iii. die struktur des meromorphismenrings. die riemannsche vermutung. *Journal für die reine und angewandte Mathematik*, 175:193–208, 1936. URL http://eudml.org/doc/149968.

[10] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California at Berkley, 1996.

[11] David Jao Luca De Feo and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[12] Jérôme Plût Luca De Feo, Cyril Hugounenq and Éric Schost. Explicit isogenies in quadratic time in any characteristic. *LMS Journal of Computation and Mathematics*, 19(A):267–282, 2016.

[13] Jean-François Mestre. La méthode des graphes. exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields*, Nagoya, 1986. Nagoya University.

[14] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145.

[15] René Schoof. Counting points on elliptic curves over finite fields. *Journal de théorie des nombres de Bordeaux*, 7(1):219–254, 1995. URL http://www.numdam.org/item/JTNB_1995__7_1_219_0.

[16] PeterW. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In IEEE Computer Society Press, editor, *Proceedings, 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Santa Fe, NM, nov 1994.

[17] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer-Verlag, 1994.

[18] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, 1992.

[19] Andrew V. Sutherland. Elliptic curves over c, 2015.

[20] Serge Vaudenay. *A classical introduction to cryptography- Applications for Communications Security*. Springer, 2006.

[21] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Serie I*, 273:238–241, juillet 1971.

[22] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, (55):497–508, 1949.