

RESEARCH AND TRAINING DEVELOPMENT PROJECT

Name : Dr. Fouazou Lontouo Perez Broon Ph.D

Estimation of Duration : 5-7 years

Email : perezfomazou@gmail.com

Title : Mathematical Cryptology, Abelian Varieties, Classical and Quantum
Computational Number Theory and Geometry

Overview of the Project : This research project is divided into three parts :

1. The first part, devoted to 12 research questions for publications on : Diophantine geometry of elliptic curve, galois representation attached to elliptic curves, symbolic computation of isogenies, counting isomorphism classes and isogeny classes of (hyper)elliptic curves (I evaluate the duration of this part at 1-2 years and if possible I can submit this part for a external funding).
2. The second part address identified training needs in mathematics, computer science and application of isogenies in cryptology. they aims to define research questions for international publications, broaden my research interest, learn and develop research skills. Also for design of courses and learning materials at graduate and post-graduate levels, with contemporary mathematics courses on recent developments of some selected research topics. These training needs are :
 - (a) A selection of eight mathematical areas with their applications in cryptology and some of current research topics on them in the literature.
 - (b) Some identified training needs (more precisely in deeply og knowledge) in programming and foundation of cryptology.
 - (b) some training and research topics in quantum algorithm and quantum algorithms for number theory.
 - (c) A selection of some current research topics on applications of isogenies in cryptology.
3. The third part is constituted of the syllabus of some already available courses.

Table des matières

1	Research and Training Development Project	1
1.1	Some open questions	2
1.2	Selected Thematics for Training Activities With Some Related Research Topics . . .	7
1.2.1	Selected Mathematics Areas	7
1.2.2	Programming and Foundation of Cryptology	10
1.2.3	Quantum Algorithm	10
1.2.4	Some Current Research Questions in Isogeny Based Cryptography	12
1.3	Syllabus of Some Courses to Generate Learning Materials at Graduate and Postgraduate Level	14
1.3.1	Fields Theory	14
1.3.2	Algebraic Number theory	16
1.3.3	Algebraic Curves	19
1.3.4	Modular Forms and Galois Representations of Elliptic Curves	22

1.1 Some open questions

1. 1. Title : Extension and Construction of Vélu's Formula, Author : Fouazou Lontouo Perez Broon

Abstract : While the original Vélu's formula on Weierstrass model of elliptic curves is expressed as a sum $I(P) = (x_P + \sum_{Q \in G^*} x_{P+Q} - x_Q, y_P + \sum_{Q \in G^*} y_{P+Q} - y_Q)$ (see [1]), the isogeny formulas on some alternate models of elliptic curves such that the Hessian, Edward and Huff models are expressed as a product $I(P) = (x \prod_{Q \in G^*} x_{P+Q}, y \prod_{Q \in G^*} y_{P+Q})$ for twisted Hessian curve, $I(P) = (\prod_{Q \in G} x_{P+Q}/x_Q, \prod_{Q \in G} y_{P+Q}/y_Q)$ and $I(P) = (\prod_{Q \in G} -x_{P+Q}/y_Q, \prod_{Q \in G} -y_{P+Q}/y_Q)$ for Edward and Huff models see [2] and [3], also the formulas given on alternate models are not unified. Precisely previous formulas on Hessian model can not be applied to subgroups of order divisible by 3 and formula for Edward and Huff model can not be applied to subgroups of order divisible by two, while the original Vélu's formula on Weierstrass model can be applied to subgroups of any order. Also on Hessian curve (resp Edward and Huff curve), coefficients of the 3-isogenies (resp

2-isogenies) and parameters of the co-domain curve are not rational since their expressions involve a cubic root (resp square root) see [4] theorem 2 (resp [2] theorem 1 and 7).

In this work, I provide multiplicative formulas to compute isogenies on Weierstrass model of elliptic curves and additive one on some alternate models. More generally, I give an algorithm which takes an alternate model of elliptic curves and first returns condition on a subgroup so that the co-domain curve is K -isomorphic to a curve in the given model. Then, if the condition is satisfied, it returns an analogous of Vélu's formulas on this model to compute the isogeny and the co-domain curve. I apply this algorithm on some models of elliptic curves to construct unified Vélu's formula on these models and to construct condition on the groups so that the co-domain curve can be K -isomorphic to a curve of the given model. Also I provide condition on a subgroup $G = \{\mathcal{O}, Q_1, \dots, Q_{n-1}\}$ so that the function $S_{i,n}(x_P, x_{P+Q_0}, \dots, x_{P+Q_{n-1}})$ is constant (where $S_{i,n}$ is the i^{th} elementary symmetric polynomial of $K[x_1, x_2, \dots, x_n]$), in fact if this function is not constant it is the first coordinate of an isogeny of kernel G (see [5]).

A comparison between the multiplicative isogeny formulas we construct on Weierstrass model of elliptic curves and the original additive Vélu's formula show that the coefficients of the kernel polynomials associated to finite subgroups satisfy some algebraic relations. Prove that these relations characterize the kernel polynomials and studying these algebraic relations as multivariate polynomials system is the objective of the work 2 below.

2. **Title : On Kernel Polynomials Associate to finite subgroups of an elliptic curve, Author : Fouazou Lontouo Perez Broon,**

Abstract : A comparison of our multiplicative formula (work 1) to compute the isogenies and the original additive Vélu's formula show that the coefficients of kernel polynomials of finite subgroups are solutions of a multivariate polynomials system. More precisely, equating our first coordinate (resp second coordinate) and the first coordinate (resp second coordinate) of Vélu's formula leads to a multivariate polynomials system. The first objective here is to prove that only the coefficients of the kernel polynomials are solutions to each of these systems (ie these systems characterize the kernel polynomials). We will then study these systems as Zero-dimensional ideals and use these characterizations to solve questions on elliptic curves and in algebraic number theory.

I already shown that the system obtained by equating the second coordinates characterizes kernel polynomials. Among works in the literature providing algebraic relations between the coefficients of the kernel polynomials we can cite [6] and

3. **Title : Counting Isomorphism Classes of Elliptic Curves Having Prescribed 3 or 4-Torsion Points Fields Over Finite Fields , Author : Fouazou Lontouo Perez Broon.**

Abstract : In this work I search the possible 3-torsion point fields (resp 4-torsion point fields) of elliptic curves over finite fields and their associated Galois representations. Then, for

each associated Galois representation I compute the number of isomorphism class of elliptic curve having this Galois representation (ie the number of J-invariant given by curves having this representation). These complete some works existing in the literature on computation isomorphism class of elliptic curves having a point of order 3 or a rational group of order 3, also work computing isomorphism class of some models of elliptic curves having a point of order 2 or containing their 2-torsion in the following papers [7, 8].

4. **Title : Counting Isomorphism Classes of Elliptic Curves Having Prescribed 5-Torsion Points Fields Over Finite Fields , Author : Fouazou Lontouo Perez Broon.**

Abstract : In this work I search the possible 5-torsion point fields of elliptic curves over finite fields and their associated Galois representations. Then, for each associated Galois representation I compute the number of isomorphism class of elliptic curve having this Galois representation (ie the number of J-invariant given by curve having this representation). These is the first step to address this counting problem more generally for ℓ -torsion point fields, where $\ell \in \mathbb{N}$ is a prime.

5. **Title : Counting Isogeny Classes of Elliptic Curves Having Prescribed 3 or 4-Torsion Points Fields Over Finite Fields , Author : Fouazou Lontouo Perez Broon.**

Abstract : The goal of this work is to compute the number of isogeny class of elliptic curves having a rational point of order 4 (resp a rational subgroup of order 4) over finite fields (ie the number of trace given by these curves). I will also address this question for elliptic curves containing their 4-torsion (ie where all the 4-torsion points are rational) and more generally for family of elliptic curve shaving same Galois representation (ie for Galois representation computed in the work...). In the literature there exist results for curve having a point of order 3 (resp a rational subgroup of order 3) in [8] and [9] give results on the numbers of isogeny classes of Edwards curves . Lets $t \in \mathbb{Z}$, $(\mathcal{M}_c)_{c \in K}$ a family of elliptic curves and $N(t)$ the number of curve of the family $(\mathcal{M}_c)_{c \in K}$ having trace t or the number of the K-isomorphism classes of the curves $(\mathcal{M}_c)_{c \in K}$ having trace t in the family. Where I will also address question to find relations between the $N(t)$ for some family of elliptic curves having same Galois 4-mod representation. In the literature results on this question for Legendre form of elliptic curves in [10, 11], for Edwards model of elliptic curves in [9] and for Hessian model of elliptic curve in [8]. In [8] Dustin Moody formulate some conjecture on this number for Hessian Model of elliptic curves, I will also address this conjecture here.

6. **Title : Counting Isogeny Classes of Elliptic Curves Having Prescribed 5-Torsion Points Fields Over Finite Fields and their trace ratio problems, Author : Fouazou Lontouo Perez Broon.**

Abstract : The goal of this work is to compute the number of isogeny class of elliptic curves having a rational point of order 5 (resp a rational subgroup of order 5) over finite fields (ie the number of trace given by these curves). I will also address this question for elliptic curves containing their 5-torsion (ie where all the 5-torsion points are rational) and more generally

for family of elliptic curve having same Galois representation (ie for Galois representation computed in the work...). As in the work 5 above I will also address the corresponding trace ratio problem in the case here.

7. **Title : Counting isogeny classes of Elliptic Curves Over Finite Field with Prescribed Galois ℓ -mod Representation , Author : Fouazou Lontouo Perez Broon.**

Abstract : The goal of this project is to compute the number of isogeny classes of elliptic curves over finite field having a prescribed Galois ℓ -mod representation (Where ℓ is a prime), these in order to generalize the results of the works 3,4,5 and 6 above to prime greater than 5. Some works exist in the literature on the Galois ℓ -mod representation of elliptic curves over finite fields [12–14].

From Zeta function associate to elliptic curves it is well known that knowing the field of definition of an elliptic curve and its trace t , we can compute its trace t_n over \mathbb{F}_{q^n} . Also for a prime ℓ we can use this to compute the smallest extension $\mathbb{F}_{q^{k_0}}$ such that $\#E(\mathbb{F}_{q^{k_0}}) \equiv 0[\ell]$. The following table gives the values of k_0 for different values of q and t modulo 5.

$q \backslash t$	0	1	2	3	4
1	4	6	1	2	3
2	8	24	2	1	24
3	8	2	24	24	1
4	1	4	12	12	4

In this work I generate such data for many primes ℓ and make some conjectures. The goal is to prove these conjectures and use them to give a way to search the formulas giving the number of isogeny classes of elliptic curves having a prescribed ℓ -torsion point field. This is in order to generalize the work of [8] which gives the formulas for the number of isogeny classes for some families of curves. Some of this conjecture are :

Conjecture 1 (already proved) : Let $E/\mathbb{F}_q : y^2 = x^3 + ax + b$ such that $\ell \nmid E(\mathbb{F}_q)$, $\ell \mid E(\mathbb{F}_{q^n})$ and $n \mid \ell - 1$. Then the points $P \in E(\mathbb{F}_{q^n})$ of order ℓ generate a \mathbb{F}_q -rational subgroup.

Conjecture 2 : If $q \pmod{\ell}$ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*$. Then up to the values of the traces modulo ℓ there are $\frac{\ell-1}{2}$ traces modulo ℓ having a \mathbb{F}_q -rational subgroups of order ℓ .

Example : If $q \equiv 13[19]$. Then 0, 1,2,5,7,12,14,17 and 18 are the values of the traces modulo 19 of the elliptic curves having a rational subgroup of order 19.

Conjecture 3 : If $q \pmod{\ell}$ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*$. Then up to the values of the traces modulo ℓ there are $\varphi(\ell + 1)$ traces modulo ℓ having ℓ -torsion point field $\mathbb{F}_{q^{(\ell+1)(\ell-1)}}$ (Where φ is the Euler's totient function).

Conjecture 4 : If $q \pmod{\ell}$ is a generator of $(\mathbb{Z}/\ell\mathbb{Z})^*$, $k \mid \ell + 1$ and $k \nmid \ell - 1$. Then up to the values of the traces modulo ℓ there are $\varphi(\frac{\ell+1}{k})$ traces modulo ℓ having ℓ -torsion point field $\mathbb{F}_{q^{(\ell-1)(\frac{\ell+1}{k})}}$ (Where φ is the Euler's totient function).

8. **Title : Counting Elliptic Curve Over Field of Rational numbers Having Prescribed Galois ℓ -mod Representation , Author : Fouazou Lontouo Perez Broon.**

Abstract : This work is an analog of the work 3,4,5,6 and 7 above for elliptic curves over rational field \mathbb{Q} rather than finite fields for works 3,4,5,6 and 7. Namely the question is to provide results on the number of elliptic curves over \mathbb{Q} having a prescribed ℓ -mod representation. More precisely provide results on the number of elliptic curves $E/\mathbb{Q} : y^2 = x^3 + ax + b$ having a prescribed Galois ℓ -mod representation and height $h(E) = \max(|4a^3|, |27b^2|)$ less than a given real number $\epsilon > 0$ (or an other height). As in the case of finite fields I will start with small integer ℓ ($\ell = 3, 4, 5, 7$ or 11). As results in the literature in this direction one can cite : [15] that solve this question for each of the torsion subgroups given by Mazur's theorem, [16–18] who address this question for elliptic curves having a rational subgroup of order 3, 4 and 7 respectively. Here are some of the families I am currently working on :

- Let (p, n) a couple of integer such that p is prime, $0 \leq n < p$ and $x^6 + 160nx^3 - 80n^2$ is irreducible. I show that the modular polynomial $\Phi_5(j(E), x)$ is irreducible when $E/\mathbb{Q} : y^2 = x^3 + ax + b, a = kp$ and $b = k'p + n$, with $k, k' \in \mathbb{Z}$. We can take for example $(p, n) = (37, 2)$.

As these cases of families which haven't rational subgroup of order 5, here i will generate some such families and count them using an appropriate height (other families could be such that the smallest irreducible factor of $\Phi_5(j(E), x)$ has degree 2 or 3). It will also be question to search the densest family.

- For (p, n) a couple of integer such that p is prime, $0 \leq n < p$ and $3x^4 + 6nx^2 - n^2$ is irreducible. We have also the following family, for which the third division polynomial is irreducible.
 $E/\mathbb{Q} : y^2 = x^3 + ax + b, a = kp + n$ and $b = k'p$, with $k, k' \in \mathbb{Z}$. We can take for example $(p, n) = (29, 2)$.

9. Title : Computing Isogeny Between Hyper-elliptic Curves , Author : Fouazou Lontouo Perez Broon.

In the work 1 above we provide other formulas to compute isogenies on elliptic curves and in the work 2 above we show that a comparison of our formulas and the previous existing one leads to some relations characterizing the finite subgroups of elliptic curves. The objective of this work is to search how to do same with hyper-elliptic curves. In the literature the following works [19–22] provide formulas to compute isogeny on hyper-elliptic curves and some application in cryptography in [23], [24], [25],[26], [27], [28], [28], [29], [30]

10. Title : Counting isomorphism classes of hyper-elliptic Curves Over Finite Fields whose Rational ℓ -torsion of their Jacobean Have a Prescribed Group Structure , Author : Fouazou Lontouo Perez Broon.

In the literature there exist results on the computation of isomorphism classes of hyper-elliptic curves over finite fields [31–33]. The group structure of the ℓ -torsion of Jacobean of genus g hyper-elliptic curve is $(\mathbb{Z}/\ell\mathbb{Z})^{2g}$. The goal of this work is to compute the number of isomorphism class of hyper-elliptic curve whose the rational ℓ -torsion is $(\mathbb{Z}/\ell\mathbb{Z})^n$ with $1 < n < 2g$. In the literature some results on the structure of the rational ℓ -torsion of Jacobean of hyper-elliptic curve in [?] .

11. **Title :When Two not Isogenous Elliptic Curves Become Isogenous on an Extension of Finite Field, Author : Fouazou Lontouo Perez Broon.**

Let $E_0/\mathbb{F}_p : y^2 = x^3 + 1$ such that $p \equiv 1[3]$ (resp $E_0/\mathbb{F}_p : y^2 = x^3 + x$ such that $p \equiv 1[4]$) and $\ell = 5$ (resp $\ell = 3$). In this work I search the conditions on p such that there is a another curve E_1/\mathbb{F}_p not \mathbb{F}_p -isogenous to E_0 but \mathbb{F}_{p^3} -isogenous (resp \mathbb{F}_{p^4} -isogenous) to E_0 by a degree ℓ isogeny. I show that p must satisfy " $\sqrt{5} \in \mathbb{F}_p$ and $\sqrt[3]{-80 \pm 36\sqrt{5}} \notin \mathbb{F}_p$ " (resp " $\sqrt{3} \in \mathbb{F}_p$ and $\sqrt[2]{-1 \pm 2/\sqrt{3}} \notin \mathbb{F}_p$ "). For a such prime the checking can be done by computing the isogeny and the co-domain curve on the corresponding field extension. Here I address the question of search ℓ for a given p, of comparing the group structure of $E_0(\mathbb{F}_{p^3})$ and $E_1(\mathbb{F}_{p^3})$ (resp $E_0(\mathbb{F}_{p^4})$ and $E_1(\mathbb{F}_{p^4})$) also of comparing their group structures over the extension of \mathbb{F}_{p^3} (resp \mathbb{F}_{p^4}) so $E_0(\mathbb{F}_{p^{3k}})$ and $E_1(\mathbb{F}_{p^{3k}})$ (resp $E_0(\mathbb{F}_{p^{4k}})$ and $E_1(\mathbb{F}_{p^{4k}})$).

Example : for $p = 73$, $E_0/\mathbb{F}_p : y^2 = x^3 + x$ and $E_1/\mathbb{F}_p : y^2 = x^3 + 29x + 35$ are \mathbb{F}_{p^4} -isogenous by a degree 3 isogeny. $E_0(\mathbb{F}_{p^4}) \sim \frac{\mathbb{Z}}{240\mathbb{Z}} \oplus \frac{\mathbb{Z}}{118320\mathbb{Z}}$ and $E_1(\mathbb{F}_{p^4}) \sim \frac{\mathbb{Z}}{80\mathbb{Z}} \oplus \frac{\mathbb{Z}}{354960\mathbb{Z}}$. So they have same cardinality but different group structure. Moreover, for all $k \in \mathbb{N}^*$, $E_0(\mathbb{F}_{p^{4k}}) \sim E_1(\mathbb{F}_{p^{4k}})$.

In the literature [34] and [35] give results on the comparison of the group structures of isogenous curves on extensions of their base fields. I will also search primes p for which E_1 have good cardinality for cryptography.

12. **Title : Efficient Computation of Division polynomial on the Alternate Models of Elliptic Curve and Application , Author : Fouazou Lontouo Perez Broon.**

Let $(\mathcal{C}_{s,t})_{s,t \in K}$ an alternate model of elliptic curve and f a degree 2 function on $\mathcal{C}_{s,t}$ such that $f(-P) = f(P)$. The gaol of this project is to give a way to construct an analogue of McKee's algorithm [36] to compute efficiently the division polynomials associate to degree 2 functions f . I will also prove an analogues of [[37] theorem 2.2 and 2.7] for these division polynomials. I hope to apply these results to generalisation of division polynomial [38], order of points on elliptic curve [39] or other.

1.2 Selected Thematics for Training Activities With Some Related Research Topics

1.2.1 Selected Mathematics Areas

1. Fields Theory

Here I will address research topics related to fields theory such that : computing Galois group of polynomials [40, 41], computation of irreducible polynomials over finite fields using elliptic curves [42, 43], computation of an isomorphism between finite fields using elliptic curves [44, 45], use of elliptic curves to construct basis for efficient arithmetic on extension of finite fields [46].

I will also address research topics related to application of fields theory in cryptography such that : efficient arithmetic of finite fields for cryptography [47], discrete logarithm problem over finite fields and application in cryptography [48] and homomorphic encryption from the finite fields isomorphism problem [49]. The main outcomes of this part of project will be contemporary courses on the above research topics, design of learning materials for a graduate course on fields theory (in section 1.5.1 we gave syllabus for a such course) and also research directions to publish contributions on above research topics. I hope through the study of these research topics to design new learning materials.

2. Algebraic Numbers Theory

Here I will address some research topics on algebraic numbers theory such that : number fields having or not a power integral basis problem [50], computing the monoid of the ideals class of the orders in number fields or more generally an étale algebra [51], study of Pisot numbers and reciprocal algebraic integers [52], [53], computation of the euclidean minimum of number fields and norm-euclidean fields [54], computation of class group and unit group [55, 56].

I will also address research topics on application of numbers theory in cryptography such that : the variants of NTRU in which \mathbb{Z} is replaced by the some rings of integers [57, 58], public key cryptosystem based on quadratic residuosity problem [59], design of public key crypto-system which security repose on principal ideal problem (PIP) [60]. The main outcomes of this part of project will be contemporary courses on the above research topics, design of learning materials for a graduate course on algebraic numbers theory (in section 1.5.2 we gave syllabus for a such course) and also research directions to publish contributions on above research topics. I hope through the study of these research topics to design new learning materials.

3. Algebraic Curves

Arithmetic of abelian varieties, computation of the isogenies between them and cryptographic applications are the main topics of this project. For this reason, this part of the project will be first devoted to group operations on Jacobean of algebraic curve [61–63] and computation of isogenies between Jacobean of high genus curves [19–22]

Besides the applications of discrete logarithm problem and isogenies in cryptography, the algebraic curves can be also used to design crypto-systems such that : Constructions of authentication codes [64], asymptotic lower bound of frameproof codes obtained from algebraic-geometry codes [65], key pre-distribution Schemes and one-time broadcast encryption schemes from algebraic curve [66], construction of separating,cover-free and perfect hash families [67, 68]. These applications are covered in the following books [69, 70].

The main outcomes of this part of project will be contemporary courses on the above research topics, design of learning materials for a graduate course on theory of algebraic curves (in section 1.5.3 we gave syllabus for a such course) and also contemporary courses on some algebraic curve research topics besides their applications in cryptography such that : study

the group structure of Picard group of curve over finite fields, counting points on a curve over finite fields and computing endomorphism ring of Jacobian, (the book [71] will be the first reference used for these learning materials and research topics following by selection of other research papers).

4. Quaternion Algebras

The quaternion algebras is used to design crypto-system such that : the block cipher [72], the variants of NTRU in which \mathbb{Z} is replaced by the quaternion algebras over finite fields [73], PKC and signature with endomorphism ring of super-singular elliptic curves [74].

The mains out put of this part of project will be contemporary courses on the previous applications, design of learning materials for a graduate course on quaternion algebras and contemporary courses on some research topics on quaternion algebras besides their applications in cryptography (the book [75] will be the main reference used for these learning materials and research topics before selection of other research papers)

5. Abelian Varieties

Here I will first design learning materials for graduate course on complex abelian varieties and abelian varieties over finite fields [76, 77]. As in the case of Jacobean of algebraic curves I will also address research questions on arithmetic of abelian varieties, computation of isogenies between them and computation of their endomorphism rings.

6. Computational and Effective aspects of Algebraic Geometry

Here I will study some useful algorithms and effective aspects of algebraic geometry, the books [78, 79] will be used for this aims. Algebraic geometry have also several application in cryptography, here I will particularly interested to post-quantum resistant schemes from intersection of conics or quadric surfaces [80, 81]

I will design learning materials for a graduate course on these algorithms and contemporary course on this cryptographic application.

7. Modular Forms and Galois Representations of Elliptic Curves

Here I will address some research topics on the computation of modular forms and their application to elliptic curves namely : in the computation of Galois representation of elliptic curves [14, 82], in the application of the modular forms the point counting algorithm [83, 84], in computation of polynomials whose super-singular j-invariants are the roots [85] and computation of the Jacobi, Debekind, Theta function with other modular polynomials [6, 86, 87]. After moduli spaces of elliptic curves we will also carry out training activities on the moduli spaces of algebraic curves and abelian varieties [88].

I will design contemporary courses on the previous research topics and learning materials for a graduate/postgraduate course on the modular space of elliptic curves by using the books [89, 90] (a primary syllabus is given in section 1.5.4).

8. Advanced Topics in Elliptic Curve

Here I will interest to some advanced topic on elliptic curves namely : elliptic curve over local and global fields, integral points of elliptic curves [91] and CM elliptic curves [92].

I will address some research questions on these topics, design learning materials for graduate course and contemporary courses.

1.2.2 Programming and Foundation of Cryptology

1. Design and Security Proving of Cryptographic Scheme

Here I will study the design and the proof of security of some cryptographic protocol. The previous cryptographic protocol which can be designed using fields theory, number theory and algebraic curves will serve here as specific case of security proving.

I will use here the following books :

[93]

<https://doi.org/10.1007/978-3-319-57048-8>

<https://doi.org/10.1007/978-3-030-63287-8>

<https://doi.org/10.1007/978-3-031-19439-9>

and also [94] and [95]

2. Programming

In this part of the project we will study some programming language useful to implement the cryptographic scheme in Hardware environment and parallel computing.

— FPGA

<https://doi.org/10.1007/978-1-4302-6248-0>

<https://doi.org/10.1007/978-3-319-26408-0>

— assembly (ARM or x86)

<https://doi.org/10.1007/978-1-4842-6267-2>

<https://doi.org/10.1007/978-1-4842-0064-3>

— parallel computing

*[Morgan Kaufmann Publishers] Multicore and GPU Programming 2ed, (2021),
Gerassimos Barlas*

1.2.3 Quantum Algorithm

The goal of this part is to first carry out training activities on quantum computing and quantum algorithms for cryptology and computational number theory and geometry, next use these to carry out research for publications on the analysis and improvement of these algorithms

1. Training Activities on Quantum Algorithm and Programming

This part of the work will be devoted to training on mathematics of quantum computing and the first example of quantum algorithms for computational number theory and geometry. Below the books that could be used.

(a) Mathematics of the Quantum computing

- Wolfgang Scherer, **Mathematics of Quantum Computing**,
<https://doi.org/10.1007/978-3-030-12358-1>
 - Giacomo Nannicini, **An Introduction to Quantum Computing, without the Physics**. SIAM Review 2020
 - Andrew M. Childs, **Lecture Notes on Quantum Algorithms**
- (b) Some quantum programming language
- Weng-Long Chang and Athanasios V. Vasilakos **Fundamentals of Quantum Programming in IBM's Quantum Computers**
 - Alexander S. Green, **Quipper : A Scalable Quantum Programming Language**
 - PETER SELINGER, **Towards a Quantum Programming Language**
 - Bernhard Ömer, **Quantum Programming in QCL**
- (c) Quantum computational complexity
- John Watrous, **Quantum Computational Complexity**
- (d) Quantum algorithm for some computational problem from mathematics
- Abhijith J., Adetokunbo Adedoyin et al 2022. **Quantum Algorithm Implementations for Beginners**. ACM Transactions on Quantum Computing 3, 4, Article 18 (December 2022), 92 pages. <https://doi.org/10.1145/3517340>
 - WIM VAN DAM AND YOSHITAKA SASAKI, **QUANTUM ALGORITHMS FOR PROBLEMS IN NUMBER THEORY, ALGEBRAIC GEOMETRY, AND GROUP THEORY**
2. **Research and training activities on quantum algorithm for cryptography and computational number theory and geometry**
- Here I will first carry out training activities on the classical and quantum algorithms to solve some computational problems on some mathematical structures (from fields theory, numbers theory, quaternion algebra, algebraic curve and algebraic geometry), next carry out research on the analysis and improvement of these quantum algorithms. In fact this project is part of a career development project mainly devoted to research and training on these structures. The other computational problems are in the description of the career development project, most those selected here are those on which there exists in the literature quantum algorithm to solve them.
- (a) In fields theory :
- discrete logarithm problem over finite fields :[96], [97] , [98],[99], [100], [101]
 - Factorisation of polynomials over finite field : [102]
- (b) In number theory :
- Ideal-svp, Ring-LWE :[103], [104],[105],[106], [107], [108],
 - computing the ideal class group (CGP), principal ideal problem (PIP) and computing the unit group : [109], [110], [111],

- (c) in algebraic curve theory :discrete logarithm problem on (hyper)elliptic curves [112], [113], [114]
- (d) Classical and Quantum Algorithm to solve the Computational Cryptographic Assumption of Isogeny Based Cryptography :
 - On SIDH-like crypto-system : full key recover [115, 116], algorithm for path finding problem [117–119], compute the endomorphism ring of super-singular elliptic curve [120–122], torsion point attack [123–128], Quantum attack [129] , [130] and cycle in isogenies graph [131, 132].
 - On CSIDH like cryptosystem : [133], [134], [135], [136],[137], [138]
- (e) quaternion algebra :
 - Computing endomorphism of super-singular elliptic curve and quaternion ℓ -isogeny path problems(classical algorithms) :[139], [140], [141],[142], [143], [144]

1.2.4 Some Current Research Questions in Isogeny Based Cryptography

1. **Design of the current sure isogeny based Post-quantum Cryptographic protocol :**
 The goal here is to study the design, the prove of security and the implementation of the isogeny based post-quantum crypto-system next define some research questions on their implementation, on their cryptanalysis or on the design of other new crypto-systems.
 - OSIDH and Orientation of super-singular isogenies graph : [145], [120] and [146]
 - CRS, SURF, and CSIDH like crypto-system : These are three post-quantum crypto-systems based on the action of the ideals class group action on a elliptic curve (ordinary elliptic curve for CRS and super-singular elliptic curve for the CSIDH and the SURF).
 - (a) On the implementation : formulas and algebraic approach [147–152] constant time implementation [147, 153, 154], library [155–158] and parallel implementation [159]
 - (b) Other CSIDH like crypto-system : with CSIDH setting and class group action many post-quantum secure cryptographic primitives can be designed such that [157, 160, 160, 161, 161–163, 163–165]
 - SIDH like crypto-system : Path finding problem in the supersingular isogeny graph is hard computation problem which have a exponential quantum complexity and is equivalent to compute the endomorphism ring of a supersingular elliptic curve. However SIDH doesn't based only on this hard problem since it publish also the images of the torsion points and for this reason it have been broken. There exist other post-quantum crypto-system based only on this computational assumption and there is also some proposition on a better way to use these torsion points information.
 - (a) Current proposition to use the torsion points informations [166, 167] the idea underlying the Castriyck and Decru attack can be also used constructively in [168], [169].

- (b) on the implementation : SIDH implementation [170, 171], on implementation of CGL Hash Function [172–174, 174, 175]
 - (c) other SIDH like crypto-system : pseudo-random functions [176, 177], digital signature [169, 178], PAKE [179], VDF [180], [122] and public key encryption [181].
2. **Meeting of Pairing and Isogeny** : The pairing are useful in cryptography since it enable to design many cryptographic protocols. They exist some works which combine the pairing and the isogeny to design the protocols. The goal of this part of our project is to study these works and define our own research questions on the implementation, protocols design or algorithms to solve the related computational assumption [182–185]
 3. **Computation of isogeny between the Jacobean of high genus curve and application in cryptography** : While most of the isogeny based crypto-systems are designed with elliptic curve some of them can be also implemented with high genus curve (namely hyper-elliptic curve of genus 2). The goal of this part of our project is to study the current existing results on the computation isogeny between high genus curve, their applications in cryptography and also the definition of our own research questions.
— [23], [24], [25],[26], [27], [28], [28], [29], [30]
 4. **Classical and Quantum Algorithm to solve the Computational Cryptographic Assumption of Isogeny Based Cryptography** :
The goal of this part of the project is to study the cryptanalysis in isogeny based cryptography and the classical/quantum algorithm to solve the computational assumptions on which repose the security of the isogenies based post-quantum protocols.
— on the cryptanalysis of the OSIDH : [120] and [186]
— on the cryptanalysis of the CSIDH like crypto-system :
— vulnerability under hardware implementation and countermeasure [187], [188],[189], [190],[189], [191]
— quantum and classical algorithm to solve the related computational assumption [133], [134], [135], [136],[137], [138]
— on the cryptanalysis of the SIDH like crypto-system : full key recover [115, 116], algorithm for path finding problem [117–119], compute the endomorphism ring of super-singular elliptic curve [120–122], torsion point attack [123–128], Quantum attack [129] , [130] and cycle in isogenies graph [131, 132].

Study these existing classical and quantum algorithm to solve the computational assumption on which repose the security of isogeny based cryptography is the goal of this part of the project and also make a research on the search of new algebraic approach to solve these assumptions.

1.3 Syllabus of Some Courses to Generate Learning Materials at Graduate and Postgraduate Level

1.3.1 Fields Theory

Chapter 1 : Fields Extensions, Rupture Field, Splitting Field and Algebraic Closure

1. First definition : Morphism between fields, fields extensions, intermediate extensions and morphism between fields extensions. Field generated by 1_K , definition of the characteristic and construction of the prime fields \mathbb{F}_p . Construction and Definition of Frobenius endomorphism, case of finite field and definition of perfect fields.
2. Algebraic elements in an fields extension and telescopic base theorem. Construction of rupture field, proof of their universal property and number of k -embedding from a rupture field $k(x)/k$ to a given field L/k . Transitivity of the algebraic fields extensions, Proof of the existence of splitting fields of a polynomial and of their uniqueness up to k -isomorphism.
3. Definition of the algebraic closures of a field, proof of the existence of a biggest intermediate algebraic extension in a given fields extension, Artin's proof of the existence of an algebraic closure field. For a given algebraic extension fields $k \subset \mathbb{K}$ and a morphism $\tau : k \longrightarrow \bar{k}$ proof the existence of an extension of τ to \mathbb{K} . Proof of that the algebraic closures of a field k are k -isomorphic.
4. For a given extension $K \subset L$ of finite degree, define trace $Tr_{L/K}$ and norm $N_{L/K}$ maps, proof that $Tr_{L/K}$ is K -linear and $N_{L/K}$ is multiplicative. Computation of them from computation of the characteristic polynomial of the K -linear map $m_x : L \longrightarrow L$, $m_x(y) = x * y$. Proof that the characteristic polynomial of m_x is a power of the minimal polynomial of x . Computing characteristic polynomial of m_x , $Tr_{L/K}$ and $N_{L/K}$ from the K -embeddings of L in \bar{K} .

Computation and direction to generate materials for the learning activities

- Linearly disjoint fields extension.
- Computation of the minimal polynomials in an algebraic fields extensions.
- Computing characteristic polynomial of m_x , $Tr_{L/K}$, $N_{L/K}$ and dual basis of a given base of the extension $K \subset L$.
- Transcendental fields extensions in positive characteristic.

Chapter 2 : Separable, Normal and Galois Fields Extensions

1. Definition of separable polynomial and separable fields extensions, some characterizations of separable the polynomials. Characterization of separable extensions $k \subseteq \mathbb{K}$ by the number of k -morphism from \mathbb{K} to \bar{k} , characterization of the separability of $k \subset k[x]$ by the separability of x , transitivity of the separable extensions.
2. Proof the existence of a primitive element for separable extension of finite degree. Characterization of the finite degree separable extensions by the finiteness of the $deg_k(\alpha)$ for

- all $\alpha \in \mathbb{K}$. Characterization of primitive extensions by the finiteness of their intermediate extensions.
3. Definition of normal fields extensions and case of splitting field of a polynomial. Definition and some characterization of Galois fields extensions. Proof of Artin's theorem and characterization of Galois extensions by the set of fixed elements of its Galois group. Galois correspondence between the intermediate extensions of $k \subseteq \mathbb{K}$ and the subgroups of the automorphism group $\text{Gal}(\mathbb{K}/k)$, characterization of the intermediate extensions $k \subseteq L \subseteq \mathbb{K}$ for which $k \subseteq L$ is a Galois extension. Definition and proof of the existence of the normal closures (resp Galois closure) for an extension of finite degree (resp a separable extension of finite degree) and an another proof of the finiteness of the intermediate extensions of a separable extension of finite degree.

Computation and direction to generate materials for the learning activities

- Normal basis theorem
- characterization of the linear disjoint sub-extensions in a Galois extensions.
- Kummer's theory, Artin-Scheier's theory, additive and multiplicative form of Hilbert 90 theorem.
- Construction of the lattice of subgroups and intermediate extensions of a Galois extension.
- Computation of the intermediate extensions of a Galois extension knowing a primitive element and inclusion criterion of these intermediate extensions.

Chapter 3 : Finite Fields

1. Cardinal of finite fields and of their extensions of finite degree. Proof that the multiplicative group of a finite fields k^* is a cyclic group. Proof of existence and uniqueness up to isomorphism of a fields of cardinal p^n . Proof that a finite field of cardinal $p^{n \cdot k}$ contain an unique field of cardinal p^n . Proof that the finite field extension $\mathbb{F}_q \mathbb{F}_{q^n}$ is a Galois's extension of cyclic Galois group generated by the Frobenius map $\text{Fr}_q(x) = x^q$.
2. Give and prove the decomposition of the polynomial $x^{q^n} - x$ in irreducible polynomials over \mathbb{F}_q . Construction and proof of the algebraic closure of the finite fields of characteristic p .

Computation and direction to generate materials for the learning activities

- Quadratic residues in finite fields, some Dirichlet's arithmetic progressions and Gauss's sum.
- Study of the trace and Norm operators in the case of finite fields extensions $\mathbb{F}_q \subset \mathbb{F}_{q^n}$.
- Study of the \mathbb{F}_q -linear endomorphism of the finite fields \mathbb{F}_{q^n}
- Primitive roots of unit in a finite fields.
- irreducibility tests of polynomials over finite fields

Chapter 4 : Splitting Fields of Polynomials

1. Proof that the Galois groups of polynomials and Galois closure extensions of the separable extensions are the subgroups of symmetric groups.
2. Writing a symmetric polynomial in term of elementary symmetric polynomials. Proof that the field of multivariate rational function is a Galois extension of the fields generated by

the elementary symmetric polynomials with Galois group isomorphic to symmetric group. Definition of the general equation of degree n and proof that its splitting field is of Galois group the symmetric group S_n .

3. Definition of the discriminant of a polynomial and their computation in term of the coefficients or the roots of the polynomial. Its use for the characterization of the separable polynomials and case of polynomial $x^n + px + q$. Characterization of the separable polynomial $P \in k[X]$ whose the square root of their discriminant $d = \sqrt{\text{disc}(P)}$ is in k and structure of the Galois group of $k[d] \subset k(P)$ in the other case (where $k(P)$ is the splitting field of P).
4. Definition of simple radical (and radical) fields extensions and solvable polynomials. Proof that a simple radical fields extension $K \subset K[a]$ with $a^n \in K$ is a Galois extension when K contain a primitive n^{th} roots of unit and give the polynomial and the Galois of this extension. Proof that for two extensions $k \subset K \subset K[a]$ where $k \subset K$ is a Galois extension and $K \subset K[a]$ is a simple radical extension, then the splitting field of the minimal polynomial of a on k is a radical extension of K . Use these previous results to prove that the Galois groups of solvable polynomials are soluble groups. Proof of the Eisenstein's irreducible criterion of polynomials $P \in \mathbb{Z}[X]$ and sample of insolvable polynomial.

Computation and direction to generate materials for the learning activities

- Intermediate extension of a cyclotomic fields extensions, relation between the cyclotomic polynomials and computation of them.
- some specifications of the general degree n equation.
- Group of the roots of a fields.
- Study and computation of the Galois group of some polynomials.

1.3.2 Algebraic Number theory

Chapter 1 : Quadratic Reciprocity Law

1. Definition of quadratic residues modulo an integer, number of quadratic residues modulo a odd prime number, proof of the Euler's criterion to characterize the quadratic residues, definition of Legendre symbol and proof of its multiplicity. computation of $(\frac{a}{p^n})$ and $(\frac{a}{2^n})$ in term of $(\frac{a}{p})$ and $(\frac{a}{8})$ and application of quadratic reciprocity law to compute the value of Legendre symbol $(\frac{p}{q})$ (can involve factorization).
2. Definition of $\bar{\mathbb{Z}}$, proof that it is a ring and $\mathbb{Z} = \mathbb{Q} \cap \bar{\mathbb{Z}}$. Characterization of the elements of $\bar{\mathbb{Z}}$ by their action on an additive subgroup of \mathbb{C} and proof that the congruence between three integers a, b and n in $\bar{\mathbb{Z}}$ is equivalent to its congruence in \mathbb{Z} . Definition of Gauss sum, computation of its square and application to proof the quadratic reciprocity law.
3. Definition of Jacobi symbol, proof some of its properties and algorithm to compute its using only euclidean division (as more expensive operation).

4. Proof of the Gauss's theorem on the group structure of $(\mathbb{Z}/p^n\mathbb{Z})^\times, (\mathbb{Z}/2^n\mathbb{Z})^\times$ and more generally $\mathbb{Z}/m\mathbb{Z}$. Extension of the Euler's criterion to characterize the elements of $\mathbb{Z}/p\mathbb{Z}$ which are a n-power.

Computation and direction to generate materials for the learning activities

- Number of square of $\mathbb{Z}/p\mathbb{Z}$ in $\{1, \dots, \frac{p-1}{2}\}$.
- Solovay-Strassen's primality test.
- Sign of the Gauss's sum.
- the generators of $(\mathbb{Z}/p\mathbb{Z})^\times$.
- Number of square in $(\mathbb{Z}/N\mathbb{Z})^\times$.

Chapter 2 : Geometry of Numbers

1. Definition of a lattice in \mathbb{R}^n , proof that the \mathbb{Z} -module generated by a \mathbb{R} -basis of is a lattice of \mathbb{R}^n and that the lattice of \mathbb{R}^n can be always write on this form. Proof that the \mathbb{Z} -basis of a lattice of \mathbb{R}^n have same cardinality n .
2. Definition of the fundamental domains of a lattice and proof that they have the same Lebesgue's measure (called co-volume of the lattice). Proof of the Minkowski's convex Body theorem and relation between the co-volume of a lattice and the co-volume of the sub-lattice contained in its.

Computation and direction to generate materials for the learning activities

- Application to prove the Fermat-Euler theorem and Lagrange theorem.
- Proof that the finitely generated subgroups A of a \mathbb{Q} -vector space V have a \mathbb{Z} -basis of cardinality $\dim_{\mathbb{Q}}(V)$.
- Computation of the co-volume of some lattice in \mathbb{Z}^n .
- Study the lattice of integer of \mathbb{R}^n ($u, v \in L$ then $u \cdot v \in \mathbb{Z}$).

Chapter 3 : Ring OF Integer of a Number Field

1. **Definition and computation of the ring of integer** : Definition of $\mathcal{O}_{\mathbb{K}}$ the integers ring of a number field \mathbb{K} . For $x \in \mathbb{K}$ prove the existence of $m \in \mathbb{Z}$ such that $m \cdot x \in \mathcal{O}_{\mathbb{K}}$ and that $\mathcal{O}_{\mathbb{K}}$ is integrally closure, characterization of the elements of $\mathcal{O}_{\mathbb{K}}$ by their minimal polynomials or kernel polynomials. Computation of $\mathcal{O}_{\mathbb{K}}$ in the case of quadratic fields.
2. **Group structure of $\mathcal{O}_{\mathbb{K}}$ and orders of \mathbb{K}** : Proof that $\mathcal{O}_{\mathbb{K}}$ is a free \mathbb{Z} -module of rang $[\mathbb{K}, \mathbb{Q}]$ and first algorithm to compute its basis. Index of a lattice in $\mathcal{O}_{\mathbb{K}}$ and definition of the discriminant of a number field.
3. **Case of cyclotomic field** : for p a prime and $\mathbb{Q}(x)/\mathbb{Q}$ with $x \in \bar{\mathbb{Z}}$ a number field, proof that $\mathbb{Z}[x]$ is of index prime to p in $\mathcal{O}_{\mathbb{K}}$ when $\text{irr}_{\mathbb{Q}}(x)$ is a Eisenstein polynomial in p and application to computation of the ring of integers of a cyclotomic field.

Computation and direction to generate materials for the learning activities

- Computing norm, trace, kernel and minimal polynomial of the elements in \mathbb{K} .
- computing the basis of the ring of integer.
- computing the discriminant of the orders.

- recognizing elements of $\mathcal{O}_{\mathbb{K}}$ using LLL.
- characterization the unities of $\mathcal{O}_{\mathbb{K}}$ using norm operator. The group of the roots of unity contained in a numbers field and Kronecker's characterization of the roots of unity of a numbers field.
- characterization of the rings of integers of a numbers field which are monogenic.
- Sign of the discriminants of the number fields and Stickelberger's proof on their values modulo 4.

Chapter 4 : FINITENESS OF THE NUMBER OF IDEALS CLASS

1. For A an order of \mathbb{K} definition of the equivalent class of an ideal, multiplication of the ideals and monoide set of the ideals class. Proof of the finiteness of the ideals class number admitting the Minkowski bound.
2. Proof that for any integer in the Minkowski's bound each ideals class have an ideal containing this integer. Computing in the case of monogenic orders the ideals J containing a given prime p and the structure of the ring A/J .
3. For a number field \mathbb{K} on degree n , construction of an embedding $\iota : \mathbb{K} \longrightarrow \mathbb{R}^n$, proof that $\iota(\mathcal{O}_{\mathbb{K}})$ in a lattice of \mathbb{R}^n and computation of its co-volume from the discriminant of $\mathcal{O}_{\mathbb{K}}$.
4. Proof that the ideal of a lattice contain a \mathbb{Z} -basis, definition of the norm of an ideal and computation of its in the case principal ideals.
5. Proof the Minkowski's upper bound of the norm $N(x)$ of the elements of an ideal I (or the upper bound of the index $|I/xA|$ when $x \in I$). Proof of the Minkowski's lower bound on the discriminant of the degree n number fields.

Computation and direction to generate materials for the learning activities

- Proof of the finiteness of the ideals class number using "pigeonhole principle".
- Explicit formula for the orders of quadratic imaginary fields.
- Characterization of the ring of integers \mathcal{O}_K by the invertibility of the ideals (or by the invertibility of the maximal ideals).
- Ring of integers of the cyclotomic fields $\mathbb{Q}(e^{2\pi i/p})$ (for p a prime).
- Hermite's theorem on infinity of number fields having same degree and same discriminant.

Chapter 5 : FACTORIZATION OF THE IDEALS

1. Define invertible ideal of a order (ideal class) and some of their properties (simplification and devise all ideal contained in it). Proof that in $\mathcal{O}_{\mathbb{K}}$ all ideal is invertible. Proof some properties of the prime ideals in a order : the existence and the finiteness of the prime ideals containing a given prime number and the uniqueness of the prime number contained in a prime ideal. Also that the prime ideals are maximal.
2. Proof that in $\mathcal{O}_{\mathbb{K}}$ every ideal can split as a product of prime ideals. Proof of the multiplicity of the norm of the ideals and application to provide the different factorizations of the ideals $p\mathcal{O}_{\mathbb{K}}$ (for p a prime).

Computation and direction to generate materials for the learning activities

- Proof that the factorial orders and principal orders are same.
- For the monogenic orders $A = \mathbb{Z}[\alpha]$: criterion for the unique factorization of the ideals, multiplicity of the norm operation $N(I)$ on the ideals (ie $N(IJ) = N(I)N(J)$) and invertibility of the prime ideals.
- Ring of integers which are not monogenic.
- Principality criterion of the ring of integers of the cyclotomic fields $\mathbb{Q}(e^{2\pi i/p})$ (for p a prime).
- Buchman-Lenstra's algorithm to factor the $p\mathcal{O}_K$ in term of prime ideals.
- Chinese Remainder Theorem (CRT) and at most number of generators of an ideal in a Dedekind domain.

Chapter 6 : Dirichlet's Unit Theorem

characterization of the unit by their norm, construction of a morphism from the unit group of K to \mathbb{R}^{r+s} . Proof that the kernel of this map is a finite cyclic group, its image is discrete, lie in a hyperplane and application to prove the Dirichlet's Unit theorem.

1.3.3 Algebraic Curves

Chapter 1 : Intersection Multiplicity

Definition of the intersection multiplicities of two affine plane curves $F = 0$, $G = 0$ (resp projective curves) at a point P and an algorithm to compute it. Definition of the multiplicity and tangent of a point on an affine curve (resp projective curves). Characterization of the tangent at a point, Jacobi criterion of smooth points and computation of their tangents.

Computation and direction to generate materials for the learning activities

- Another definition of the intersection multiplicity of a line and a curve (as smallest degree of the monomials of an univariate polynomial) and another characterization of the singular points, tangents and m -fold points on a curve (or points of multiplicity m).
- Characterization of curves having finitely many singular points.
- Study of inflection points, cusp points and Hessian of a curve.
- Study of the polar curve of a point with respect of a curve, definition of nucleus of a curves and strange curves.
- some results from elimination theory :
 1. Characterization of curves $F = 0, G = 0$ having a common factor (also irreducible curve $F=0$ dividing a curve $G = 0$)
 2. Relation between intersection multiplicity of two curves and resultant. Definition of the index of an irreducible curve and proof that curve of index null have only ordinary singularity (singularity with distinct tangents).

Chapter 2 : Bézout Theorem and Some Applications

- Proof of Bézout theorem.
- Definition of rational transformation between curves and characterization of rational transformations which are birational (Cremona transformation). Study the particular case of quadratic transformation between curve.

Resolution of singularity :

1. Definition of virtual genus of a curve and proof that it is not negative.
2. Transformation of a curve to an another having only ordinary singularity by sequence of quadratic transformations. Comparing the genus of a curve (resp ideal generated by its) with the genus of it image by a quadratic transformation (resp ideal generated by its). Definition of terrible point on a curve.

Chapter 3 : Branch AND Parametrization

- Investible elements of the ring $K[[X, Y]]$, Characterization of the K-homomorphism, K-monomorphism and K-automorphism of the ring $K[[t]]$. For a curve $F(x, y) = 0$ with $F(0, 0) = 0$ and $\frac{\partial F}{\partial Y} \neq 0$ proof of the existence of a parametrization $x = t$ and $y = c_1 t + c_2 t^2 \dots$. Using this parametrization to compute the intersection multiplicity of two curves at a non-singular point. Hensel's lemma to prove the reducibility of a polynomial $F \in K[[x]][y]$ when $F(0, Y)$ is reducible.
- Definition of branch representation, their orders and equivalence between them. Image of a branch representation by a K-monomorphism of $K[[t]]$, relation between the order of a branch and the order of its image, definition of primitive and imprimitive branch representation. Study of the fields $K(x(t), y(t))$ where $(x(t), y(t))$ is an affine branch representation, proof that each branch representations is the image by a K-monomorphism of $K[[t]]$ of a primitive branch representation and definition of the ramification index of a branch representation. definition of reducible branch, proof that a branch representation of order n can be write on the form $x(t) = u + t^n; y(t) = v + \eta(t)$ with $\text{ord}(\eta(t)) \geq n$. Use this form to characterize reducible branch and imprimitive branches.
- Proof the existence and unicity of a branch of a curve centered at a simple point. Definition of the intersection multiplicity of a curve and a branch representation. Definition of local quadratic transformation and geometric transform of a curve, application to prove the finiteness of the number of branch at a given point of a curve. Proof that in the case of ordinary singularities there is equality between the number of branches and the multiplicity of the point. Alternate definition of intersection multiplicity of two curves in term of the intersection of one with the branches of other.
- Given two irreducible curves $F = 0$ and $G = 0$ definition of the Noether's condition at a point P and proof that polynomials satisfying the Noether's condition at all point are in the ideal (F, G) . Give and prove the Lasker-Noether decomposition of the ideal (F, G) .
- Definition of the Noether's condition and characterization of the polynomials of the ideal (F, G) where $F, G \in K[X, Y]$. Prove the Lasker-Noether's decomposition of the ideal.

Chapter 4 : FUNCTIONS, DIVISORS, MAPS BETWEEN CURVES AND DIFFERENTIALS

1. Define the multiplicity of functions at a point of a curve. Proof that the local ring at a point of a curve has an unique maximal ideal which is principal and computation of the uniformizer. Define the divisor of a function, proof that their degree is null and that function of divisor

null are constants.

2. Definition of Picard group of a curve. In the case of curve of degree greater than 3 prove that there is an embedding from curve to its Picard group. In the case of cubic use this embedding to construct a group law on the points of curve.
- Definition of generic points of a curve, Proof that they are isomorphic for irreducible curve and that branch representation are generic points . Use the generic points to provide an alternate definition of the function field of a curve and the rational map from a curve (given by two generic points such that the coordinates of one being rational function of the coordinates of the other). Study the case of bi-rational transformation between curves and define "model of curve".
- Definition of the place of a function field $K(\mathcal{C})$ and use this to provide an alternate definition of zeros and poles of the functions. Proof that the number of zeros or poles of a function f in $[K(\mathcal{C}), K(f)]$. In positive characteristic give and prove the purely inseparable sub-extensions of $K \subset K(\mathcal{C})$ with a criterion for separability in $K(\mathcal{C})$. Definition of separable and inseparable morphism, proof that Frobenius maps $\pi_q(x, y) = (x^q, y^q)$ is inseparable of degree q .

Chapter 5 : RIEMANN-ROCH THEOREM

1. Definition of the Riemann-Roch space $L(D)$ associated to a divisor and proof that they are vector spaces. The cases of zero divisor and the divisors of negative degrees, comparison of $L(D)$ by comparing their associated divisors, isomorphism between the $L(D)$ associated to equivalent divisors.
2. Give and prove an upper bound of the $\dim_k(L(D))$ in term of degree of the associated divisor. Explicit $\dim_k(L(D))$ in the cases of curves of degree one or two. Cases of divisors (P) and (P)-(Q) for curves of degree at least 3.
3. Definition of the genus of a curve and proof of the Riemann's theorem on the lower bound of $\dim_k(L(D))$ in term of genus and degree of the associated divisor.
4. Definition of the canonical divisor class on a plane algebraic curve and proof of an equivalent definition as divisor of a differential. Degree of a canonical divisor and proof of the Riemann-Roch's theorem.

Chapter 6 : CARDINALITY OF CURVES OVER FINITE FIELDS

- For \mathcal{C}/\mathbb{F}_q a curve of genus g , proof that the knowing of $\text{card}(\mathcal{C}(\mathbb{F}_{q^i}))$ $i \in \{1, \dots, g\}$ is equivalent to the knowing of the coefficient of Zeta function and enable to compute the cardinality of the curve over any other extension of \mathbb{F}_q (by functional equation of Zeta function).
- Definition of the irreducible divisors $D = P + P^\sigma + \dots + P^{\sigma^n}$ (where $\sigma : x \mapsto x^q$, $P \in \mathcal{C}(\mathbb{F}_{q^n})$ and $P \notin \mathcal{C}(\mathbb{F}_{q^i})$ with $i < n$) and rewriting of Zeta function in term of the number of effective \mathbb{F}_q -rational divisors.
- Proof that $\text{card}(\text{Pic}^n(\mathcal{C})(\mathbb{F}_q))$ is finite and $\text{card}(\text{Pic}^n(\mathcal{C})(\mathbb{F}_q)) = \text{card}(\text{Pic}^0(\mathcal{C})(\mathbb{F}_q))$. Use these to prove that the Zeta function is a rational function $Z(\mathcal{C}, \mathbb{F}_q) \in \mathbb{Q}(T)$. Use this rational expression to prove that curve over finite fields always have rational divisor of degree 1.

- Proof that $c \mapsto K_C - c$ is a bijection on the set of divisor of degree less than $2g - 1$ and use this to prove the functional equation satisfied by Zeta function.
- Proof of the Riemann's hypothesis
- Proof of the Hasse-Weil's bound, Hasse-Weil-Serre's bound, Ihara's bound, and family of Oesterle's bound.

1.3.4 Modular Forms and Galois Representations of Elliptic Curves

Chapter 1 : Galois Representations Attached to Elliptic Curves

Subgroup of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$ and their Dickson classification, Elliptic curve define over \mathbb{Q} (more generally over local and global field). Computing the torsion points field of an elliptic curve, algorithm to compute the representation $\rho_{E,\ell}$ and certificate its surjectivity. ℓ -adic Galois representation ρ_{E,ℓ^∞}

Chapter 2 : Modular Curve

Elliptic curve over complex number (elliptic function, complex tori, analytic map between complex tori and endomorphism ring of complex tori). Discrete and congruent subgroup of $SL_2(\mathbb{R})$, construction of the modular curve $Y(H)$ associated to a discrete subgroup $H \subset SL_2(\mathbb{R})$ as the action of this subgroup on the upper-half plan (proof of their topological properties and chart for its Riemann surface structure). Cusps and Elliptic points associated to a discrete subgroup of $SL_2(\mathbb{R})$ and construction of the modular curve $X(H)$ (proof that it is compact and charts for its Riemann surface structure). The fundamental domain and elliptic points for $SL_2(\mathbb{Z})$, formula to compute the genus of the modular curve $X(H)$ when H is a congruent subgroup of $SL_2(\mathbb{Z})$.

Chapter 3 : Modular forms

- Definition of modular form of weight k to $SL_2(\mathbb{R})$ (and cusp form), example of the Eisenstein's series, proof the existence of their q -development, fitness of the dimension of space of modular form of weight k . q -development of the normalized Eisenstein's series, Jacobi's function and J -invariant function. $K/12$ formula and application to compute the dimension of $\mathcal{S}_k(SL_2(\mathbb{R}))$ for $k < 12$ and explicit dimension of $\mathcal{S}_k(SL_2(\mathbb{R}))$.
- For a congruent subgroup Γ of $SL_2(\mathbb{R})$ definition of modular form of weight k with respect to Γ and condition of existence a q_h -development. Example the Eisenstein serie $G_2, N \in \mathcal{M}_2(\Gamma_0(N))$ and definition of the Dedekind eta function.
- Definition of automorphic form of weight k with respect to Γ and proof that their vector space is isomorphic to vector space of meromorphic differentials of $X(\Gamma)$. Dimension formula for dimension of the vector spaces $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$.

Bibliographie

- [1] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273 : 305–347, 1971.
- [2] Dustin Moody and Daniel Shumow. Analogues of Vélu’s formulas for isogenies on alternate models of elliptic curves. *Mathematics of Computation*, 85(300) :1929–1951, 2016.
- [3] Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted hessian curves. *Journal of Mathematical Cryptology*, 15 :345–358, 03 2021. doi : 10.1515/jmc-2020-0037.
- [4] Fouazou Lontouo Perez Broon and Emmanuel Fouotsa. Analogue of vélu’s formulas for computing isogenies over hessian model of elliptic curves. *IACR Cryptol. ePrint Arch.*, page 1480, 2019. URL <https://eprint.iacr.org/2019/1480>.
- [5] Josep M. Miret, Ramiro Moreno Chiral, and Anna Rio. Generalization of vélu’s formulae for isogenies between elliptic curves. *Publicacions Matemàtiques*, Proceed. I JTN : 147–163, 06 2007. doi : 10.5565/PUBLMAT_PJTN05_07.
- [6] François Morain. Computing the charlap-coley-robbins modular polynomials, 2023. URL <https://arxiv.org/abs/2302.05217>.
- [7] Reza Farashahi and Igor Shparlinski. On the number of distinct elliptic curves in some families. *Des. Codes Cryptography*, 54 :83–99, 01 2010. doi : 10.1007/s10623-009-9310-2.
- [8] Dustin Moody and Hongfeng Wu. Families of elliptic curves with rational 3-torsion. *Journal of Mathematical Cryptology*, 5(3-4) :225–246, 2012. doi : doi: 10.1515/jmc-2011-0013. URL <https://doi.org/10.1515/jmc-2011-0013>.
- [9] Omran Ahmadi and Robert Granger. On isogeny classes of edwards curves over finite fields. *Journal of Number Theory*, 132(6) :1337–1358, 2012. ISSN 0022-314X. doi :

- <https://doi.org/10.1016/j.jnt.2011.12.013>. URL <https://www.sciencedirect.com/science/article/pii/S0022314X1200025X>.
- [10] Nicholas M. Katz and. 2, 3, 5, legendre : \pm trace ratios in families of elliptic curves. *Experimental Mathematics*, 19(3) :267–277, 2010. doi : 10.1080/10586458.2010.10390623. URL <https://doi.org/10.1080/10586458.2010.10390623>.
- [11] Roland Auer and Jaap Top. Legendre elliptic curves over finite fields. *Journal of Number Theory*, 95(2) :303–312, 2002. ISSN 0022-314X. doi : <https://doi.org/10.1006/jnth.2001.2760>. URL <https://www.sciencedirect.com/science/article/pii/S0022314X0192760X>.
- [12] Andrew V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Math. Comput.*, 81(278) :1131–1147, 2012. doi : 10.1090/S0025-5718-2011-02538-X. URL <https://doi.org/10.1090/S0025-5718-2011-02538-X>.
- [13] Igor E. Shparlinski and Liangyi Zhao. Elliptic curves in isogeny classes. *Journal of Number Theory*, 191 :194–212, 2018. ISSN 0022-314X. doi : <https://doi.org/10.1016/j.jnt.2018.04.017>. URL <https://www.sciencedirect.com/science/article/pii/S0022314X18301367>.
- [14] ANDREW V. SUTHERLAND. Computing images of galois representations attached to elliptic curves. *Forum of Mathematics, Sigma*, 4 :e4, 2016. doi : 10.1017/fms.2015.33.
- [15] Robert Harron and Andrew Snowden. Counting elliptic curves with prescribed torsion. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 2017(729) : 151–170, 2017. doi : doi:10.1515/crelle-2014-0107. URL <https://doi.org/10.1515/crelle-2014-0107>.
- [16] Maggie Pizzo, Carl Pomerance, and John Voight. Counting elliptic curves with an isogeny of degree three. *Proceedings of the American Mathematical Society, Series B*, 7 :28–42, 03 2020. doi : 10.1090/bproc/45.
- [17] Carl Pomerance and Edward Schaefer. Elliptic curves with galois-stable cyclic subgroups of order 4. *Research in Number Theory*, 7, 06 2021. doi : 10.1007/s40993-021-00259-9.
- [18] Grant Molnar and John Voight. Counting elliptic curves over the rationals with a 7-isogeny. *Research in Number Theory*, 9, 10 2023. doi : 10.1007/s40993-023-00482-6.

- [19] Romain Cosset and Damien Robert. Computing (ℓ, ℓ) -isogenies in polynomial time on jacobians of genus 2 curves. *Math. Comput.*, 84(294) :1953–1975, 2015. doi : 10.1090/S0025-5718-2014-02899-8. URL <https://doi.org/10.1090/S0025-5718-2014-02899-8>.
- [20] Sean Ballentine, Aurore Guillevic, Elisa Lorenzo García, Chloe Martindale, Maike Massierer, Benjamin Smith, and Jaap Top. Isogenies for point counting on genus two hyperelliptic curves with maximal real multiplication. In Everett W. Howe, Kristin E. Lauter, and Judy L. Walker, editors, *Algebraic Geometry for Coding Theory and Cryptography*, pages 63–94, Cham, 2017. Springer International Publishing. ISBN 978-3-319-63931-4.
- [21] Jean-Marc Couveignes and Tony Ezome. Computing functions on jacobians and their quotients. *LMS Journal of Computation and Mathematics*, 18(1) :555–577, 2015. doi : 10.1112/S1461157015000169.
- [22] Enea Milio. Computing isogenies between jacobians of curves of genus 2 and 3. *Math. Comput.*, 89(323) :1331–1364, 2020. doi : 10.1090/mcom/3486. URL <https://doi.org/10.1090/mcom/3486>.
- [23] Ariana Goh, Chu-Wee Lim, and Yan Bo Ti. Generalising fault attacks to genus two isogeny cryptosystems. *2022 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 38–49, 2022.
- [24] Craig Costello and Benjamin Smith. The supersingular isogeny problem in genus 2 and beyond. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 151–168, Cham, 2020. Springer International Publishing. ISBN 978-3-030-44223-1.
- [25] Elie Eid. Fast computation of hyperelliptic curve isogenies in odd characteristic. *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, 2020.
- [26] Ramsès Fernández-València. Undeniable signatures based on isogenies of supersingular hyperelliptic curves. *ArXiv*, abs/1908.07458, 2019.
- [27] Maria Corte-Real Santos, Craig Costello, and Sam Frengley. An algorithm for efficient detection of (n, n) -splittings and its application to the isogeny problem in dimension 2. *IACR Cryptol. ePrint Arch.*, 2022 :1736, 2022.
- [28] Toshiyuki Katsura and Katsuyuki Takashima. Counting richelot isogenies between superspecial abelian surfaces. *Open Book Series*, 2020.

- [29] Wouter Castryck, Thomas Decru, and Benjamin A. Smith. Hash functions from superspecial genus-2 curves using richelot isogenies. *Journal of Mathematical Cryptology*, 14 :268 – 292, 2019.
- [30] E. V. Flynn and Yan Bo Ti. Genus two isogeny cryptography. In Jintai Ding and Rainer Steinwanddt, editors, *Post-Quantum Cryptography*, pages 286–306, Cham, 2019. Springer International Publishing. ISBN 978-3-030-25510-7.
- [31] Y. Choie and D. Yun. Isomorphism classes of hyperelliptic curves of genus 2 over F_q . In Lynn Batten and Jennifer Seberry, editors, *Information Security and Privacy*, pages 190–202, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg. ISBN 978-3-540-45450-2.
- [32] Luis Hernández Encinas, Alfred Menezes, and Jaime Muñoz Masqué. Isomorphism classes of genus-2 hyperelliptic curves over finite fields. *Appl. Algebra Eng. Commun. Comput.*, 13(1) :57–65, 2002. doi : 10.1007/S002000100092. URL <https://doi.org/10.1007/s002000100092>.
- [33] Yingpu Deng. Isomorphism classes of hyperelliptic curves of genus 3 over finite fields. *Finite Fields and Their Applications*, 12(2) :248–282, 2006. ISSN 1071-5797. doi : <https://doi.org/10.1016/j.ffa.2005.05.006>. URL <https://www.sciencedirect.com/science/article/pii/S1071579705000389>.
- [34] J. Cullinan. A remark on the group structure of elliptic curves in towers of finite fields. *New York Journal of Mathematics*, 24 :856–864, 09 2018.
- [35] Clemens Heuberger and Michela Mazzoli. Elliptic curves with isomorphic groups of points over finite field extensions. *Journal of Number Theory*, 181, 05 2016. doi : 10.1016/j.jnt.2017.05.028.
- [36] James McKee. Computing division polynomials. *Mathematics of Computation*, 63 (208) :767–771, 1994. ISSN 00255718, 10886842. URL <http://www.jstor.org/stable/2153297>.
- [37] Fedor Bogomolov and Hang Fu. Division polynomials and intersection of projective torsion points. *European Journal of Mathematics*, 2, 09 2016. doi : 10.1007/s40879-016-0111-7.
- [38] Generalized division polynomials. 94. doi : 10.7146/math.scand.a-14436. URL <https://www.mscaand.dk/article/view/14436>.

- [39] Igor Shparlinski. Orders of points in families of elliptic curves. *Proceedings of the American Mathematical Society*, 148 :1, 10 2019. doi : 10.1090/proc/14901.
- [40] Claus Fieker and Jürgen Klüners. Computation of galois groups of rational polynomials. *LMS J. Comput. Math.*, 17 :141–158, 2012. URL <https://api.semanticscholar.org/CorpusID:119652633>.
- [41] Claus Fieker and Nicole Sutherland. Computing splitting fields using galois theory and other galois constructions. *Journal of Symbolic Computation*, 116 :243–262, 2023. ISSN 0747-7171. doi : <https://doi.org/10.1016/j.jsc.2022.10.001>. URL <https://www.sciencedirect.com/science/article/pii/S0747717122000980>.
- [42] Jean-Marc Couveignes and Reynald Lercier. Fast construction of irreducible polynomials over finite fields (version of 22 apr. *Israel Journal of Mathematics*, 194, 05 2009. doi : 10.1007/s11856-012-0070-8.
- [43] Alp Bassa, Gaetan Bisson, and Roger Oyono. Iterative constructions of irreducible polynomials from isogenies. *Finite Fields Their Appl.*, 97 :102429, 2023. URL <https://api.semanticscholar.org/CorpusID:257038939>.
- [44] Anand Kumar Narayanan. Fast computation of isomorphisms between finite fields using elliptic curves. In Lilya Budaghyan and Francisco Rodríguez-Henríquez, editors, *Arithmetic of Finite Fields*, pages 74–91, Cham, 2018. Springer International Publishing. ISBN 978-3-030-05153-2.
- [45] Ludovic Brielle, Luca Feo, Javad Doliskani, Jean-Pierre Flori, and Éric Schost. Computing isomorphisms and embeddings of finite fields. *Mathematics of Computation*, 88, 05 2017. doi : 10.1090/mcom/3363.
- [46] Jean-Marc Couveignes and Reynald Lercier. Elliptic periods for finite fields. *Finite Fields and Their Applications*, 15(1) :1–22, 2009. ISSN 1071-5797. doi : <https://doi.org/10.1016/j.ffa.2008.07.004>. URL <https://www.sciencedirect.com/science/article/pii/S1071579708000452>.
- [47] Sylvain Duquesne. Finite field arithmetic in large characteristic for classical and post-quantum cryptography. In Sihem Mesnager and Zhengchun Zhou, editors, *Arithmetic of Finite Fields*, pages 79–106, Cham, 2023. Springer International Publishing. ISBN 978-3-031-22944-2.
- [48] *Computing Discrete Logarithms*, page 106–139. London Mathematical Society Lecture Note Series. Cambridge University Press, 2021.

- [49] Yarkin Doröz, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, Berk Sunar, William Whyte, and Zhenfei Zhang. Fully homomorphic encryption from the finite field isomorphism problem. In Michel Abdalla and Ricardo Dahab, editors, *Public-Key Cryptography – PKC 2018*, pages 125–155, Cham, 2018. Springer International Publishing. ISBN 978-3-319-76578-5.
- [50] Bablesh Jhorar and Sudesh K. Khanduja. On power basis of a class of algebraic number fields. *International Journal of Number Theory*, 12(08) :2317–2321, 2016. doi : 10.1142/S1793042116501384. URL <https://doi.org/10.1142/S1793042116501384>.
- [51] Stefano Marseglia. Computing the ideal class monoid of an order. *Journal of the London Mathematical Society*, 101(3) :984–1007, 2020. doi : <https://doi.org/10.1112/jlms.12294>. URL <https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms.12294>.
- [52] Qiang Wu and Zhuo Zhang. On the smallest houses of reciprocal algebraic integers. *Journal of Number Theory*, 177 :170–180, 2017. ISSN 0022-314X. doi : <https://doi.org/10.1016/j.jnt.2017.01.012>. URL <https://www.sciencedirect.com/science/article/pii/S0022314X1730077X>.
- [53] T. ZAIMI, M. J. BERTIN, and A. M. ALJOUIEEE. On number fields without a unit primitive element. *Bulletin of the Australian Mathematical Society*, 93(3) :420–432, 2016. doi : 10.1017/S0004972715001410.
- [54] PIERRE LEZOWSKI. Computation of the euclidean minimum of algebraic number fields. *Mathematics of Computation*, 83(287) :1397–1426, 2014. ISSN 00255718, 10886842. URL <http://www.jstor.org/stable/24488287>.
- [55] Jean-François Biasse, Claus Fieker, Tommy Hofmann, and Aurel Page. Norm relations and computational problems in number fields. *Journal of the London Mathematical Society*, 105(4) :2373–2414, 2022. doi : <https://doi.org/10.1112/jlms.12563>. URL <https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms.12563>.
- [56] Jean-François Biasse and Claus Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS Journal of Computation and Mathematics*, 17(A) :385–403, 2014. doi : 10.1112/S1461157014000345.
- [57] Miguel Bote and Javier Diaz-Vargas. Stru : A variant of ntru over $\mathbb{Z}[\sigma]$. *Advances in Mathematics of Communications*, 01 2024. doi : 10.3934/amc.2024027.
- [58] Monica Nevins, Camelia Karimianpour, and Ali Miri. Ntru over rings beyond F . *Designs, Codes and Cryptography*, 56, 07 2010. doi : 10.1007/s10623-009-9342-7.

- [59] Kazue Sako. *Goldwasser-Micali Encryption Scheme*, pages 516–516. Springer US, Boston, MA, 2011. ISBN 978-1-4419-5906-5. doi : 10.1007/978-1-4419-5906-5_19. URL https://doi.org/10.1007/978-1-4419-5906-5_19.
- [60] Johannes Buchmann, Markus Maurer, and Bodo Moller. Cryptography based on number fields with large regulator. *Journal de theorie des nombres de Bordeaux*, 12(2) : 293–307, 2000. URL http://www.numdam.org/item/JTNB_2000__12_2_293_0/.
- [61] Sylvain Duquesne. Montgomery scalar multiplication for genus 2 curves. In Duncan Buell, editor, *Algorithmic Number Theory*, pages 153–168, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg. ISBN 978-3-540-24847-7.
- [62] Izuru Kitamura, Masanobu Katagi, and Tsuyoshi Takagi. A complete divisor class halving algorithm for hyperelliptic curve cryptosystems of genus two. In Colin Boyd and Juan Manuel González Nieto, editors, *Information Security and Privacy*, pages 146–157, Berlin, Heidelberg, 2005. Springer Berlin Heidelberg. ISBN 978-3-540-31684-8.
- [63] P. Gaudry. Fast genus 2 arithmetic based on theta functions. *Journal of Mathematical Cryptology*, 1(3) :243–265, 2007. doi : doi:10.1515/JMC.2007.012. URL <https://doi.org/10.1515/JMC.2007.012>.
- [64] Chaoping Xing, Huaxiong Wang, and Kwok Lam. Constructions of authentication codes from algebraic curves over finite fields. *Information Theory, IEEE Transactions on*, 46 :886 – 892, 06 2000. doi : 10.1109/18.841168.
- [65] Chaoping Xing. Asymptotic bounds on frameproof codes. *IEEE Transactions on Information Theory*, 48(11) :2991–2995, 2002. doi : 10.1109/TIT.2002.804111.
- [66] Hao Chen, San Ling, Carles Padró, Huaxiong Wang, and Chaoping Xing. Key predistribution schemes and one-time broadcast encryption schemes from algebraic geometry codes. In Matthew G. Parker, editor, *Cryptography and Coding*, pages 263–277, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg. ISBN 978-3-642-10868-6.
- [67] Lihua Liu and Hao Shen. Explicit constructions of separating hash families from algebraic curves over finite fields. *Des. Codes Cryptogr.*, 41(2) :221–233, 2006. doi : 10.1007/S10623-006-9004-Y. URL <https://doi.org/10.1007/s10623-006-9004-y>.
- [68] Huaxiong Wang and Chaoping Xing. Explicit constructions of perfect hash families from algebraic curves over finite fields. *Journal of Combinatorial Theory, Series A*, 93(1) :112–124, 2001. ISSN 0097-3165. doi : <https://doi.org/10.1006/jcta.2000.3068>. URL <https://www.sciencedirect.com/science/article/pii/S0097316500930681>.

- [69] Harald Niederreiter and Chaoping Xing. *1. Finite Fields and Function Fields*, pages 1–29. Princeton University Press, Princeton, 2010. ISBN 9781400831302. doi : doi: 10.1515/9781400831302-002. URL <https://doi.org/10.1515/9781400831302-002>.
- [70] Harald Niederreiter, Huaxiong Wang, and Chaoping Xing. *FUNCTION FIELDS OVER FINITE FIELDS AND THEIR APPLICATIONS TO CRYPTOGRAPHY*, volume 6, pages 59–104. 11 2006. ISBN 978-1-4020-5333-7. doi : 10.1007/1-4020-5334-4_2.
- [71] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic Curves over a Finite Field*. Princeton University Press, stu - student edition edition, 2008. ISBN 9780691096797. URL <http://www.jstor.org/stable/j.ctt1287kdw>.
- [72] Muhammad Sajjad, Tariq Shah, H Alsaud, and Maha Alammari. Designing pair of nonlinear components of a block cipher over quaternion integers. *AIMS Mathematics*, 8 :21089–21105, 07 2023. doi : 10.3934/math.20231074.
- [73] Khadijeh Bagheri, Mohammad-Reza Sadeghi, and Daniel Panario. A non-commutative cryptosystem based on quaternion algebras. *Designs, Codes and Cryptography*, 86, 10 2018. doi : 10.1007/s10623-017-0451-4.
- [74] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology*, 33 : 130 – 175, 2017. URL <https://api.semanticscholar.org/CorpusID:253632688>.
- [75] John Voight. *Quaternion Algebras*. 01 2021. ISBN 978-3-030-56692-0. doi : 10.1007/978-3-030-56694-4.
- [76] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2004. ISBN 9783540204886. URL <https://books.google.cm/books?id=MOW2gEP7HIkC>.
- [77] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.
- [78] Igor R. Shafarevich and Miles Reid. *Basic algebraic geometry 1 (2nd, revised and expanded ed.)*. Springer-Verlag, Berlin, Heidelberg, 1994. ISBN 0387548122.
- [79] David A. Cox, John Little, and Donal O’Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer Publishing Company, Incorporated, 3rd edition, 2010. ISBN 1441922571.

- [80] Daniele Di Tullio and Manoj Gyawali. A post-quantum key exchange protocol from the intersection of quadric surfaces. *J. Supercomput.*, 79(15) :16529–16558, 2023. doi : 10.1007/S11227-023-05146-X. URL <https://doi.org/10.1007/s11227-023-05146-x>.
- [81] Alberto Alzati, Daniele Di Tullio, Manoj Gyawali, and Alfonso Tortora. A post-quantum key exchange protocol from the intersection of conics. *Journal of Symbolic Computation*, 126 :102343, 2025. ISSN 0747-7171. doi : <https://doi.org/10.1016/j.jsc.2024.102343>. URL <https://www.sciencedirect.com/science/article/pii/S0747717124000476>.
- [82] Jean-Pierre Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15 :259–331, 1971. URL <https://api.semanticscholar.org/CorpusID:120153037>.
- [83] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.
- [84] François Morain. Using the charlap-coley-robbins polynomials for computing isogenies, 2023. URL <https://arxiv.org/abs/2303.00346>.
- [85] Masanobu Kaneko and Don Zagier. Supersingular j-invariants, hypergeometric series, and atkin’s orthogonal polynomials. 1998. URL <https://api.semanticscholar.org/CorpusID:124678207>.
- [86] HUGO LABRANDE. Computing jacobi’s theta in quasi-linear time. *Mathematics of Computation*, 87(311) :pp. 1479–1508, 2018. ISSN 00255718, 10886842. URL <https://www.jstor.org/stable/90019421>.
- [87] RÉGIS DUPONT. Fast evaluation of modular functions using newton iterations and the agm. *Mathematics of Computation*, 80(275) :1823–1847, 2011. ISSN 00255718, 10886842. URL <http://www.jstor.org/stable/23075380>.
- [88] Maxim Kazaryan, Sergei Lando, and Victor Prasolov. *Algebraic Curves : Towards Moduli Spaces*. 01 2018. ISBN 978-3-030-02942-5. doi : 10.1007/978-3-030-02943-2.
- [89] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer New York, 2006. ISBN 9780387272269. URL <https://books.google.cm/books?id=EXZCAAAQBAJ>.
- [90] William Stein. Modular forms, a computational approach.
- [91] Joseph H Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics. Springer, 2nd edition, 2009.

- [92] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 1994. ISBN 9780387943282. URL <https://books.google.cm/books?id=dnZOVdo-7BsC>.
- [93] Joachim von zur Gathen. *CryptoSchool*. Springer Publishing Company, Incorporated, 1st edition, 2015. ISBN 3662484234.
- [94] Oded Goldreich. *Foundations of Cryptography*, volume 1. Cambridge University Press, 2001. doi : 10.1017/CBO9780511546891.
- [95] Goldreich Oded. *Foundations of Cryptography : Volume 2, Basic Applications*. Cambridge University Press, USA, 1st edition, 2009. ISBN 052111991X.
- [96] Martin Ekerå. Quantum algorithms for computing general discrete logarithms and orders with tradeoffs. *Journal of Mathematical Cryptology*, 15(1) :359–407, 2021. doi : doi:10.1515/jmc-2020-0006. URL <https://doi.org/10.1515/jmc-2020-0006>.
- [97] Jin-Yi Cai and Ben Young. Quantum algorithms for discrete log require precise rotations. *ACM Transactions on Quantum Computing*, 6(3), June 2025. doi : 10.1145/3736421. URL <https://doi.org/10.1145/3736421>.
- [98] Martin Ekerå and Joel Gärtner. Extending regev’s factoring algorithm to compute discrete logarithms. In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography*, pages 211–242, Cham, 2024. Springer Nature Switzerland. ISBN 978-3-031-62746-0.
- [99] Minki Hhan, Takashi Yamakawa, and Aaram Yun. Quantum complexity for discrete logarithms and related problems. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology – CRYPTO 2024*, pages 3–36, Cham, 2024. Springer Nature Switzerland. ISBN 978-3-031-68391-6.
- [100] Martin Ekerå and Johan Håstad. Quantum algorithms for computing short discrete logarithms and factoring rsa integers. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography*, pages 347–363, Cham, 2017. Springer International Publishing. ISBN 978-3-319-59879-6.
- [101] Martin Ekerå. On post-processing in the quantum algorithm for computing short discrete logarithms. *Des. Codes Cryptography*, 88(11) :2313–2335, November 2020. ISSN 0925-1022. doi : 10.1007/s10623-020-00783-2. URL <https://doi.org/10.1007/s10623-020-00783-2>.

- [102] Javad Doliskani. Toward an optimal quantum algorithm for polynomial factorization over finite fields. *Quantum Info. Comput.*, 19(1–2) :1–13, February 2019. ISSN 1533-7146.
- [103] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016*, pages 559–585, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. ISBN 978-3-662-49896-5.
- [104] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time. *J. ACM*, 68(2), January 2021. ISSN 0004-5411. doi : 10.1145/3431725. URL <https://doi.org/10.1145/3431725>.
- [105] Alice Pellet-Mary, Guillaume Hanrot, and Damien Stehlé. Approx-svp in ideal lattices with pre-processing. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 685–716, Cham, 2019. Springer International Publishing. ISBN 978-3-030-17656-3.
- [106] Changmin Lee, Alice Pellet-Mary, Damien Stehlé, and Alexandre Wallet. An lll algorithm for module lattices. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 59–90, Cham, 2019. Springer International Publishing. ISBN 978-3-030-34621-8.
- [107] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-svp. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology – EUROCRYPT 2017*, pages 324–348, Cham, 2017. Springer International Publishing. ISBN 978-3-319-56620-7.
- [108] Jean-François Biasse and Fang Song. On the quantum attacks against schemes relying on the hardness of finding a short generator of an ideal in *Journal of Mathematical Cryptology*, 13(3-4) :151–168, 2019. doi : doi:10.1515/jmc-2015-0046. URL <https://doi.org/10.1515/jmc-2015-0046>.
- [109] Jean-François Biasse and Fang Song. *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, pages 893–902. doi : 10.1137/1.9781611974331.ch64. URL <https://epubs.siam.org/doi/abs/10.1137/1.9781611974331.ch64>.
- [110] Sean Hallgren. Fast quantum algorithms for computing the unit group and class group of a number field. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on*

- Theory of Computing*, STOC '05, page 468–474, New York, NY, USA, 2005. Association for Computing Machinery. ISBN 1581139608. doi : 10.1145/1060590.1060660. URL <https://doi.org/10.1145/1060590.1060660>.
- [111] Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev, and Fang Song. A quantum algorithm for computing the unit group of an arbitrary degree number field. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '14, page 293–302, New York, NY, USA, 2014. Association for Computing Machinery. ISBN 9781450327107. doi : 10.1145/2591796.2591860. URL <https://doi.org/10.1145/2591796.2591860>.
 - [112] Yan Huang, Zhaofeng Su, Fangguo Zhang, Yong Ding, and Rong Cheng. Quantum algorithm for solving hyperelliptic curve discrete logarithm problem. *Quantum Information Processing*, 19(2), January 2020. ISSN 1570-0755. doi : 10.1007/s11128-019-2562-5. URL <https://doi.org/10.1007/s11128-019-2562-5>.
 - [113] Chao Chen, Peidong Guan, Yan Huang, and Fangguo Zhang. Quantum circuits for hyperelliptic curve discrete logarithms over the mersenne prime fields. *Quantum Information Processing*, 22, 07 2023. doi : 10.1007/s11128-023-04017-x.
 - [114] Thomas Häner, Samuel Jaques, Michael Naehrig, Martin Roetteler, and Mathias Soeken. Improved quantum circuits for elliptic curve discrete logarithms. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 425–444, Cham, 2020. Springer International Publishing. ISBN 978-3-030-44223-1.
 - [115] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on sidh. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 448–471, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-30589-4.
 - [116] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023. doi : 10.1007/978-3-031-30589-4_16. URL https://doi.org/10.1007/978-3-031-30589-4_16.
 - [117] Emanuele Bellini, Jorge Chavez-Saab, Jesús-Javier Chi-Domínguez, Andre Esser, Sorina Ionica, Luis Rivera-Zamarripa, Francisco Rodríguez-Henríquez, Monika Trimoska, and Floyd Zweydinger. Parallel isogeny path finding with limited memory. In Takanori

- Isobe and Santanu Sarkar, editors, *Progress in Cryptology – INDOCRYPT 2022*, pages 294–316, Cham, 2022. Springer International Publishing. ISBN 978-3-031-22912-1.
- [118] Yasuhiko Ikematsu, Ryoya Fukasaku, Momonari Kudo, Masaya Yasuda, Katsuyuki Takashima, and Kazuhiro Yokoyama. Hybrid meet-in-the-middle attacks for the isogeny path-finding problem. *Proceedings of the 7th ACM Workshop on ASIA Public-Key Cryptography*, 2020.
- [119] Yasushi Takahashi, Momonari Kudo, Ryoya Fukasaku, Yasuhiko Ikematsu, Masaya Yasuda, and Kazuhiro Yokoyama. Algebraic approaches for solving isogeny problems of prime power degrees. *Journal of Mathematical Cryptology*, 15 :31 – 44, 2020.
- [120] Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 345–371, Cham, 2022. Springer International Publishing. ISBN 978-3-031-07082-2.
- [121] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2021.
- [122] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016*, pages 63–91, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. ISBN 978-3-662-53887-6.
- [123] Tako Boris Fouotsa and Christophe Petit. A new adaptive attack on sidh. In Steven D. Galbraith, editor, *Topics in Cryptology – CT-RSA 2022*, pages 322–344, Cham, 2022. Springer International Publishing. ISBN 978-3-030-95312-6.
- [124] Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Charlotte Weitkämper. One-way functions and malleability oracles : Hidden shift attacks on isogeny-based protocols. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 242–271, Cham, 2021. Springer International Publishing. ISBN 978-3-030-77870-5.
- [125] Samuel Dobson, Steven D. Galbraith, Jason T. LeGrow, Yan Bo Ti, and Lukas Zobernig. An adaptive attack on 2-sidh. *International Journal of Computer Mathematics : Computer Systems Theory*, 6 :387 – 404, 2021.
- [126] Péter Kutas and Christophe Petit. Torsion point attacks on "sidh-like" cryptosystems. *IET Inf. Secur.*, 17 :161–170, 2022.

- [127] Andrea Basso and Fabien Pazuki. On the supersingular gpst attack. *Journal of Mathematical Cryptology*, 16 :14 – 19, 2019.
- [128] Tako Boris Fouotsa, Péter Kutas, Simon-Philipp Merz, and Yan Bo Ti. On the isogeny problem with torsion point information. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 142–161, Cham, 2022. Springer International Publishing. ISBN 978-3-030-97121-2.
- [129] Reza Azarderakhsh, Jean-François Biasse, Rami El Khatib, Brandon Langenberg, and Benjamin Pring. Parallelism strategies for the tuneable golden-claw finding problem. *International Journal of Computer Mathematics : Computer Systems Theory*, 6 :337 – 363, 2021.
- [130] Gora Adj, Jes’us-Javier Chi-Dom’inguez, Víctor Mateu, and Francisco Rodr’iguez-Henr’iquez. Faulty isogenies : a new kind of leakage. *IACR Cryptol. ePrint Arch.*, 2022 :153, 2022.
- [131] Guanju Xiao, Lixia Luo, and Yingpu Deng. Constructing cycles in isogeny graphs of supersingular elliptic curves. *Journal of Mathematical Cryptology*, 15(1) :454–464, 2021. doi : doi:10.1515/jmc-2020-0029. URL <https://doi.org/10.1515/jmc-2020-0029>.
- [132] Wissam Ghantous. Loops, multi-edges and collisions in supersingular isogeny graphs. *Advances in Mathematics of Communications*, 2021.
- [133] Jean-François Biasse, Annamaria Iezzi, and Michael J. Jacobson. A note on the security of csidh. In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology – INDOCRYPT 2018*, pages 153–168, Cham, 2018. Springer International Publishing. ISBN 978-3-030-05378-9.
- [134] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the csidh : Optimizing quantum evaluation of isogenies. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 409–441, Cham, 2019. Springer International Publishing. ISBN 978-3-030-17656-3.
- [135] David Jao, Jason T. LeGrow, Christopher Leonardi, and Luis Ruiz-Lopez. A subexponential-time, polynomial quantum space algorithm for inverting the cm group action. *Journal of Mathematical Cryptology*, 14 :129 – 138, 2020.
- [136] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of csidh. *Advances in Cryptology – EUROCRYPT 2020*, 12106 :493 – 522, 2020.