Chapitre un

Early career development Research Project

Name : Dr. Fouazou Lontouo Perez Broon Ph.D
Duration : Five years
Email : fouazouperez@gmail.com
Title : Mathematical Cryptology, Abelian Varieties, Computational Number Theory and Geometry

The aims of this project is to carry out research activities for scientific publications in the fields of "number theory, abelian varieties, computation of the isogenies and application in cryptology". For this, I will also carry out training activities in order to deepen my research capabilities. More precisely, I selected some research areas "algebraic number theory, algebraic curve, fields theory, modular forms, quaternion algebra, algebraic geometry and some advanced topics in elliptic curve" on which I will design learning materials for graduate and postgraduate courses and contemporary courses (course based on some recent research papers on a given research topic). In fact, by designing these materials, I will collect useful tools for research and deepen my research capacities. In this research project, I also propose some research topics directly connected to previous themes and recent papers on these topics for contemporary courses. The main outcomes of these training activities will be the design of contemporary courses, design of materials for graduate and postgraduate learning/teaching and research direction for publications.

This research project also gathers some applications of the areas "algebraic number theory, algebraic curve, field theory, quaternion algebra and algebraic geometry " in cryptography. These applications will be used for the part of this project devoted to design and proofs of security in cryptography, more precisely contemporary courses will be designed on these applications and I will also address research questions on these applications.

This project also involves training activities on hardware programming, performant software programming and quantum computing for cryptography and computational aspect of number theory and geometry, for which the algorithms from number theory will serve as examples.

Apart the training activities and the professional developments of this project, the main objective of this project is research on "abelian varieties, computation of isogenies and application in post-

quantum cryptography" some research directions are given on these subjects with contemporary courses to design on current issues and the latest advances.

Table des matières

1.1 Selected Thematics for Training Activities With Some Related Research Topics

1.1.1 Fields Theory

Here I will address research topics related to fields theory such that : computing Galois group of polynomials [1, 2], computation of irreducible polynomials over finite fields using elliptic curves

[3, 4], computation of an isomorphism between finite fields using elliptic curves [5, 6], use of elliptic curves to construct basis for efficient arithmetic on extension of finite fields [7].

I will also address research topics related to application of fields theory in cryptography such that : efficient arithmetic of finite fields for cryptography [8], discrete logarithm problem over finite fields and application in cryptography [9] and homomorphic encryption from the finite fields isomorphism problem [10]. 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.

1.1.2 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 [11], computing the monoid of the ideals class of the orders in number fields or more generally an étale algebra [12], study of Pisot numbers and reciprocal algebraic integers [13], [14], computation of the euclidean minimum of number fields and norm-euclidean fields [15], computation of class group and unit group [16, 17].

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 [18, 19], public key cryptosystem based on quadratic residuosity problem [20], design of public key crypto-system which security repose on principal ideal problem (PIP) [21]. 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.

1.1.3 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 [22–24] and computation of isogenies between Jacobean of high genus curves [25–28]

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 [29], asymptotic lower bound of frameproof codes obtained from algebraic-geometry codes [30], key pre-distribution Schemes and one-time broadcast encryption schemes from algebraic curve [31], construction of separating,cover-free and perfect hash families [32, 33]. These applications are covered in the following books [34, 35].

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 [36] will be the first reference used for these learning materials and research topics following by selection of other research papers).

1.1.4 Quaternion Algebras

The quaternion algebras is used to design crypto-system such that : the block cipher [37], the variants of NTRU in which $\mathbb{Z}$ is replaced by the quaternion algebras over finite fields [38], PKC and signature with endomorphism ring of super-singular elliptic curves [39].

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 [40] will be the main reference used for these learning materials and research topics before selection of other research papers)

1.1.5 Abelian Varieties

Here I will first design learning materials for graduate course on complex abelian varieties and abelian varieties over finite fields [41, 42]. 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.

1.1.6 Computational and Effective aspects of Algebraic Geometry

Here I will study some useful algorithms and effective aspects of algebraic geometry, the books [43, 44] 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 [45, 46]

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

1.1.7 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 [47, 48], in the application of the modular forms the point counting algorithm [49, 50], in computation of polynomials whose super-singular j-invariants are the roots [51] and computation of the Jacobi, Debekind, Theta function with other modular polynomials [52–54]. After moduli spaces of elliptic

curves we will also carry out training activities on the moduli spaces of algebraic curves and abelian varieties [55].

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 [56, 57] (a primary syllabus is given in section 1.5.4).

1.1.8 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 [58] and CM elliptic curves [59].

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

1.2 Programming, Design and Security Proving in Cryptography

1.2.1 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 :

[60]

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 [61] and [62]

1.2.2 Programming and Quantum Algorithm

In this part of the project we will :

1. 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

2. study the quantum algorithm and their using to solve the computational assumptions on which repose the security of public key crypto-system
`https://doi.org/10.1049/ise2.12081`
`https://doi.org/10.1145/3517340`
Renato Portugal *Basic quantum algorithms* arxiv 2023

1.3 Some Current Research Question 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 : [63], [64] and [65]
— 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 [66–71] constant time implementation [66, 72, 73], library [74–77] and parallel implementation [78]
   (b) Other CSIDH like crypto-system : with CSIDH setting and class group action many post-quantum secure cryptographic primitives can be designed such that [76, 79, 79, 80, 80–82, 82–84]
— 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 [85, 86] the idea underlying the Castriyck and Decru attack can be also used constructively in [87], [88].
   (b) on the implementation : SIDH implementation [89, 90], on implementation of CGL Hash Function [91–93, 93, 94]
   (c) other SIDH like crypto-system : pseudo-random functions [95, 96], digital signature [88, 97], PAKE [98], VDF [99], [100] and public key encryption [101].

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 [102–105]
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.
   — [106], [107], [108],[109], [110], [111], [111], [112], [113]
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 : [64] and [114]
   — on the cryptanalysis of the CSIDH like crypto-system :
      — vulnerability under hardware implementation and countermeasure [115], [116],[117], [118],[117], [119]
      — quantum and classical algorithm to solve the related computational assumption [120], [121], [122], [123],[124], [125]
   — on the cryptanalysis of the SIDH like crypto-system : full key recover [126, 127], algorithm for path finding problem [128–130], compute the endomorphism ring of super-singular elliptic curve [64, 100, 131], torsion point attack [132–137], Quantum attack [138] , [139] and cycle in isogenies graph [140, 141].

   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.

1.4 Some open questions

1. **Algebraic relations satisfying by the representations of the isogenies of prime power degree :** In [142] we give some algebraic relations $\{f_i(\sigma_1, \sigma_2, ..., \sigma_n) = 0\}_{i \in I}$ satisfied by the kernel polynomials $D = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - ...\sigma_n$ which can be used directly to compute the kernel polynomials (by solving the multivariate polynomials system $f_i = 0$). In the cryptographic context, the kernel polynomials have many coefficients (e.g ℓ^n in the

SIDH case) and it would be interesting in these cases to find algebraic relations by using rather the compact representations of these types of isogenies which exist in the literature (for example a path in the graph of isogenies $j_1, j_2, ..., j_n$.) Here we want also to use these algebraic relations to find the circles in the isogenies graph. Contrary to the Schoof's relations (who give some relations between the coefficients σ_i) our algebraic relations can be apply in the case of field of small characteristic.

2. **Algebraic approach to solve the path finding problem in the graph of super-singular 2-isogenies :** In [130] two algebraic approaches to solve the path finding problem in the super-singular ℓ-isogenies graph (with ℓ odd) are given. Our goal here is to research the algebraic approaches in the case of the graph of 2-isogeny. More precisely, their second approach uses the Schoof's relations which concern only the odd isogenies, find analog of Schoof's relations in the case of cyclic isogenies of two power degree and use them in the path finding problem. Also they use the odd modular polynomial ($\phi_\ell(j_i, j_{i+1})$ with ℓ odd) in their first approach to find in path between two j-invariant j_1 and j_n, by solving the multivariate polynomial system $\{\phi_\ell(j_i, j_{i+1}) = 0\}_{i=1}^{i=n-1}$. Here we will also search an algebraic approach in the case of graph of 2-isogeny for example by using the radical 2-isogenies.
3. **On the isogeny/isomorphism class of super-singular elliptic curve**
   Here we want to solve the two following questions on the isogenies class of super-singular curves
   (a) search a model of curve for the super-singular elliptic curve in characteristic $p = 1 mod(4)$ see the end of section 1 of [143] (see also section 3.2 of [143] and prop 8 of [144] for the sub-case $p = 7 mod(8)$ and $p = 3 mod(8)$ respectively).
   (b) In [145] a conjecture on the number of super-singular Hessian $H_d : x^3 + y^3 + 1 = dxy$ elliptic curve defined over $\mathbb{F}_{p^2}$ is given in the case $p = 2 mod(3)$

   $$h * j \text{ where } h \text{ is the class number of } \mathbb{Q}(\sqrt{-q}) \text{ and } j = 1, 2 \text{ or } 4$$

   here we want to prove this conjecture.
   Also the question of finding a relation between $N(A)$ and $N(-A)$ is posed , where $N(t)$ is the number of Hessian curve of trace t.
4. Unlike curves of genus 1 curve which admit a model up to K-isomorphism (the Weierstrass model). High genus curve ($g > 1$) have several models. Here we want to apply the existing algorithms to compute the isogenies between abelian varieties (or high genus curve) to specific curve models, get explicit formulas on these models and see if this gives us a significant improvement or search more efficient algorithms/formulas to compute explicitly the isogenies on these curve models.

1.5 Syllabus of Some Course to Generate Learning Materials at Graduate Level

1.5.1 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 $m_x : L \longrightarrow L, \quad m_x(y) = x * y$. 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 $Gal(\mathbb{K}/k)$, 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*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 Frobenus map $Fr_q(x) = x^q$.
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.
— irreduciblity 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 $d = \sqrt{disc(P)}$ 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.

1.5.2 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 $\mathbb{Z} = \mathbb{Q} \bigcap \bar{\mathbb{Z}}$. 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 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 $\{1, ..., \frac{p-1}{2}\}$.
— 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 $m * x \in \mathcal{O}_{\mathbb{K}}$ 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 $irr_{\mathbb{Q}}(x)$ 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.

1.5.3 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 $F = O, G = 0$ 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 birationel (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 $y = c_1 t + c_2 t^2$..... 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 $ord(\eta(t)) \geqslant n$. 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 $card(\mathcal{C}(\mathbb{F}_{q^i}))$ $i \in \{1, ..., g\}$ is equivalent to the knowing of the coefficient of Zeta function and enable to compute the carnality of the curve aver any other extension of $\mathbb{F}_q$ (by functional equation of Zeta function).

— Definition of the irreducible divisors $D = P + P^\sigma + ... + P^{\sigma^n}$ (where $\sigma : x \longmapsto x^q$, $P \in \mathcal{C}(\mathbb{F}_{q^n})$ 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 $card(Pic^n(\mathcal{C})(\mathbb{F}_q))$ is finite and $card(Pic^n(\mathcal{C})(\mathbb{F}_q)) = card(Pic^0(\mathcal{C})(\mathbb{F}_q))$. 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 $c \longmapsto K_{\mathcal{C}} - c$ 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.

1.5.4 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). Cups 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 cups 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] 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`.

[2] 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`.

[3] 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.

[4] 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`.

[5] 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.

[6] Ludovic Brieulle, 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.

[7] 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`.

[8] 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.

[9] *Computing Discrete Logarithms*, page 106–139. London Mathematical Society Lecture Note Series. Cambridge University Press, 2021.

[10] Yarkın 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.

[11] 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`.

[12] 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`.

[13] 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`.

[14] T. ZAIMI, M. J. BERTIN, and A. M. ALJOUIEE. On number fields without a unit primitive element. *Bulletin of the Australian Mathematical Society*, 93(3) :420–432, 2016. doi : 10.1017/S0004972715001410.

[15] 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`.

[16] 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`.

[17] 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.

[18] 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.

[19] 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.

[20] 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`.

[21] 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/`.

[22] 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.

[23] 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.

[24] 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`.

[25] 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`.

[26] 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.

[27] 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.

[28] 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`.

[29] 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.

[30] Chaoping Xing. Asymptotic bounds on frameproof codes. *IEEE Transactions on Information Theory*, 48(11) :2991–2995, 2002. doi : 10.1109/TIT.2002.804111.

[31] 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.

[32] 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`.

[33] 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`.

[34] 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`.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] John Voight. *Quaternion Algebras*. 01 2021. ISBN 978-3-030-56692-0. doi : 10.1007/978-3-030-56694-4.

[41] 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.

[42] James S. Milne. Abelian varieties (v2.00), 2008. Available at www.jmilne.org/math/.

[43] Igor R. Shafarevich and Miles Reid. *Basic algebraic geometry 1 (2nd, revised and expanded ed.)*. Springer-Verlag, Berlin, Heidelberg, 1994. ISBN 0387548122.

[44] 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.

[45] 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.

[46] 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.

[47] 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.

[48] 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`.

[49] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1999.

[50] François Morain. Using the charlap-coley-robbins polynomials for computing isogenies, 2023. URL `https://arxiv.org/abs/2303.00346`.

[51] Masanobu Kaneko and Don Zagier. Supersingular j-invariants, hypergeometric series, and atkin's orthogonal polynomials. 1998. URL `https://api.semanticscholar.org/CorpusID:124678207`.

[52] 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`.

[53] 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`.

[54] François Morain. Computing the charlap-coley-robbins modular polynomials, 2023. URL `https://arxiv.org/abs/2302.05217`.

[55] 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.

[56] 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=EXZCAAAAQBAJ`.

[57] William Stein. Modular forms, a computational approach.

[58] Joseph H Silverman. *The arithmetic of elliptic curves*. Graduate Texts in Mathematics. Springer, 2nd edition, 2009.

[59] 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=dnZ0Vdo-7BsC`.

[60] Joachim von zur Gathen. *CryptoSchool*. Springer Publishing Company, Incorporated, 1st edition, 2015. ISBN 3662484234.

[61] Oded Goldreich. *Foundations of Cryptography*, volume 1. Cambridge University Press, 2001. doi : 10.1017/CBO9780511546891.

[62] Goldreich Oded. *Foundations of Cryptography : Volume 2, Basic Applications*. Cambridge University Press, USA, 1st edition, 2009. ISBN 052111991X.

[63] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *J. Math. Cryptol.*, 14(1) :414–437, 2020. doi : 10.1515/jmc-2019-0034. URL `https://doi.org/10.1515/jmc-2019-0034`.

[64] 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.

[65] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields Their Appl.*, 69 :101777, 2020.

[66] Michael Meyer and Steffen Reith. A faster way to the csidh. In Debrup Chakraborty and Tetsu Iwata, editors, *Progress in Cryptology – INDOCRYPT 2018*, pages 137–152, Cham, 2018. Springer International Publishing. ISBN 978-3-030-05378-9.

[67] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 493–519. Springer, 2020.

[68] Daniel Bernstein, Luca Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *Open Book Series*, 4 :39–55, 12 2020. doi : 10.2140/obs.2020.4.39.

[69] Wouter Castryck, Thomas Decru, Marc Houben, and Frederik Vercauteren. Horizontal racewalking using radical isogenies. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 67–96, Cham, 2022. Springer Nature Switzerland. ISBN 978-3-031-22966-4.

[70] Gustavo Banegas, Valerie Gilchrist, Anaëlle Le Dévéhat, and Benjamin Smith. Fast and frobenius : Rational isogeny evaluation over finite fields. *CoRR*, abs/2306.16072, 2023. doi : 10.48550/arXiv.2306.16072. URL `https://doi.org/10.48550/arXiv.2306.16072`.

[71] Hiroshi Onuki and Tomoki Moriya. Radical isogenies on montgomery curves. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 473–497, Cham, 2022. Springer International Publishing. ISBN 978-3-030-97121-2.

[72] Kohei Nakagawa, Hiroshi Onuki, Atsushi Takayasu, and Tsuyoshi Takagi. L1-norm ball for csidh : Optimal strategy for choosing the secret key space. *Discret. Appl. Math.*, 328 :70–88, 2020.

[73] Hiroshi Onuki, Yusuke Aikawa, Tsutomu Yamazaki, and Tsuyoshi Takagi. A constant-time algorithm of csidh keeping two points. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 103-A :1174–1182, 2020.

[74] Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez. Karatsuba-based square-root vélu's formulas applied to two isogeny-based protocols. *Journal of Cryptographic Engineering*, 13 :89–106, 2022.

[75] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The sqale of csidh : sublinear vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12 :349–368, 2021.

[76] Robi Pedersen. Decsidh : Delegating isogeny computations in the csidh setting. In Avishek Adhikari, Ralf Küsters, and Bart Preneel, editors, *Progress in Cryptology – INDOCRYPT 2021*, pages 337–361, Cham, 2021. Springer International Publishing. ISBN 978-3-030-92518-5.

[77] Amir Jalali, Reza Azarderakhsh, Mehran Mozaffari Kermani, and David Jao. Towards optimized and constant-time csidh on embedded devices. In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, 2019.

[78] Ganma Kato and Koutarou Suzuki. Speeding up csidh using parallel computation of isogeny. *2020 7th International Conference on Advance Informatics : Concepts, Theory and Applications (ICAICTA)*, pages 1–6, 2020.

[79] Luca De Feo and Steven D. Galbraith. Seasign : Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2019*, pages 759–789, Cham, 2019. Springer International Publishing. ISBN 978-3-030-17659-4.

[80] Luca De Feo and Michael Meyer. Threshold schemes from isogeny assumptions. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-*

Key Cryptography – PKC 2020, pages 187–212, Cham, 2020. Springer International Publishing. ISBN 978-3-030-45388-6.

[81] Michel Abdalla, Thorsten Eisenhofer, Eike Kiltz, Sabrina Kunzweiler, and Doreen Riepel. Password-authenticated key exchange from group actions. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*, pages 699–728, Cham, 2022. Springer Nature Switzerland. ISBN 978-3-031-15979-4.

[82] Saikrishna Badrinarayanan, Daniel Masny, Pratyay Mukherjee, Sikhar Patranabis, Srinivasan Raghuraman, and Pratik Sarkar. Round-optimal oblivious transfer and mpc from computational csidh. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *Public-Key Cryptography – PKC 2023*, pages 376–405, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-31368-4.

[83] Tako Boris Fouotsa and Christophe Petit. Sims : A simplification of sigamal. In *Post-Quantum Cryptography*, 2021.

[84] Kunal Dey, Sumit Kumar Debnath, Pantelimon Stănică, and Vikas Srivastava. A post-quantum signcryption scheme using isogeny based cryptography. *Journal of Information Security and Applications*, 69 :103280, 2022. ISSN 2214-2126. doi : https://doi.org/10.1016/j.jisa.2022.103280. URL `https://www.sciencedirect.com/science/article/pii/S2214212622001387`.

[85] Tako Boris Fouotsa, Tomoki Moriya, and Christophe Petit. M-sidh and md-sidh : Countering sidh attacks by masking information. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 282–309, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-30589-4.

[86] Andrea Basso and Tako Boris Fouotsa. New SIDH countermeasures for a more efficient key exchange. *IACR Cryptol. ePrint Arch.*, page 791, 2023. URL `https://eprint.iacr.org/2023/791`.

[87] Andrea Basso, Luciano Maino, and Giacomo Pope. FESTA : fast encryption from supersingular torsion attacks. *IACR Cryptol. ePrint Arch.*, page 660, 2023. URL `https://eprint.iacr.org/2023/660`.

[88] Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. Sqisignhd : New dimensions in cryptography. *IACR Cryptol. ePrint Arch.*, 2023 :436, 2023.

[89] Craig Costello, Patrick Longa, and Michael Naehrig. Efficient algorithms for supersingular isogeny diffie-hellman. In Matthew Robshaw and Jonathan Katz, editors,

Advances in Cryptology – CRYPTO 2016, pages 572–601, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. ISBN 978-3-662-53018-4.

[90] Jesse Elliott and Aaron Hutchinson. Supersingular isogeny diffie-hellman with legendre form. *IACR Cryptol. ePrint Arch.*, page 870, 2022. URL `https://eprint.iacr.org/2022/870`.

[91] Hikari Tachibana, Katsuyuki Takashima, and Tsuyoshi Takagi. Constructing an efficient hash function from 3-isogenies. *JSIAM Letters*, 9 :29–32, 2017. doi : 10.14495/jsiaml.9.29.

[92] Yuji HASHIMOTO and Koji NUIDA. Efficient construction of cgl hash function using legendre curves. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, advpub :2022DMP0003, 2023. doi : 10.1587/transfun.2022DMP0003.

[93] Reo YOSHIDA and Katsuyuki TAKASHIMA. Computing a sequence of 2-isogenies on supersingular elliptic curves. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E96.A(1) :158–165, 2013. doi : 10.1587/transfun.E96.A.158.

[94] Miraz Uz Zaman, Aaron Hutchinson, and Manki Min. Implementation aspects of supersingular isogeny-based cryptographic hash function. In Zygmunt J. Haas, Ravi Prakash, Habib Ammari, and Weili Wu, editors, *Wireless Internet - 15th EAI International Conference, WiCON 2022, Virtual Event, November 2022, Proceedings*, volume 464 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 14–27. Springer, 2022. doi : 10.1007/978-3-031-27041-3_2. URL `https://doi.org/10.1007/978-3-031-27041-3_2`.

[95] Dan Boneh, Dmitry Kogan, and Katharine Woo. Oblivious pseudorandom functions from isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 520–550, Cham, 2020. Springer International Publishing. ISBN 978-3-030-64834-3.

[96] Andrea Basso. Poster : A post-quantum oblivious prf from isogenies. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, 2022.

[97] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign : Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing. ISBN 978-3-030-64837-4.

[98] Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T. LeGrow. Towards isogeny-based password-authenticated key establishment. *Journal of Mathematical Cryptology*, 15 :18 – 30, 2020.

[99] Jorge Chavez-Saab, Francisco Rodríguez-Henríquez, and Mehdi Tibouchi. Verifiable isogeny walks : Towards an isogeny-based postquantum vdf. In Riham AlTawy and Andreas Hülsing, editors, *Selected Areas in Cryptography*, pages 441–460, Cham, 2022. Springer International Publishing. ISBN 978-3-030-99277-4.

[100] 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.

[101] Luca De Feo, Cyprien Delpech de Saint Guilhem, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski. Séta : Supersingular encryption from torsion attacks. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2021*, pages 249–278, Cham, 2021. Springer International Publishing. ISBN 978-3-030-92068-5.

[102] Jeffrey Burdges and Luca De Feo. Delay encryption. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology – EUROCRYPT 2021*, pages 302–326, Cham, 2021. Springer International Publishing. ISBN 978-3-030-77870-5.

[103] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 248–277, Cham, 2019. Springer International Publishing. ISBN 978-3-030-34578-5.

[104] Péter Kutas, Christophe Petit, and Javier Silva. Trapdoor ddh groups from pairings and isogenies. In Orr Dunkelman, Michael J. Jacobson, Jr., and Colin O'Flynn, editors, *Selected Areas in Cryptography*, pages 431–450, Cham, 2021. Springer International Publishing. ISBN 978-3-030-81652-0.

[105] Takeshi Koshiba and Katsuyuki Takashima. New assumptions on isogenous pairing groups with applications to attribute-based encryption. In *International Conference on Information Security and Cryptology*, 2018.

[106] 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.

[107] 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.

[108] Elie Eid. Fast computation of hyperelliptic curve isogenies in odd characteristic. *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*, 2020.

[109] Ramsès Fernàndez-València. Undeniable signatures based on isogenies of supersingular hyperelliptic curves. *ArXiv*, abs/1908.07458, 2019.

[110] 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.

[111] Toshiyuki Katsura and Katsuyuki Takashima. Counting richelot isogenies between superspecial abelian surfaces. *Open Book Series*, 2020.

[112] 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.

[113] E. V. Flynn and Yan Bo Ti. Genus two isogeny cryptography. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*, pages 286–306, Cham, 2019. Springer International Publishing. ISBN 978-3-030-25510-7.

[114] Pierrick Dartois and Luca De Feo. On the security of osidh. In Goichiro Hanaoka, Junji Shikata, and Yohei Watanabe, editors, *Public-Key Cryptography – PKC 2022*, pages 52–81, Cham, 2022. Springer International Publishing. ISBN 978-3-030-97121-2.

[115] Fabio Campos, Juliane Krämer, and Marcel Müller. *Safe-Error Attacks On SIKE And CSIDH*, page 104–125. Springer-Verlag, Berlin, Heidelberg, 2021. ISBN 978-3-030-95084-2. URL `https://doi.org/10.1007/978-3-030-95085-9_6`.

[116] Fabio Campos, Matthias J. Kannwischer, Michael Meyer, Hiroshi Onuki, and Marc Stöttinger. Trouble at the csidh : Protecting csidh with dummy-operations against fault injection attacks. *2020 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)*, pages 57–65, 2020.

[117] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for csidh. In Peter Schwabe and Nicolas Thériault, editors, *Progress in Cryptology – LATINCRYPT 2019*, pages 173–193, Cham, 2019. Springer International Publishing. ISBN 978-3-030-30530-7.

[118] 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 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part II*, volume 11477 of *Lecture Notes in Computer Science*, pages 409–441. Springer, 2019. doi : 10.1007/978-3-030-17656-3_15. URL `https://doi.org/10.1007/978-3-030-17656-3_15`.

[119] Gustavo Banegas, Juliane Kramer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotakova, and Monika Trimoska. Disorientation faults in csidh. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology – EUROCRYPT 2023*, pages 310–342, Cham, 2023. Springer Nature Switzerland. ISBN 978-3-031-30589-4.

[120] 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.

[121] 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.

[122] 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.

[123] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of csidh. *Advances in Cryptology – EUROCRYPT 2020*, 12106 :493 – 522, 2020.

[124] Jean-François Biasse, Xavier Bonnetain, Benjamin Pring, André Schrottenloher, and William Jay Youmans. A trade-off between classical and quantum circuit size for an attack against csidh. *Journal of Mathematical Cryptology*, 15 :4 – 17, 2020.

[125] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 523–548, Cham, 2020. Springer International Publishing. ISBN 978-3-030-45724-2.

[126] 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.

[127] 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`.

[128] 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.

[129] 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.

[130] 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.

[131] 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.

[132] 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.

[133] 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.

[134] 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.

[135] Péter Kutas and Christophe Petit. Torsion point attacks on "sidh-like" cryptosystems. *IET Inf. Secur.*, 17 :161–170, 2022.

[136] Andrea Basso and Fabien Pazuki. On the supersingular gpst attack. *Journal of Mathematical Cryptology*, 16 :14 – 19, 2019.

[137] 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.

[138] 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.

[139] 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.

[140] 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`.

[141] Wissam Ghantous. Loops, multi-edges and collisions in supersingular isogeny graphs. *Advances in Mathematics of Communications*, 2021.

[142] Fouazou Lontouo Perez Broon. Multiplicative vélu's formula, computation of the kernel polynomials and some applications. *submited to "Mathematic of Computation"*, (PREPRINT), Feb-Ma 2023.

[143] Wouter Castryck and Thomas Decru. Csidh on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 111–129, Cham, 2020. Springer International Publishing. ISBN 978-3-030-44223-1.

[144] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH : an efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[145] Dustin Moody and Hongfeng Wu. Families of elliptic curves with rational 3-torsion. *J. Math. Cryptol.*, 5(3-4) :225–246, 2012. doi : 10.1515/jmc-2011-0013. URL `https://doi.org/10.1515/jmc-2011-0013`.

[146] J. S. Milne. *Fields and Galois Theory*. Kea Books, Ann Arbor, MI, 2022.

[147] Daniele Di Tullio and Manoj Gyawali. A post-quantum signature scheme from the secant variety of the grassmannian. *Iran J. Comput. Sci.*, 6(4) :431–443, 2023. doi : 10.1007/S42044-023-00150-Z. URL `https://doi.org/10.1007/s42044-023-00150-z`.

[148] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion -isogeny path problem. *LMS Journal of Computation and Mathematics*, 17, 06 2014. doi : 10.1112/S1461157014000151.

[149] René SCHOOF. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1) :219–254, 1995. ISSN 12467405, 21188572. URL `http://www.jstor.org/stable/43972442`.

[150] J.-F. Biasse, X. Bonnetain, E. Kirshanova, A. Schrottenloher, and F. Song. Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. *IET Information Security*, 17(2) :171–209, 2023. doi : https://doi.org/10.1049/ise2.12081. URL `https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/ise2.12081`.

[151] Bruno Sterner. Commitment schemes from supersingular elliptic curve isogeny graphs. *IACR Cryptol. ePrint Arch.*, 2021 :1031, 2021.

[152] Reza Azarderakhsh, David Jao, Brian Koziel, Jason T. LeGrow, Vladimir Soukharev, and Oleg Taraskin. How not to create an isogeny-based pake. In *Applied Cryptography and Network Security : 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part I*, page 169–186, Berlin, Heidelberg, 2020.

Springer-Verlag. ISBN 978-3-030-57807-7. doi : 10.1007/978-3-030-57808-4_9. URL https://doi.org/10.1007/978-3-030-57808-4_9.

[153] Tom Fisher. The hessian of a genus one curve. *Proceedings of the London Mathematical Society*, 104(3) :613–648, 2012. doi : https://doi.org/10.1112/plms/pdr039. URL https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/plms/pdr039.

[154] Michela Artebani and Igor Dolgachev. The hesse pencil of plane cubic curves. *L'Enseign Math*, 55, 12 2006. doi : 10.4171/LEM/55-3-3.

[155] Fouazou Lontouo Perez Broon, Fouotsa Emmanuel, and Daniel Tieudjo. Division polynomials on the hessian model of elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–16, 11 2020. doi : 10.1007/s00200-020-00470-8.

[156] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170) :483–494, 1985. ISSN 00255718, 10886842. URL http://www.jstor.org/stable/2007968.

[157] 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.

[158] Mihai Putinar and Seth Sullivant. Emerging applications of algebraic geometry. 2008.

[159] Laura Menini, Corrado Possieri, and Antonio Tornambè. *Algebraic Geometry for Robotics and Control Theory.* WORLD SCIENTIFIC (EUROPE), 2021. doi : 10.1142/q0308. URL https://www.worldscientific.com/doi/abs/10.1142/q0308.

[160] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer Science & Business Media, 2013.

[161] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer New York, 2008. ISBN 9780387356501. URL https://books.google.cm/books?id=yCsDO425PC0C.

[162] Carlos Moreno. *Algebraic Curves over Finite Fields.* Cambridge Tracts in Mathematics. Cambridge University Press, 1991. doi : 10.1017/CBO9780511608766.

[163] MATT DELONG. Using elliptic curves to produce quadratic number fields of high three-rank. *The Rocky Mountain Journal of Mathematics*, 34(2) :599–618, 2004. ISSN 00357596, 19453795.

[164] Marc Hindry and Joseph H. Silverman. *The Geometry of Curves and Abelian Varieties*, pages 6–167. Springer New York, New York, NY, 2000. ISBN 978-1-4612-1210-2. doi : 10.1007/978-1-4612-1210-2_2. URL https://doi.org/10.1007/978-1-4612-1210-2_2.

[165] V.K. Murty. *Introduction to Abelian Varieties*. CRM monograph series. American Mathematical Soc., 1986. ISBN 9780821870051. URL https://books.google.cm/books?id=1bJKqHqWgp4C.

[166] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. ISBN 3–5440–55640–0.

[167] A Uma Maheswari and Prabha Durairaj. Factoring polynomials using elliptic curves. *International Journal of Engineering and Technology(UAE)*, 7 :112–117, 10 2018. doi : 10.14419/ijet.v7i4.10.20819.

[168] H.W. Lenstra. Factoring integers with elliptic curves. *Ann. of Math., 126, 649 - 673 (1987)*, 126, 11 1987. doi : 10.2307/1971363.

[169] Katsuya Miyake. Twists of Hessian Elliptic Curves and Cubic Fields. *Annales mathématiques Blaise Pascal*, 16(1) :27–45, 2009. doi : 10.5802/ambp.251. URL http://www.numdam.org/articles/10.5802/ambp.251/.

[170] Dino J. Lorenzini. An invitation to arithmetic geometry. 1996.

[171] *Arithmetic and Geometry*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2015. doi : 10.1017/CBO9781316106877.

[172] Denis Xavier Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptol.*, 22(1) :93–113, 2009. doi : 10.1007/s00145-007-9002-x. URL https://doi.org/10.1007/s00145-007-9002-x.

[173] Christophe Doche, Thomas Icart, and David R. Kohel. Efficient scalar multiplication by isogeny decompositions. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, editors, *Public Key Cryptography - PKC 2006*, pages 191–206, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-33852-9.

[174] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign : Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 64–93. Springer, 2020. doi : 10.1007/978-3-030-64837-4_3. URL https://doi.org/10.1007/978-3-030-64837-4_3.

[175] Reinier Bröker, Kristin E. Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Math. Comput.*, 81(278) :1201–1231, 2012. doi : 10.1090/S0025-5718-2011-02508-1. URL https://doi.org/10.1090/S0025-5718-2011-02508-1.

[176] 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.

[177] Mireille Fouquet and François Morain. Isogeny volcanoes and the sea algorithm. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory*, pages 276–291, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg. ISBN 978-3-540-45455-7.

[178] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory. Proceedings of a conference in honor of A. O. L. Atkin, Chicago, IL, USA, September 1995*, pages 21–76. Providence, RI : American Mathematical Society, 1998. ISBN 0-8218-0880-X.

[179] Andrew V. Sutherland. Computing hilbert class polynomials with the chinese remainder theorem. *Math. Comput.*, 80(273) :501–538, 2011. doi : 10.1090/S0025-5718-2010-02373-7. URL https://doi.org/10.1090/S0025-5718-2010-02373-7.

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

[181] Daniel Shumow. Isogenies of elliptic curves : A computational approach. *IACR Cryptol. ePrint Arch.*, page 522, 2009. URL http://eprint.iacr.org/2009/522.

[182] Alin Bostan, François Morain, Bruno Salvy, and Éric Schost. Fast algorithms for computing isogenies between elliptic curves. *Math. Comput.*, 77(263) :1755–1778, 2008. doi : 10.1090/S0025-5718-08-02066-8. URL https://doi.org/10.1090/S0025-5718-08-02066-8.

[183] René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory, Series A*, 46(2) :183–211, 1987. ISSN 0097-3165. doi : https://doi.org/10.1016/0097-3165(87)90003-3. URL https://www.sciencedirect.com/science/article/pii/0097316587900033.

[184] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, Ser. 4, 2(4) :521–560, 1969. doi : 10.24033/asens.1183. URL http://www.numdam.org/articles/10.24033/asens.1183/.

[185] Tetsuya Izu, Jun Kogure, Masayuki Noro, and Kazuhiro Yokoyama. Efficient implementation of schoof's algorithm. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology — ASIACRYPT'98*, pages 66–79, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg. ISBN 978-3-540-49649-6.

[186] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted hessian curves. In Kristin Lauter and Francisco Rodríguez-Henríquez, editors, *Progress in Cryptology – LATINCRYPT 2015*, pages 269–294, Cham, 2015. Springer International Publishing. ISBN 978-3-319-22174-8.

[187] 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.

[188] Katsuyuki Okeya, Hiroyuki Kurumatani, and Kouichi Sakurai. Elliptic curves with the montgomery-form and their cryptographic applications. In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography*, pages 238–257, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg. ISBN 978-3-540-46588-1.

[189] Reza R. Farashahi, Hongfeng Wu, and Chang-An Zhao. Efficient arithmetic on elliptic curves over fields of characteristic three. In Lars R. Knudsen and Huapeng Wu, editors, *Selected Areas in Cryptography*, pages 135–148, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-35999-6.

[190] Reza R. Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, pages 243–260, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[191] Reza R. Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In Phong Q. Nguyen and David Pointcheval, editors, *Public Key Cryptography – PKC 2010*, pages 243–260, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg. ISBN 978-3-642-13013-7.

[192] Pradeep Kumar Mishra and Vassil Dimitrov. Efficient quintuple formulas for elliptic curves and efficient scalar multiplication using multibase number representation. In Juan A. Garay, Arjen K. Lenstra, Masahiro Mambo, and René Peralta, editors, *Information Security*, pages 390–406, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-75496-1.

[193] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology – AFRICACRYPT 2008*, pages 389–405, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg. ISBN 978-3-540-68164-9.

[194] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. Ntru : A ring-based public key cryptosystem. In Joe P. Buhler, editor, *Algorithmic Number Theory*, pages 267–288, Berlin, Heidelberg, 1998. Springer Berlin Heidelberg. ISBN 978-3-540-69113-6.

[195] R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44 :114–116, January 1978.

[196] Pascal Giorgi, Laurent Imbert, and Thomas Izard. Optimizing elliptic curve scalar multiplication for small scalars. In Franklin T. Luk, Mark S. Schmalz, Gerhard X. Ritter, Junior Barrera, and Jaakko T. Astola, editors, *Mathematics for Signal and Information Processing*, volume 7444, pages 209 – 218. International Society for Optics and Photonics, SPIE, 2009. doi : 10.1117/12.827689. URL `https://doi.org/10.1117/12.827689`.

[197] Dustin Moody. Division polynomials for jacobi quartic curves. In *ISSAC*, pages 265–272. ACM, 2011.

[198] Peter W. Shor. Algorithms for quantum computation : Discrete logarithms and factoring. In *FOCS*, pages 124–134. IEEE Computer Society, 1994.

[199] Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. How to construct csidh on edwards curves. In Stanislaw Jarecki, editor, *Topics in Cryptology – CT-RSA 2020*, pages 512–537, Cham, 2020. Springer International Publishing. ISBN 978-3-030-40186-3.

[200] Satoshi Furukawa, Noboru Kunihiro, and Katsuyuki Takashima. Multi-party key exchange protocols from supersingular isogenies. In *ISITA*, pages 208–212. IEEE, 2018.

[201] David Jao, Stephen Miller, and Ramarathnam Venkatesan. Do all elliptic curves of the same order have the same difficulty of discrete log ? 12 2004. ISBN 978-3-540-30684-9. doi : 10.1007/11593447_2.

[202] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, pages 29–50, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-76900-2.

[203] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In Kaoru Kurosawa, editor, *Advances in Cryptology – ASIACRYPT 2007*, pages 29–50, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg. ISBN 978-3-540-76900-2.

[204] Alfred J. Menezes. *Elliptic curve public key cryptosystems*, volume 234 of *The Kluwer international series in engineering and computer science*. Kluwer, 1997.

[205] Jean-François Biasse, Xavier Bonnetain, Benjamin Pring, André Schrottenloher, and William Youmans. A trade-off between classical and quantum circuit size for an attack against CSIDH. *J. Math. Cryptol.*, 15(1) :4–17, 2020.

[206] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 330–353, Cham, 2017. Springer International Publishing. ISBN 978-3-319-70697-9.

[207] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8 (1) :1–29, 2014. doi : doi:10.1515/jmc-2012-0016. URL `https://doi.org/10.1515/jmc-2012-0016`.

[208] Craig Costello. B-SIDH : supersingular isogeny diffie-hellman using twisted torsion. In *ASIACRYPT (2)*, volume 12492 of *Lecture Notes in Computer Science*, pages 440–463. Springer, 2020.

[209] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS J. Comput. Math*, 2 :118–138, 1999.

[210] 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(1) :31–44, 2021. doi : doi:10.1515/jmc-2020-0072. URL `https://doi.org/10.1515/jmc-2020-0072`.

[211] 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 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes*

in Computer Science, pages 63–91, 2016. doi : 10.1007/978-3-662-53887-6_3. URL https://doi.org/10.1007/978-3-662-53887-6_3.

[212] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In *ASIACRYPT (2)*, pages 330–353. Springer, 2017. doi : 10.1007/978-3-319-70697-9_12.

[213] Péter Kutas, Simon-Philipp Merz, Christophe Petit, and Charlotte Weitkämper. One-way functions and malleability oracles : Hidden shift attacks on isogeny-based protocols. In *EUROCRYPT (1)*, volume 12696 of *Lecture Notes in Computer Science*, pages 242–271. Springer, 2021.

[214] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings : Reductions and solutions. In *EUROCRYPT (3)*, pages 329–368. Springer, 2018. doi : 10.1007/978-3-319-78372-7_11.

[215] Greg Kuperberg. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In *TQC*, volume 22 of *LIPIcs*, pages 20–34. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2013.

[216] Daniel J. Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the csidh : Optimizing quantum evaluation of isogenies. 11477 :409–441, 2019. doi : 10.1007/978-3-030-17656-3_15.

[217] Jean-François Biasse, Annamaria Iezzi, and Michael J. Jacobson Jr. A note on the security of CSIDH. In *INDOCRYPT*, volume 11356 of *Lecture Notes in Computer Science*, pages 153–168. Springer, 2018.

[218] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of CSIDH and ordinary isogeny-based schemes. *IACR Cryptol. ePrint Arch.*, 2018 :537, 2018.

[219] David Jao, Jason 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(1) :129–138, 2020. doi : doi:10.1515/jmc-2015-0057. URL https://doi.org/10.1515/jmc-2015-0057.

[220] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2) :120–126, 1978. ISSN 0001-0782. doi : http://doi.acm.org/10.1145/359340.359342.

[221] Victor S. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*,

volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985. doi : 10.1007/3-540-39799-X_31.

[222] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177) : 203–209, January 1987. ISSN 0025-5718.

[223] Suhri Kim. Complete analysis of implementing isogeny-based cryptography using huff form of elliptic curves. *IACR Cryptol. ePrint Arch.*, 2021 :85, 2021. URL `https://eprint.iacr.org/2021/085`.

[224] Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized method for computing odd-degree isogenies on edwards curves. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part II*, volume 11922 of *Lecture Notes in Computer Science*, pages 273–292. Springer, 2019. doi : 10.1007/978-3-030-34621-8_10. URL `https://doi.org/10.1007/978-3-030-34621-8_10`.

[225] Gilles Brassard and Moti Yung. One-way group actions. In *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 94–107. Springer, 1990. doi : 10.1007/3-540-38424-3_7.

[226] Lawrence C Washington. *Elliptic curves : number theory and cryptography*. CRC press, 2008.

[227] Olivier Billet and Marc Joye. The Jacobi model of an elliptic curve and side-channel analysis. In Marc Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 34–42, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[228] P. Y. Liardet and N. P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In Çetin K. Koç, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, pages 391–401, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[229] Edlyn Teske. An elliptic curve trapdoor system. *Journal of Cryptology*, 19(1) :115–133, 2006.

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

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

[232] Reynald Lercier and François Morain. Computing isogenies between elliptic curves over $\mathbb{F}_p^n$ using Couveignes's algorithm. *Mathematics of Computation*, 69(229) :351–370, 2000.

[233] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273 : 305–347, 1971.

[234] Peter L Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177) :243–264, 1987.

[235] Hongfeng Wu and Rongquan Feng. Elliptic curves in Huff's model. *Wuhan University Journal of Natural Sciences*, 17(6) :473–480, 2012.

[236] Marc Joye, Mehdi Tibouchi, and Damien Vergnaud. Huff's model for elliptic curves. In *International Algorithmic Number Theory Symposium*, pages 234–250. Springer, 2010.

[237] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3) :393–422, 2007.

[238] David Kohel. The geometry of efficient arithmetic on elliptic curves. *Arithmetic, Geometry, Coding Theory and Cryptography*, 637 :95–109, 2015.

[239] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, and Ed Dawson. Faster group operations on elliptic curves. In *Proceedings of the Seventh Australasian Conference on Information Security*, volume 98, pages 7–20. Australian Computer Society, Inc., 2009.

[240] Nigel P Smart. The Hessian form of an elliptic curve. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 118–125. Springer, 2001.

[241] Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 402–410. Springer, 2001.

[242] Dustin Moody and Hongfeng Wu. Families of elliptic curves with rational 3-torsion. *Journal of Mathematical Cryptology*, 5(3-4) :225–246, 2012.

[243] Lawrence C Washington. *Elliptic curves : number theory and cryptography*. Chapman and Hall/CRC, 2003.

[244] Trond Stølen Gustavsen and Kristian Ranestad. A simple point counting algorithm for Hessian elliptic curves in characteristic three. *Applicable Algebra in Engineering, Communication and Computing*, 17(2) :141–150, 2006.

[245] William Fulton. *Algebraic curves : An introduction to algebraic geometry*. 2008. `http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf`.

[246] David S Dummit and Richard M Foote. *Abstract Algebra*. John Wiley & Sons, Inc., 3rd edition, 2004.

[247] Joost Renes. Computing isogenies between Montgomery curves using the action of (0, 0). In *The Eighth International Conference on Post-Quantum Cryptography, PQ-Crypto*, pages 229–247. Springer, 2017.

[248] 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.

[249] Christophe Doche, Thomas Icart, and David R. Kohel. Efficient scalar multiplication by isogeny decompositions. In *International Workshop on Public Key Cryptography*, pages 191–206. Springer, 2006.

[250] Dustin Moody. Using 5-isogenies to quintuple points on elliptic curves. *Information Processing Letters*, 111(7) :314–317, 2011.

[251] Emmanuel Fouotsa. Parallelizing pairings on Hessian elliptic curves. *Arab Journal of Mathematical Sciences*, 25(1) :29 – 42, 2019.

[252] Fouazou Lontouo Perez and Emmanuel Fouotsa. `http://www.emmanuelfouotsa-prmais.org/Portals/22/Algo_hess_divpol.ipynb.zip`.

[253] Laurence Washington. *Elliptic curves, Number theory and cryptography*. Chapman and Hall, 2 edition, 2008.

[254] Fouazou Lontouo Perez and Emmanuel Fouotsa. Analogue of vélu's formulas for computing isogenies over hessian model of elliptic curves. Cryptology ePrint Archive, Report 2019/1480, 2019. `https://eprint.iacr.org/2019/1480`.

[255] Maciej Ulas. On torsion points on an elliptic curves via division polynomials. *Zeszyty Naukowe Uniwersytetu Jagiellonskiego. Universitatis Iagellonicae Acta Mathematica*, 1285, 01 2005.

[256] Dustin Moody. Division polynomials for jacobi quartic curves. pages 265–272, 01 2011. doi : 10.1145/1993886.1993927.

[257] J. Gonzalez. On the division polynomials of elliptic curves, contributions to the algorithmic study of problems of arithmetic moduli. *Rev. R. Acad. Cienc. Exactas F´ıs. Nat*, 94(3) :377–381, 2000.

[258] J. McKee. Computing division polynomials. *Mathematics of Computations*, 63(208) : 17–23, 2010.

[259] Fedor Bogov and Hang Fu. Division polynomials and intersection of projective torsion points. *Eur. J. Math.s*, 2(3) :644–660, 2016.

[260] H. Verdure. Factorisation patterns of division polynomials. *Proc. Japan Acad. Ser. A Math. Sci*, 80(5) :79–82, 2004.

[261] Michael Lesk and Brian Kernighan. Computer typesetting of technical journals on UNIX. In *Proceedings of American Federation of Information Processing Societies : 1977 National Computer Conference*, pages 879–888, Dallas, Texas, 1977.

[262] D. Sadornil. A note on factorisation of division polynomials, 2006.

[263] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp*, 44(170) :483–494, 1985.

[264] J. Miret, R. Moreno, A. Rio, and M. Valls. Computing the l-power torsion of an elliptic curve over a finite field. *Math. Comp*, 78(267) :1767–1786, 2009.

[265] Trygve Nagell. Solution de quelque problemes dans la theorie arithmetique des cubiques planes du premier genre. *Wid. Akad. Skrifter Oslo I, Nr*, 1, 1935.

[266] Fedor Bogomolov and Hang Fu. Elliptic curves with large intersection of projective torsion points. *Eur. J. Math.*, 4(2) :555–560, 2018.

[267] Fedor Bogomolov, Hang Fu, and Yuri Tschinkel. Torsion of elliptic curves and unlikely intersections. *Geometry and Physics : A Festschrift in Honour of Nigel Hitchin*, 1(2) : 19–38, 2018.

[268] Javad Doliskani. On division polynomial pit and supersingularity. *Appl. Algebra Eng. Commun. Comput.*, 29(5) :393–407, 2018.

[269] Dieulefait Luis, Gonzalez-Jimenez Enrique, and jimenez urroz Jorge. On fields of definition of torsion points of elliptic curves with complex multiplication. In *Proceedings of the American Mathematical Society.*, volume 139, 2009.

[270] JI. Garcia-Selfa, M.A. Olalla, and J.M. Tornero. Computing the rational torsion of an elliptic curve using tate normal form. *J. Number Theory 96*, 96 :76–88, 2002.

[271] Hanson Smith. Ramification in the division fields of elliptic curves and an application to sporadic points on modular curves, 2018.

[272] I. Burhanuddin and M. Huang. Elliptic curve torsion points and division polynomials. *Computational Aspects of Algebraic Curves*, 13 :13–37, 2005.

[273] González-Jiménez, Enrique, and Álvaro Lozano-Robledo. On the torsion of rational elliptic curves over quartic fields. *Mathematics of Computation*, 87(311) :1457–1478, 2017.

[274] Filip Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on x1(n). *Mathematical Research Letters*, 23(1) :245–272, 2016.

[275] Rongquan Feng and Hongfeng Wu. A mean value formula for elliptic curves. *Journal of Numbers*, 2014 :1–5, 2014.

[276] R. Moloney and G. McGuire. Two kinds of division polynomials for twisted edwards curves. *Appl. Alg. Eng. Com. Comp.*, 22 :321–345, 2011.

[277] Dustin Moody. Mean value formulas for twisted edwards curves. *Journal of Combinatorics and Number Theory*, 3(2), 2011.

[278] Rongquan Feng and Hongfeng Wu. A mean value formula for elliptic curves. Cryptology ePrint Archive, Report 2009/586, 2009. `https://eprint.iacr.org/2009/586`.

[279] Dustin Moody. Mean value formulas for twisted edwards curves. Cryptology ePrint Archive, Report 2010/142, 2010. `https://eprint.iacr.org/2010/142`.

[280] Dustin Moody. Divison polynomials for alternate models of elliptic curves. Cryptology ePrint Archive, Report 2010/630, 2010. `https://eprint.iacr.org/2010/630`.

[281] Marc Joye and Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 402–410, 2001.

[282] Nigel P. Smart. The hessian form of an elliptic curve. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, number Generators, pages 118–125, 2001.

[283] Reza Rezaeian Farashahi and Marc Joye. Efficient arithmetic on hessian curves. In *Public Key Cryptography - PKC 2010, 13th International Conference on Practice and Theory in Public Key Cryptography, Paris, France, May 26-28, 2010. Proceedings*, pages 243–260, 2010.

[284] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted hessian curves. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico. Proceedings*, pages 269–294, 2015.

[285] Haihua Gu, Dawu Gu, and WenLu Xie. Efficient pairing computation on elliptic curves in hessian form. In *Information Security and Cryptology - ICISC 2010 - 13th International Conference, Seoul, Korea, December 1-3, 2010, Revised Selected Papers*, pages 169–176, 2010.

[286] Emmanuel Fouotsa. Parallelizing pairings on hessian elliptic curves. *Arab Journal of Mathematical Sciences*, 25(1) :555–579, 2019. doi : 10.1016/j.ajmsc.2018.06.001.

[287] Dustin Moody and Daniel Shumow. Analogues of vélu's formulas for isogenies on alternate models of elliptic curves. *Math. Comput.*, 85(300) :1929–1951, 2016.

[288] Jesús-Javier Chi-Domínguez and Francisco Rodríguez-Henríquez. Optimal strategies for CSIDH. *IACR Cryptol. ePrint Arch.*, 2020 :417, 2020. URL `https://eprint.iacr.org/2020/417`.

[289] Luca De Feo, Jean Kieffer, and Benjamin Smith. Towards practical key exchange from ordinary isogeny graphs. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part III*, volume 11274 of *Lecture Notes in Computer Science*, pages 365–394. Springer, 2018.

[290] Kohei Nakagawa, Hiroshi Onuki, Atsushi Takayasu, and Tsuyoshi Takagi. L_1-norm ball for CSIDH : optimal strategy for choosing the secret key space. *IACR Cryptol. ePrint Arch.*, 2020 :181, 2020. URL `https://eprint.iacr.org/2020/181`.

[291] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3) :209–247, 2014.

[292] Xiu Xu, Wei Yu, Kunpeng Wang, and Xiaoyang He. Constructing isogenies on extended jacobi quartic curves. In Kefei Chen, Dongdai Lin, and Moti Yung, editors, *Information Security and Cryptology - 12th International Conference, Inscrypt 2016,*

Beijing, China, November 4-6, 2016, Revised Selected Papers, volume 10143 of *Lecture Notes in Computer Science*, pages 416–427. Springer, 2016.

[293] Hüseyin Hisil. *Elliptic curves, group law, and efficient computation.* PhD thesis, Queensland University of Technology, 2010. URL `https://eprints.qut.edu.au/33233/`.

[294] Olivier Billet and Marc Joye. The jacobi model of an elliptic curve and side-channel analysis. In Marc P. C. Fossorier, Tom Høholdt, and Alain Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 1 5th International Symposium, AAECC-1 5, Toulouse, France, May 1 2-1 6,2003, Proceedings*, volume 2643 of *Lecture Notes in Computer Science*, pages 34–42. Springer, 2003.

[295] J. Vélu. Isogenies entre courbes elliptiques. *CR Acad. Sci. Paris*, Séries A(273).

[296] Isogeny formulas for jacobi intersection and twisted hessian curves, 2020.

[297] Yan Huang, Fangguo Zhang, Zhi Hu, and Zhijie Liu. Optimized arithmetic operations for isogeny-based cryptography on huff curves. In Joseph K. Liu and Hui Cui, editors, *Information Security and Privacy - 25th Australasian Conference, ACISP 2020, Perth, WA, Australia, November 30 - December 2, 2020, Proceedings*, volume 12248 of *Lecture Notes in Computer Science*, pages 23–40. Springer, 2020.

[298] Robert Dryło, Tomasz Kijko, and Michał Wroński. Efficient montgomery-like formulas for general huff's and huff's elliptic curves and their applications to the isogeny-based cryptography. Cryptology ePrint Archive, Report 2020/526, 2020. `https://eprint.iacr.org/2020/526`.

[299] T. Izu and T. Takagi. Exceptional procedure attack on elliptic curve cryptosystems. *PKC 2003 , LNCS, Springer*, vol. 2567, pp. 224-239, 2003.

[300] Joao Paulo Da Silva and Julio Lopez annd Ricardo Dahab.

[301] W. Stein. Sage mathematics software (version 4.8). *The Sage Group*, 2012. `http://www.sagemath.org`.

[302] Cannon J. Bosma, W. and C. Playout. The magma algebra system i. the user language. *J. Symbolic Comput.*, vol. 24(3-4), pp. 235-265, 1997.

[303] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Domínguez, Luca De Feo, Francisco Rodríguez-Henríquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *Progress in Cryptology - LATINCRYPT 2019 - 6th*

International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2-4, 2019, Proceedings, pages 173–193, 2019.

[304] Javad Doliskani, Geovandro C. C. F. Pereira, and Paulo S. L. M. Barreto. Faster cryptographic hash function from supersingular isogeny graphs. *IACR Cryptology ePrint Archive*, 2017 :1202, 2017. URL `http://eprint.iacr.org/2017/1202`.

[305] Suhri Kim, Kisoon Yoon, Young-Ho Park, and Seokhie Hong. Optimized method for computing odd-degree isogenies on edwards curves. *IACR Cryptology ePrint Archive*, 2019 :110, 2019. URL `https://eprint.iacr.org/2019/110`.

[306] Reza Azarderakhsh, Elena Bakos Lang, David Jao, and Brian Koziel. Edsidh : Supersingular isogeny diffie-hellman key exchange on edwards curves. In *Security, Privacy, and Applied Cryptography Engineering - 8th International Conference, SPACE 2018, Kanpur, India, December 15-19, 2018, Proceedings*, pages 125–141, 2018.

[307] Michael Meyer and Steffen Reith. A faster way to the CSIDH. *IACR Cryptology ePrint Archive*, 2018 :782, 2018. URL `https://eprint.iacr.org/2018/782`.

[308] Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian Curves. In *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, pages 269–294, 2015.

[309] P.S.L.M. Barreto, B. Lynn, and M. Scott. Efficient implementation of pairing-based cryptosystems. *Journal of Cryptology*, vol. 17(4), pp. 321-334, 2004.

[310] Mireille Fouquet and François Morain. Isogeny volcanoes and the SEA algorithm. In *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, pages 276–291, 2002.

[311] Noam D. Alkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory, Proceedings*, pages 21–76, 1997.

[312] Joost Renes. Computing isogenies between montgomery curves using the action of (0, 0). In *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, pages 229–247, 2018.

[313] Steven D. Galbraith, Xibin Lin, and Michael Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. *J. Cryptology*, 24(3) :446–469, 2011.

[314] Emmanuel Fouotsa, Nadia El Mrabet, and Aminatou Pecha. Magma code for the implementation of optimal ate pairing on elliptic curves with $k = 9, 15, 27$. In *http ://www.emmanuelfouotsa-prmais.org/Portals/22/OptAteOddegree.txt*, 2018.

[315] Thinh Dang and Dustin Moody. Twisted hessian isogenies. *IACR Cryptology ePrint Archive*, 2019 :1003, 2019.

[316] João Paulo da Silva, Ricardo Dahab, and Julio López. 2-isogenies between elliptic curves in hesse model. In *Anais do XVIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*, pages 57–64. SBC, 2018.

[317] J.H. Silvermann. *The Arithmetic of elliptic curves*, volume 106 of graduate texts in Mathematics. Springer-Verlag, 2009.

[318] Suhri Kim, Kisoon Yoon, Jihoon Kwon, Seokhie Hong, and Young-Ho Park. Efficient isogeny computations on twisted edwards curves. *Security and Communication Networks*, 2018 :5747642 :1–5747642 :11, 2018.

[319] Neriman Gamze Orhon and Hüseyin Hisil. Speeding up huff form of elliptic curves. *Des. Codes Cryptogr.*, 86(12) :2807–2823, 2018.

[320] Rene Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp*, 44(3) :483–494, 1985.

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

[322] Debiao He, Jianhua Chen, and Jin Hu. A random number generator based on isogenies operations. *IACR Cryptology ePrint Archive*, 2010 :94, 2010.

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

[324] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 190–200, 2001.

[325] Xiu Xu, Wei Yu, Kunpeng Wang, and Xiaoyang He. Constructing isogenies on extended Jacobi quartic curves. In *Information Security and Cryptology - 12th International Conference, Inscrypt 2016, Beijing, China, November 4-6, 2016, Revised Selected Papers*, pages 416–427, 2016.

[326] D. V Chudnovsky and G. V. Chudnovky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests,. *Advances in Applied Mathematics*, vol. 7(4), pp. 385-434, 1986.

[327] Lijun Zhang, Kunpeng Wang, Hong Wang, and Dingfeng Ye. Another elliptic curve model for faster pairing computation. In *Information Security Practice and Experience - 7th International Conference, ISPEC 2011, Guangzhou, China, May 30 - June 1, 2011. Proceedings*, pages 432–446, 2011.

[328] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *IACR Cryptol. ePrint Arch.*, 2020 :341, 2020. URL `https://eprint.iacr.org/2020/341`.

[329] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. *IACR Cryptol. ePrint Arch.*, 2020 :1108, 2020. URL `https://eprint.iacr.org/2020/1108`.

[330] P. W. Shor. Algorithms for quantum computation : discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi : 10.1109/SFCS.1994.365700.

[331] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. Math. Commun.*, 4(2) :215–235, 2010. doi : 10.3934/amc.2010.4.215. URL `https://doi.org/10.3934/amc.2010.4.215`.

[332] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519. Springer, 2020. doi : 10.1007/978-3-030-64834-3_17. URL `https://doi.org/10.1007/978-3-030-64834-3_17`.

[333] Jesus-Javier Chi-Dominguez and Francisco Rodriguez-Henriquez. Optimal strategies for csidh. *Advances in Mathematics of Communications*, 10 2020. doi : 10.3934/amc.2020116.

[334] Craig Costello and Hüseyin Hisil. A simple and compact algorithm for SIDH with arbitrary degree isogenies. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*,

pages 303–329. Springer, 2017. doi : 10.1007/978-3-319-70697-9_11. URL https://doi.org/10.1007/978-3-319-70697-9_11.

[335] Joost Renes. Computing isogenies between montgomery curves using the action of (0, 0). In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, volume 10786 of *Lecture Notes in Computer Science*, pages 229–247. Springer, 2018. doi : 10.1007/978-3-319-79063-3_11. URL https://doi.org/10.1007/978-3-319-79063-3_11.

[336] Dustin Moody. Divison polynomials for alternate models of elliptic curves. *IACR Cryptol. ePrint Arch.*, 2010 :630, 2010. URL http://eprint.iacr.org/2010/630.

[337] Richard Moloney and Gary McGuire. Two kinds of division polynomials for twisted edwards curves. *Appl. Algebra Eng. Commun. Comput.*, 22(5-6) :321–345, 2011. doi : 10.1007/s00200-011-0153-5. URL https://doi.org/10.1007/s00200-011-0153-5.

[338] Fouazou Lontouo Perez Broon, Fouotsa Emmanuel, and Daniel Tieudjo. Division polynomials on the hessian model of elliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–16, 11 2020. doi : 10.1007/s00200-020-00470-8.

[339] Fouazou Lontouo Perez Broon, Thinh Dang, Emmanuel Fouotsa, and Dustin Moody. Isogenies on twisted hessian curves. *Journal of Mathematical Cryptology*, 15(1) : 345–358, 2021. doi : doi:10.1515/jmc-2020-0037. URL https://doi.org/10.1515/jmc-2020-0037.

[340] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. Status report on the first round of the nist post-quantum cryptography standardization process, 2019-01-31 2019.

[341] Dustin Moody. Post quantum cryptography standardization : Announcement and outline of nist's call for submissions., 2016. URL https://csrc.nist.gov/Presentations/2016/Announcement-and-outline-of-NIST-s-Call-for-Submis.

[342] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, and Daniel Smith-Tone. Status report on the first round of the nist post-quantum cryptography standardization process, 2020. URL https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf.

[343] Andreas Gathmann. Plane algebraic curves, 2017. https://www.mathematik.uni-kl.de/~gathmann/class/curves-2018/curves-2018.pdf.

[344] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted edwards curves. In Serge Vaudenay, editor, *Progress in Cryptology - AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008. Proceedings*, volume 5023 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 2008. doi : 10.1007/978-3-540-68164-9_26. URL https://doi.org/10.1007/978-3-540-68164-9_26.

[345] Marc Joye, Mehdi Tibouchi, and Damien Vergnaud. Huff's model for elliptic curves. In Guillaume Hanrot, François Morain, and Emmanuel Thomé, editors, *Algorithmic Number Theory, 9th International Symposium, ANTS-IX, Nancy, France, July 19-23, 2010. Proceedings*, volume 6197 of *Lecture Notes in Computer Science*, pages 234–250. Springer, 2010. doi : 10.1007/978-3-642-14518-6_20. URL https://doi.org/10.1007/978-3-642-14518-6_20.

[346] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48 :243–264, 1987. ISSN 0025–5718. URL : http ://links.jstor.org/sici ?sici=0025-5718(198701)48 :177<243 :STPAEC>2.0.CO ;2

[347] Katsuyuki Okeya and Kouichi Sakurai. Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a montgomery-form elliptic curve. In Çetin Kaya Koç, David Naccache, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, volume 2162 of *Lecture Notes in Computer Science*, pages 126–141. Springer, 2001. doi : 10.1007/3-540-44709-1_12. URL https://doi.org/10.1007/3-540-44709-1_12.

[348] Arnold K. Pizer. Ramanujan graphs and Hecke operators. *Bulletin (New Series) of the American Mathematical Society*, 23(1) :127 – 137, 1990. doi : bams/1183555725. URL https://doi.org/.

[349] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones mathematicae*, 2 :134–144, 1966. URL http://eudml.org/doc/141848.

[350] Satoshi Furukawa, Noboru Kunihiro, and Katsuyuki Takashima. Multi-party key exchange protocols from supersingular isogenies. In *2018 International Symposium on Information Theory and Its Applications (ISITA)*, pages 208–212, 2018. doi : 10.23919/ISITA.2018.8664316.

[351] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2017. doi : 10.1007/978-3-319-70694-8_1. URL https://doi.org/10.1007/978-3-319-70694-8_1.

[352] Oleg Taraskin, Vladimir Soukharev, David Jao, and Jason T. LeGrow. Towards isogeny-based password-authenticated key establishment. *J. Math. Cryptol.*, 15 (1) :18–30, 2020. doi : 10.1515/jmc-2020-0071. URL https://doi.org/10.1515/jmc-2020-0071.

[353] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) :644–654, November 1976.

[354] Daniel Shumow. Isogenies of elliptic curves : A computational approach. *CoRR*, abs/0910.5370, 2009. URL http://arxiv.org/abs/0910.5370.

[355] Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Yi-Kai Liu. Status report on the first round of the nist post-quantum cryptography standardization process, 2019-01-31 00 :01 :00 2019. URL https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=927303.

[356] Dustin Moody, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu, Carl Miller, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, and Jacob Alperin-Sheriff. Status report on the second round of the nist post-quantum cryptography standardization process, 2020-07-22 2020.