Contributions aux aspects effectifs des variétés abéliennes et à leurs applications

Gaetan Bisson

CONTRIBUTIONS AUX ASPECTS EFFECTIFS DES VARIÉTÉS ABÉLIENNES ET À LEURS APPLICATIONS

GAETAN BISSON

Mémoire présenté à l'université de la Polynésie française
en vue de l'obtention de l'habilitation à diriger les recherches,
spécialité mathématiques.

Soutenu publiquement le 19 juin 2023 devant le jury ci-après.

RAPPORTEURS

Jean-Marc Couveignes	*Professeur, Université de Bordeaux*
Sylvain Duquesne	*Professeur, Université de Rennes*
Renate Scheidler	*Professeur, University of Calgary*

EXAMINATEURS

Laurent Imbert	*Directeur de recherche, CNRS Montpellier*
Elisa Lorenzo García	*Maîtresse-assistante, Université de Neuchâtel*
Alexander Rahm	*Professeur, Université de la Polynésie française*

Table des matières

Remerciements

Ce mémoire n'aurait jamais vu le jour sans les encouragements récurrents de mes collègues ni sans la bienveillance de cette formidable communauté scientifique que j'ai eu la chance et le privilège de rejoindre. Je vous adresse un grand merci à tous et tout particulièrement à :

Jean-Marc Couveignes pour ses conseils avisés.

Sylvain Duquesne et Renate Scheidler pour leur immense soutien.

Laurent Imbert, Elisa Lorenzo García et Alexander Rahm pour me faire honneur.

Takakazu Satoh, Pierrick Gaudry et Tanja Lange pour m'avoir guidé.

Kristin Lauter et Igor Shparlinski pour m'avoir accompagné.

Roger Oyono pour son accueil, sa confiance et son amitié.

Samir Perlaza pour être un collègue d'exception.

Drew Sutherland, Damien Robert, Marco Streng, Mehdi Tibouchi, Dimitar Jetchev et Alp Bassa pour nos fructueux échanges d'idées.

Alexey Zykin, Stéphane Ballet et Philippe Lebacque pour leur énergie contagieuse.

Samuele Anni et Benjamin Wesolowski pour leur plume persuasive.

Christophe Ritzenthaler pour son activité de contrôle.

Enfin, je ne pourrais remercier assez ceux qui me supportent quotidiennement, y compris en dehors des heures de bureau : Noam, Manon et Prescillia.

Gaetan Bisson
Punaauia, avril 2023

Synthèse des activités

Après l'obtention en 2011 de mon doctorat co-encadré par Pierrick Gaudry (France) et Tanja Lange (Pays-Bas), j'ai effectué un bref stage dans l'équipe de Kristin Lauter chez Microsoft Research (États-Unis) puis ai rejoint comme chercheur postdoctoral le laboratoire d'Igor Shparlinski à l'université de Macquarie (Australie) où je suis resté deux années avant d'être recruté comme maître de conférences à l'université de la Polynésie française. Ce chapitre résume succinctement mes activités professionnelles pendant ces périodes.

Production scientifique

En postdoctorat, mon activité de recherche s'est naturellement inscrite dans la continuité de mon sujet de thèse afin d'achever l'exploration de pistes déjà envisagées. Cela a notamment abouti à une méthode de calcul des anneaux d'endomorphismes des variétés abéliennes en temps sous-exponentiel, améliorant et généralisant de multiples résultats antérieurs et permettant de nouveaux records de calcul.

Ces travaux, de par leurs liens avec d'autres problématiques, m'ont conduit à progressivement élargir mes thématiques de recherche et à former de nouvelles collaborations ; c'est ainsi que, pendant les années ayant suivi mon recrutement comme maître de conférences, j'ai pu répondre à une conjecture de van Wamelen portant sur une généralisation du problème du nombre de classes de Gauss ainsi que développer une application des isogénies à la construction de revêtements exceptionnels.

Plus récemment, mes intérêts scientifiques se sont encore diversifiés par le biais de travaux communs avec des collègues de mon laboratoire. Cela a permis de consolider les liens internes à notre petite structure et a débouché sur de nouveaux résultats concernant notamment la théorie de l'information pure mais aussi l'application d'outils géométriques à l'analyse d'un phénomène d'irréductibilité sur les corps finis.

Ce sont ainsi dix articles de recherche, dont sept depuis mon doctorat, qui ont été publiés dans des revues internationales à comité de lecture telles *Mathematics of Computation* ou encore *Mathematical Research Letters*, auxquels s'ajoutent trois prépublications et une bibliothèque logicielle. Une bibliographie complète est présentée ci-après.

Réseau scientifique

Au travers des activités ci-dessus, mes collaborations se sont largement diversifiées : je compte désormais deux coauteurs au sein de mon laboratoire ; l'obtention d'un projet ANR m'a permis de tisser un véritable réseau scientifique avec de jeunes collègues des universités partenaires (Bordeaux, Marseille, Rennes) ; j'ai enfin développé des liens internationaux avec NTT (Japon) ainsi que les universités de Leiden, Princeton et Sheffield.

Rayonnement scientifique

Depuis mon recrutement comme maître de conférences, j'ai co-organisé quatre colloques internationaux : *Geometry and cryptography (GeoCrypt),* 26 participants, UPF, octobre 2013 ; *Non-archimedean analytic geometry : theory and practice,* 28 participants, UPF, août 2015 ; *Arithmetic, geometry, cryptography and coding theory (AGC2T),* 93 participants, CIRM, juin 2019 ; *Géométrie algébrique, théorie des nombres et applications,* 21 participants, UPF, août 2021. Deux ont débouché sur une édition d'actes et un troisième devrait aboutir prochainement.

J'ai aussi eu l'honneur d'être conférencier plénier ou invité à quatre colloques internationaux : *Theoretical and practical aspects of the discrete logarithm problem,* ETH Zürich (Suisse), mai 2014 ; *Effective moduli spaces and applications to cryptography,* Université de Rennes, juin 2014 ; *L-functions and algebraic varieties,* Higher School of Economics (Russie), février 2018 ; *Computations and their uses in number theory,* CIRM, mars 2023.

À ceci s'ajoute un travail d'expertise régulier (environ quatre par an) pour des revues phares du domaine, notamment *Journal of Algebra*, *LMS Journal of Computation and Mathematics*, *Mathematics of Computation*, *Algorithmic Number Theory Symposium*, *CRYPTO* ou encore *EUROCRYPT*.

Encadrement de la recherche

Ma première expérience de co-encadrement doctoral, débutée en septembre 2022 avec Alexander Rahm, s'est malheureusement interrompue après deux mois pour difficultés personnelles du doctorant. J'avais précédemment co-encadré un stage de M2, au printemps 2022 avec Benjamin Wesolowski, et un stage de M1 à l'été 2016. L'éloignement et l'isolement de la Polynésie française limitent sensiblement les opportunités d'encadrement.

Animation de la recherche

Depuis juin 2019, en tant que directeur adjoint de mon laboratoire (GAATI, EA 3893), je soutien le directeur sur des missions variées comme l'évaluation HCERES, la gestion budgétaire mais surtout l'animation de notre petite équipe notamment via l'organisation de séminaires et l'invitation de chercheurs étrangers.

Depuis mars 2021, je siège aussi comme membre élu à la commission de la recherche du conseil académique de mon université, ce qui me conduit à étudier des dossiers scientifiques variés car émanant de toutes les disciplines représentées.

J'ai porté puis coordonné deux projets de recherche : *Cryptographic hash functions of number theoretic origins,* financé à hauteur de 26 kEUR par l'université de Macquarie de 2012 à 2014 ; *Methods for Low Dimensional Abelian Varieties (MELODIA),* financé à hauteur de 160 kEUR par l'ANR de 2021 à 2025. Ce second projet présente la particularité d'impliquer quatre universités partenaires : Bordeaux, Marseille, Polynésie, Rennes. Je répond aussi régulièrement aux appels à projets internes de notre université : bourse de thèse, organisation de colloque, mobilité entrante, ATER, etc.

Enfin, je mets un point d'honneur à adosser mes enseignements à la recherche ; ceux-ci représentent une part importante de mon temps de travail avec 358 HETD par an en moyenne depuis mon recrutement comme maître de conférences. Je suis par ailleurs impliqué dans les tâches collectives inhérentes à la formation via la création, en 2017, puis la coordination depuis, du cycle universitaire préparatoire aux grandes écoles (CUPGE) et, plus récemment, la direction du département Sciences, Technologies, Santé.

Bibliographie complète

Articles de recherche antérieurs au doctorat

[1] Gaetan Bisson et Takakazu Satoh. « More discriminants with the Brezing–Weng method ». *Progress in Cryptology — INDOCRYPT 2008*. Tome 5365. Lecture Notes in Computer Science. Springer, 2008, pages 389-399. doi : 10.1007/978-3-540-89754-5_30.

[2] Gaetan Bisson et Andrew V. Sutherland. « Computing the endomorphism ring of an ordinary elliptic curve over a finite field ». *Journal of Number Theory* 131.5 (2011) : *Elliptic Curve Cryptography*, pages 815-831. doi : 10.1016/j.jnt.2009.11.003.

[3] Gaetan Bisson et Andrew V. Sutherland. « A low-memory algorithm for finding short product representations in finite groups ». *Designs, Codes and Cryptography* 63.1 (2012), pages 1-13. doi : 10.1007/s10623-011-9527-8.

Thèse de doctorat

[4] Gaetan Bisson. *Endomorphism Rings in Cryptography*. Eindhoven University of Technology & Institut National Polytechnique de Lorraine, 2011. isbn : 90-386-2519-7. doi : 10.6100/IR714676.

Articles de recherche postérieurs au doctorat

[5] Gaetan Bisson. « Computing endomorphism rings of elliptic curves under the GRH ». *Journal of Mathematical Cryptology* 5.2 (2012), pages 101-113. doi : 10.1515/jmc.2011.008.

[6] Gaetan Bisson. « Computing endomorphism rings of abelian varieties of dimension two ». *Mathematics of Computation* 84.294 (2015), pages 1977-1989. doi : 10.1090/S0025-5718-2015-02938-X.

[7] Gaetan Bisson et Marco Streng. « On polarised class groups of orders in quartic CM-fields ». *Mathematical Research Letters* 24.2 (2017), pages 247-270. doi : 10.4310/MRL.2017.v24.n2.a1.

[8] Gaetan Bisson et Mehdi Tibouchi. « 同種写像を用いた置換有理関数の生成手法 ». *Symposium on Cryptography and Information Security — SCIS 2017*. Référence 3B2-3. IEICE, 2017.

[9] Gaetan Bisson et Mehdi Tibouchi. « Constructing permutation rational functions from isogenies ». *SIAM Journal on Discrete Mathematics* 32.3 (2018), pages 1741-1749. doi : 10.1137/17M1135736.

[10] Gaetan Bisson et Roger Oyono. « On the vaccination threshold for Covid-19 in French Polynesia ». *Pacific Health* 5 (2022). doi : 10.24135/pacifichealth.v5i.59.

[11] Samir M. Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie et Stefano Rini. « Empirical risk minimization with relative entropy regularization : optimality and sensitivity analysis ». *International Symposium on Information Theory — ISIT 2022*. IEEE, 2022, pages 684-689. doi : 10.1109/ISIT50566.2022.9834273.

Prépublications

[12] Samir M. Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie et Stefano Rini. *Empirical risk minimization with generalized relative entropy regularization*. Soumis à *Journal of Machine Learning Research*. Rapport scientifique 9454. Institut national de recherche en informatique et en automatique, 2021. URL : https://hal.inria.fr/INRIA-RRRT/hal-03560072.

[13] Alp Bassa, Gaetan Bisson et Roger Oyono. « Iterative constructions of irreducible polynomials from isogenies ». Cornell University arXiv repository. 2023. DOI : 10.48550/arXiv.2302.09674.

[14] Samir M. Perlaza, Iñaki Esnaola, Gaetan Bisson et H. Vincent Poor. « The impact of data aggregation on the validation of the Gibbs algorithm ». Soumis à *International Symposium on Information Theory — ISIT 2023*. 2023.

Bibliothèque logicielle

[15] Gaetan Bisson, Romain Cosset et Damien Robert. *AVIsogenies*. A library for computing isogenies between abelian varieties. Première version en 2010 ; dernière version en 2021. Agence pour la protection des programmes, IDDN.FR.001.440011.000.R.P.2010.000.10000. URL : https://gitlab.inria.fr/roberdam/avisogenies/.

Édition d'ouvrages collectifs

[16] Stéphane Ballet, Gaetan Bisson, Roger Oyono, Renate Scheidler et Nicolas Thériault, éditeurs. *Advances in Mathematics of Communications. Special issue on GEOCRYPT 2013*. Tome 8. 4. American Institute of Mathematical Sciences, 2014. URL : https://www.aimsciences.org/journal/1930-5346/2014/8/4.

[17] Stéphane Ballet, Gaetan Bisson et Irene Bouw, éditeurs. *Arithmetic, Geometry, Cryptography and Coding Theory*. Tome 770. Contemporary Mathematics. American Mathematical Society, 2021. ISBN : 1-4704-5426-2. DOI : 10.1090/conm/770.

Introduction aux travaux de recherche

Grandes thématiques

La structure de groupe est l'une des plus fondamentales en mathématiques. Lorsque les éléments d'un groupe, sa loi et son inverse sont tous décrits explicitement par des équations polynomiales, on parle de groupe algébrique. Un théorème de Chevalley [14] décompose tout groupe algébrique en un groupe de matrices et un groupe algébrique projectif connexe, ce que l'on appelle communément une *variété abélienne*.

Ces objets furent longtemps étudiés pour leurs propriétés théoriques, notamment dans le cadre du douzième problème de Hilbert [2]. Les variétés abéliennes les plus élémentaires, celles de dimension un, portent le nom de *courbes elliptiques* et admettent des formes particulièrement explicites, telle $y^2 = x^3 + ax + b$. Elles sont l'objet de théories singulièrement riches comme la conjecture de modularité de Taniyama–Shimura qui fut démontrée [79] partiellement pour en déduire le grand théorème de Fermat [61, 62].

Parallèlement, la cryptographie moderne se développa grâce aux mathématiques et, en particulier, grâce aux groupes algébriques qui sont des candidats évidents pour cette tâche de par leurs propriétés effectives. Les groupes de matrices présentent une structure transparente les rendant inadaptés [54, 68] et c'est ainsi qu'on bâtit des systèmes cryptographiques grâce aux courbes elliptiques [37, 39] puis grâce aux variétés abéliennes de dimension supérieure [44] ; aujourd'hui, de tels systèmes sécurisent les protocoles de communication SSH et TLS, pour n'en citer que deux.

Ces multiples applications ont largement motivé le développement de méthodes effectives. Concrètement, cela consiste à concevoir puis à analyser des algorithmes permettant de construire et de manipuler de manière explicite des objets mathématiques. S'agissant de variétés abéliennes, l'ensemble de ces techniques relève plus spécifiquement du domaine de la théorie algorithmique des nombres.

C'est dans ce contexte que s'inscrivent mes travaux de recherche. Ils portent sur les variétés abéliennes, leurs morphismes appelés isogénies ainsi que d'autres concepts afférents ; ils consistent, d'une part, à comprendre et à expliciter leurs propriétés d'un point de vue effectif et, d'autre part, à les exploiter afin d'attaquer des problèmes ouverts en théorie algorithmique des nombres et en cryptographie.

Résumé des travaux

Ce mémoire présente une sélection de travaux effectués depuis mon doctorat. Il est organisé en quatre chapitres traitant chacun de thématiques relativement indépendantes. Le lecteur est invité à se référer aux articles originaux pour tout complément d'information et notamment pour les démonstrations des résultats énoncés.

Chapitre 1. Après une courte introduction à la théorie de la multiplication complexe de Shimura et Taniyama, sur laquelle repose la majorité de mes contributions, ce chapitre décrit des travaux fondamentaux concernant la structure d'objets au cœur de cette théorie : les groupes de classes polarisés. On obtient des critères explicites caractérisant les couples d'ordres $(\mathcal{O}, \mathcal{O}')$ d'un corps CM quartique vérifiant $\mathfrak{C}(\mathcal{O}) = \mathfrak{C}(\mathcal{O}')$. Ils sont ensuite appliqués, d'une part, à la résolution d'une conjecture de van Wamelen concernant l'énumération des surfaces abéliennes définies sur $\mathbb{Q}$ avec multiplication complexe et, d'autre part, à l'analyse d'une méthode de calcul des anneaux d'endomorphismes qui fait l'objet du chapitre suivant.

Chapitre 2. La structure du graphe d'isogénies et ses grands enjeux sont présentés. Elle est intimement liée à la notion d'anneau d'endomorphisme des variétés abéliennes. En exploitant la théorie de la multiplication complexe et, plus précisément, le lien entre les isogénies horizontales et les idéaux des groupes de classes polarisés, on obtient le premier algorithme de complexité sous-exponentielle permettant de calculer les anneaux d'endomorphismes des surfaces abéliennes. Sa complexité est démontré sous hypothèses heuristiques.

Chapitre 3. Ce chapitre décrit deux contributions consistant à exploiter les propriétés de certaines isogénies afin d'attaquer des problèmes concernant les corps finis. La première application porte sur la construction de revêtements exceptionnels de la droite projective, un problème important tant en mathématiques pures qu'en cryptographie. La seconde application porte sur la construction de présentations itérées de corps finis, via une méthode explicite produisant des polynômes irréductibles par composition.

Chapitre 4. On présente des travaux indépendants en théorie de l'information pure et dure. Il s'agit de généraliser aux mesures σ-finies le problème de minimisation du risque empirique avec régularisation par entropie relative (ERM-RER), ce qui permet d'unifier trois théories existantes. On montre que la solution à ce problème est une mesure de Gibbs dont on étudie certaines propriétés dont le comportement asymptotique.

Chapitre 1

Théorie de la multiplication complexe

1.1 Contexte général et problématiques

Soit $\mathscr{A}$ une variété abélienne de dimension g définie sur un corps k que l'on supposera donnée sous une forme effective, par exemple comme la variété jacobienne d'une courbe algébrique ou encore par des fonctions thêtas, donc implicitement munie d'une polarisation principale. Le problème soutenant la plupart des applications cryptographiques est le suivant.

Définition 1.1.1. *Le problème du logarithme discret consiste, étant donnés deux points P et Q de $\mathscr{A}(k)$, à déterminer, s'il en existe, un scalaire $\lambda \in \mathbb{Z}$ vérifiant $Q = \lambda P$.*

Pour k fini et $g \leqslant 2$, sauf rarissimes exceptions, ce problème n'admet aucune solution connue plus efficace que l'approche générique de complexité $O\left(|\mathscr{A}(k)|^{1/2}\right)$. Les variétés abéliennes sont les seuls groupes effectifs connus qui possèdent cette propriété. Leurs isomorphismes transportent ce problème mais sont sans conséquence car très bien compris.

Théorème 1.1.2 (Torelli [4, 13]). *Deux courbes algébriques définies sur un corps parfait sont isomorphes si et seulement si leurs variétés jacobiennes le sont.*

Ce résultat est rendu effectif par la théorie des invariants qui fournit des outils très explicites pour caractériser ces isomorphismes, tels le j-invariant pour le cas de la dimension $g = 1$, c'est-à-dire pour les courbes elliptiques, ou encore les invariants d'Igusa et de Rosenhain dans le cas de la dimension $g = 2$ [15, 32, 50]. Portons désormais notre attention sur des morphismes plus généraux.

Définition 1.1.3. *On appelle isogénie tout morphisme de variétés abéliennes qui, sur la cloture algébrique du corps de base, est surjectif et de noyau fini.*

Sur les corps fini, les couples de variétés isogènes sont caractérisés par le résultat suivant.

Théorème 1.1.4 (Tate [18]). *Deux variétés abéliennes simples sur un corps fini sont isogènes si et seulement si leurs endomorphismes de Frobenius ont le même polynôme caractéristique.*

Calculer le polynôme caractéristique de l'endomorphisme de Frobenius d'une variété abélienne sur un corps fini k revient à déterminer son nombre de points sur des extensions de k. De multiples algorithmes, dits de comptage des points, permettent d'effectuer ce calcul efficacement, tant en dimension un [36] qu'en dimension supérieure [46].

L'anneau d'endomorphismes $\mathrm{End}(\mathscr{A})$ de la variété abélienne $\mathscr{A}$ est un objet plus général contenant, en particulier, l'endomorphisme de Frobenius π lorsque k est fini. Pour l'étudier, on se muni d'un plongement $\iota : K \to \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ où K est un corps de nombres, cette structure étant transportée via les isogénies. Lorsqu'un tel plongement satisfait $\deg(K) = 2g$, on dit que $\mathscr{A}$ a multiplication complexe par K ou, plus exactement, par son ordre $\iota^{-1}(\mathrm{End}(\mathscr{A}))$ que l'on identifie par abus de langage avec l'anneau d'endomorphismes $\mathrm{End}(\mathscr{A})$ lui-même. Le corps K est alors un corps CM, c'est-à-dire une extension quadratique imaginaire d'un corps de nombres totalement réel de degré g.

Toutes les variétés abéliennes ordinaires absolument simples définies sur les corps finis ont multiplication complexe. Leurs anneaux d'endomorphismes sont inchangés par extension du corps de base et sont exactement les ordres du corps quadratique imaginaire $K = \mathbb{Q}(\pi)$ contenant $\mathbb{Z}[\pi, \overline{\pi}]$ et stables par conjugaison complexe [9, 24].

Les énoncés suivants précisent le lien entre isogénies et anneaux d'endomorphismes.

Définition 1.1.5. *Soit K un corps CM, K_0 son sous corps totalement réel et $\mathcal{O}$ un ordre stable par conjugaison complexe. On appelle groupe de classes polarisé le quotient $\mathfrak{C}(\mathcal{O}) = I/P$ où I désigne le groupe des couples $(\mathfrak{a}, \rho)$ avec $\mathfrak{a}$ idéal fractionnaire inversible de $\mathcal{O}$ et $\rho \in K_0$ totalement positif satisfaisant $\mathfrak{a}\overline{\mathfrak{a}} = \rho\mathcal{O}$ et où P est le sous-groupe des éléments de la forme $(\mu\mathcal{O}, \mu\overline{\mu})$ pour $\mu \in K^\times$.*

Théorème 1.1.6 (Shimura–Taniyama [16])**.** *Le groupe $\mathfrak{C}(\mathcal{O})$ agit librement sur l'ensemble des classes d'isomorphismes des variétés abéliennes d'anneau d'endomorphismes $\mathcal{O}$, l'idéal $(\mathfrak{a}, \rho)$ agissant par l'isogénie $\mathscr{A} \to \mathscr{A}/\bigcap_{\alpha\in\mathfrak{a}} \ker(\alpha)$ de degré $\mathrm{N}(\mathfrak{a})$.*

Le groupe de classes polarisé $\mathfrak{C}(\mathcal{O})$ décrit ainsi la structure de certaines isogénies que l'on qualifie d'horizontales. Dans le cas de la dimension un, c'est-à-dire des courbes elliptiques, on a $K_0 = \mathbb{Q}$ et le groupe de classes polarisé $\mathfrak{C}(\mathcal{O})$ n'est autre que le groupe de classes usuel $\mathrm{cl}(\mathcal{O})$ dont la structure est bien comprise, y compris d'un point de vue effectif.

Dans ce contexte, dont nous n'avons fait que survoler les concepts clefs et leurs principales interactions, quelques unes des grandes problématiques sont les suivantes.

La théorie des invariants. Les invariants permettent de représenter efficacement les classes d'isomorphismes de variétés abéliennes par des nombres algébriques. Les informations pertinentes pour de nombreux problèmes peuvent ainsi être condensées en de simples polynômes. La construction de nouveaux invariants et l'obtention de bornes sur leur hauteur est un problème important, tant en dimension deux [71, 86, 99, 126, 139] qu'en dimension trois où l'on distingue les variétés jacobiennes des courbes hyperelliptiques [21, 124] de celles des courbes non hyperelliptiques [38, 101, 159].

Le comptage des points. Les conjectures de Weil [10] montrent que déterminer le nombre de points d'une variété abélienne sur de petites extensions du corps de base équivaut à en calculer la fonction zêta ou encore l'endomorphisme de Frobenius π. On en déduit notamment le corps CM $\mathbb{Q}(\pi)$ qui constitue un prérequis à l'exploitation de la théorie de la multiplication complexe. Des techniques de calcul efficaces ont été développées en petite caractéristique [76, 81, 103] ainsi qu'en dimension un [36, 40, 48, 64] mais leurs extensions en grande caractéristique et dimension supérieure restent encore perfectibles [46, 74, 77].

Le calcul d'isogénies. Étant donné un sous-groupe maximal isotrope H d'une variété abélienne $\mathscr{A}$, le calcul de l'isogénie quotient $\mathscr{A} \to \mathscr{A}/H$ admet une solution classique pour les courbes elliptiques [26] mais il fallut attendre quarante ans pour qu'elle soit étendue en dimension supérieure [113, 125, 137]. Ce calcul est au cœur de nombreuses applications tant constructives que destructives en cryptographie [67, 70] dont dernièrement dans le domaine post-quantique [131, 167, 169, 172].

Les variétés abéliennes avec multiplication complexe. Il s'agit ici de caractériser les variétés abéliennes avec multiplication complexe définies sur les les corps de nombres et, en premier lieu, sur $\mathbb{Q}$; ce problème généralise celui du nombre de classes de Gauss : seules treize corps quadratiques imaginaires possèdent un groupe de classes trivial [12, 17, 22] et on en déduit treize courbes elliptiques sur $\mathbb{Q}$ avec multiplication complexe [20]. L'extension de ces travaux aux surfaces abéliennes, entamée par van Wamelen [72, 73], a été achevée grâce aux résultats présentés dans la section ci-après. Plus récemment, le cas de la dimension trois a lui aussi été étudié [149].

Les sections suivantes décrivent des travaux communs avec Marco Streng [141].

1.2 Groupes de classes polarisés

Le groupe des classes polarisé $\mathfrak{C}(\mathcal{O}) = I/P$ introduit à la définition 1.1.5 est inchangé si les ensembles I et P sont restreints aux idéaux premiers à un entier fixé. Ceci permet de comparer ces groupes lorsque l'ordre considéré varie. Plus précisément, soient $\mathcal{O} \subset \mathcal{O}'$ deux ordres d'un même corps CM, tous deux stables par conjugaison complexe. En se restreignant aux idéaux premiers à l'indice $[\mathcal{O}' : \mathcal{O}]$, l'application $\mathfrak{a} \to \mathfrak{a}\mathcal{O}'$ induit un morphisme surjectif $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$ dont on cherche ici à caractériser le cas d'isomorphisme. Rappelons d'abord brièvement la situation en dimension un.

Cas des corps quadratiques imaginaires. Dans le cas $g = 1$, le groupe de classes polarisé $\mathfrak{C}(\mathcal{O})$ n'est autre que le groupe de classes usuel. Pour tout ordre $\mathcal{O}$ de conducteur $\mathfrak{f}$ d'un corps de nombre K dont $\mathcal{O}_K$ désigne l'anneau des entiers, ce groupe satisfait la suite exacte

$$1 \to \mathcal{O}^\times \to \mathcal{O}_K^\times \to \frac{(\mathcal{O}_K/\mathfrak{f})^\times}{(\mathcal{O}/\mathfrak{f})^\times} \to \mathrm{cl}(\mathcal{O}) \to \mathrm{cl}(\mathcal{O}_K) \to 1.$$

Lorsque K est un corps quadratique imaginaire, le conducteur est $\mathfrak{f} = f\,\mathcal{O}_K$ avec $f = [\mathcal{O}_K : \mathcal{O}]$ et, en explicitant la structure du quotient central, on obtient

$$h(\mathcal{O}) = h(\mathcal{O}_K)\frac{f}{[\mathcal{O}_K^\times : \mathcal{O}^\times]}\prod_{p \mid f}\left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right);$$

ainsi, l'égalité $h(\mathcal{O}) = h(\mathcal{O}')$ implique $[\mathcal{O}' : \mathcal{O}] \mid 6$ si $K = \mathbb{Q}\left(\sqrt{-3}\right)$ et $[\mathcal{O}' : \mathcal{O}] \mid 2$ sinon.

Cas des corps CM quartiques. Soit Φ un type d'un corps CM quartique non biquadratique K, cette dernière contrainte n'excluant que des variétés non simples ; on note Φ^r et K^r le type et le corps CM réflexe associé. Notre problème s'exprime en terme de la norme type réflexe

$$\mathrm{N}_{\Phi^r} : \begin{cases} I_{K^r} \longrightarrow I_K \\ \quad \mathfrak{a} \longmapsto \left(\mathrm{N}_{\Phi^r}(\mathfrak{a}), \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a})\right) \end{cases}$$

et plus précisément de son noyau

$$\Omega_{\mathcal{O}} = \ker\left((I_K \to \mathfrak{C}(\mathcal{O})) \circ \mathrm{N}_{\Phi^r}\right) \subset I_{K^r}.$$

En effet, l'image $I_{K^r}/\Omega_{\mathcal{O}}$ contient exclusivement des isogénies de type (ℓ, ℓ) donc efficacement calculables et exploitables par les méthodes du chapitre 2, ce qui n'est pas nécessairement le cas de $\mathfrak{C}(\mathcal{O})$; de surcroit, ce quotient apparait naturellement [16, Main theorem 3] comme

le groupe de Galois du corps de modules des variétés abéliennes de type Φ et d'anneau d'endomorphismes $\mathcal{O}$.

Soient donc $\mathcal{O} \subset \mathcal{O}'$ deux ordres de K vérifiant $\Omega_{\mathcal{O}} = \Omega_{\mathcal{O}'}$, condition toujours satisfaite dans le cas d'isomorphisme $\mathfrak{C}(\mathcal{O}) \to \mathfrak{C}(\mathcal{O}')$. Notons K_0 le sous corps totalement réel, $\mathcal{O}_K$ l'anneau des entiers et posons $f = [\mathcal{O}_K : \mathcal{O}]$. Des manipulations de théorie des nombres relativement élémentaires permettent de déduire que le noyau

$$\ker\left(\frac{(\mathcal{O}'/f\,\mathcal{O}_K)^\times}{(\mathcal{O}/f\,\mathcal{O}_K)^\times \mu_{\mathcal{O}'}} \longrightarrow \frac{(\mathcal{O}' \cap K_0/f\,\mathcal{O}_K)^\times}{(\mathcal{O} \cap K_0/f\,\mathcal{O}_K)^\times}\right)$$

est d'exposant au plus deux ; on se ramène ainsi d'un problème portant sur les idéaux à un problème portant sur les éléments. En décomposant ces anneaux quotients sur les idéaux premiers, des techniques de théorie des groupes permettent d'obtenir le résultat suivant qui borne l'indice $[\mathcal{O}' : \mathcal{O}]$.

Théorème 1.2.1 ([141, Th. 5]). *Soient $\mathcal{O} \subset \mathcal{O}' \neq \mathbb{Z}[\zeta_5]$ deux ordres d'un corps CM quartique non biquadratique K vérifiant $\Omega_{\mathcal{O}} = \Omega_{\mathcal{O}'}$. L'entier $[\mathcal{O}' : \mathcal{O}] / [\mathcal{O}' \cap K_0 : \mathcal{O} \cap K_0]$ divise $2^{10}3^4$.*

Dans le cas particulier $\mathcal{O}' = \mathcal{O}_K$ et supposant l'ordre $\mathcal{O}$ stable par conjugaison complexe, on peut expliciter la structure de K et sa théorie de Galois de sorte à obtenir un résultat plus fort qui s'affranchit de l'indice $[\mathcal{O}' \cap K_0 : \mathcal{O} \cap K_0]$ et étend donc plus naturellement le résultat classique obtenu dans le cas $g = 1$.

Théorème 1.2.2 ([141, Th. 4]). *Soit $\mathcal{O}$ un ordre stable par conjugaison complexe d'un corps CM quartique non biquadratique $K \neq \mathbb{Q}(\zeta_5)$ vérifiant $\Omega_{\mathcal{O}} = \Omega_{\mathcal{O}_K}$. On a*

$$[\mathcal{O}_K : \mathcal{O}]^2 \mid 2^{40}3^{16}\,\mathrm{N}_{K_0/\mathbb{Q}}\left(\Delta_{K/K_0}\right).$$

1.3 Application à une conjecture de van Wamelen

Soit $\mathcal{A}$ une surface abélienne définie sur $\mathbb{Q}$ absolument simple avec multiplication complexe par un ordre $\mathcal{O}$. Murabayashi et Umegaki [82] montrent que, si l'ordre est maximal, alors $\mathcal{O} = \mathcal{O}_K$ avec $K = \mathbb{Q}[x]/(x^4 + Ax^2 + B)$ pour l'un des treize triplets $[D, A, B]$ ci-dessous, où D désigne le discriminant du sous corps réel.

$[5, 5, 5]$	$[5, 10, 20]$	$[5, 65, 845]$	$[5, 85, 1445]$	
$[8, 4, 2]$	$[8, 20, 50]$	$[13, 13, 13]$	$[13, 26, 52]$	$[13, 65, 325]$
$[29, 29, 29]$	$[37, 37, 333]$	$[53, 53, 53]$	$[61, 61, 592]$	

Pour chacun de ces corps, van Wamelen explicite au plus deux classes d'isomorphismes pour $\mathcal{A}$ [72], dix-neuf au total, et démontrent qu'elles ont bien multiplication complexe [73] mais pas nécessairement par l'ordre maximal.

Par la théorie de la multiplication complexe [16, Main theorem 3], la condition $\mathcal{O} = \mathrm{End}(\mathcal{A})$ implique $\Omega_{\mathcal{O}} = \Omega_{\mathcal{O}_K} = I_{K^r}$. En explicitant les structures CM et réflexes de ces treize corps, on parvient à borner les indices $[\mathcal{O}_K : \mathrm{End}(\mathcal{A})]$ et donc à démontrer que les classes d'isomorphismes de van Wamelen ont bien multiplication complexe par un ordre maximal. On en déduit le résultat suivant.

Théorème 1.3.1 ([141, Th. 16]). *Les dix-neuf surfaces abéliennes de [72] sont, à isomorphisme près, exactement celles ayant multiplication complexe par un ordre maximal.*

Cette approche permet aussi de traiter le cas non maximal. Sept corps CM quartiques K supplémentaires vérifient $\Omega_{\mathcal{O}_K} = I_{K^r}$ [136, 175]. Pour chacun, le théorème 1.2.2 permet d'énumérer les ordres $\mathcal{O} \subset \mathcal{O}_K$ par lesquels les surfaces abéliennes peuvent avoir multiplication complexe, c'est-à-dire vérifiant $\Omega_{\mathcal{O}} = \Omega_{\mathcal{O}_K}$. Toute surface abélienne $\mathcal{A}$ avec multiplication complexes par un tel ordre $\mathcal{O}$ est $(2,2)$, $(3,3)$, $(4,4)$ ou $(5,5)$-isogène à une surface abélienne d'anneau d'endomorphismes $\mathcal{O}_K$ et peut ainsi être calculée par la bibliothèque logicielle AVIsogenies [113]. L'énoncé suivant en découle.

Théorème 1.3.2 ([141, Th. 17 et paragraphe suivant]). *Les variétés jacobiennes des courbes*

$$y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1,$$
$$y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$$

sont, à isomorphisme près, les deux seules surfaces abéliennes définies sur $\mathbb{Q}$ avec multiplication complexe par un ordre non maximal.

1.4 Application au calcul des anneaux d'endomorphismes

Soit $\mathcal{A}$ une variété abélienne ordinaire absolument simple définie sur un corps fini. Les isogénies de noyau isotrope maximal isomorphe à $(\mathbb{Z}/\ell\mathbb{Z})^2$ sont efficacement calculables ce qui permet, via le théorème 1.1.6, de déterminer si un ordre $\mathcal{O}$ donné satisfait $\mathrm{N}_\Phi(p_\mathcal{O}) \subset \Omega_{\mathrm{End}(\mathcal{A})}$. Voir le chapitre 2. Le résultat suivant, conséquence du théorème 1.2.1 décrit alors dans quelle mesure cela caractérise l'anneau $\mathrm{End}(\mathcal{A})$ lui-même.

Théorème 1.4.1 ([141, Cor. 22]). *Soient $\mathcal{O}$ et $\mathcal{O}'$ deux ordres d'un corps CM quartique non biquadratique K contenant $\mathbb{Z}[\pi, \overline{\pi}]$, stables par la multiplication complexe et satisfaisant*

$$\mathrm{N}_\Phi(p_\mathcal{O}) \subset \Omega_{\mathcal{O}'} \qquad \textit{et} \qquad \mathrm{N}_\Phi(p_{\mathcal{O}'}) \subset \Omega_\mathcal{O}.$$

Alors les indices $[\mathcal{O} : \mathcal{O} \cap \mathcal{O}']$ et $[\mathcal{O} \cap K_0 : \mathcal{O} \cap \mathcal{O}' \cap K_0]$ ont même valuation en tous les nombres premiers $\ell > 41$.

Reste, pour complètement déterminer l'anneau d'endomorphismes $\mathrm{End}(\mathcal{A})$, à l'évaluer localement en les nombres premiers ℓ inférieurs à 42 ou pouvant être absorbés par l'indice issu de la multiplication réelle ; des arguments de théorie analytique des nombres montrent, sous heuristiques, que la densité des variétés abéliennes concernées est nulle. On en déduit notamment que les méthodes décrites dans la section suivante sont de complexité sous-exponentielle dans le cas moyen.

Chapitre 2

Calcul des anneaux d'endomorphismes

2.1 Structure du graphe d'isogénies

Un autre problème important soutenant la sécurité des systèmes cryptographiques qui exploitent des variétés abéliennes, particulièrement ceux proposés pour un usage post-quantique, est le suivant.

Problème 2.1.1 (recherche d'isogénie). *Étant données deux variétés abéliennes isogènes $\mathscr{A}$ et $\mathscr{B}$ de dimension g définies sur un corps fini k, déterminer une isogénie explicite $\mathscr{A} \to \mathscr{B}$.*

Lorsque $\mathscr{A}$ et $\mathscr{B}$ ont multiplication complexe par un même ordre $\mathcal{O}$, la meilleure solution connue est l'algorithme générique [70] de complexité $O(\sqrt{|\mathfrak{C}(\mathcal{O})|})$. Les deux problèmes que voici sont donc d'importance capitale :

1. Déterminer l'anneau d'endomorphismes d'une variété abélienne donnée.
2. Exploiter la structure du graphes d'isogénies afin de se ramener au cas de multiplication complexe par un ordre présentant un petit nombre de classes ; idéalement, l'ordre maximal.

Les méthodes permettant de déterminer l'anneau d'endomorphismes d'une variété abélienne ordinaire définie sur un corps fini k étaient toutes de complexité exponentielle en la taille $\log|k|$ du corps de base [65, 106, 112] jusqu'à mes travaux de doctorat portant sur le cas des courbes elliptiques [119] ; celle-ci a ensuite été améliorée notamment afin d'être rigoureusement démontrée sous l'hypothèse de Riemann généralisée uniquement [122]. Des travaux plus récents [173] ont encore largement amélioré l'état de l'art. L'extension de ces résultats aux surfaces abéliennes fait l'objet de la section 2.4.

En première approximation, la structure du graphe d'isogénies est régie par deux résultats : d'une part, le théorème 1.1.6 qui décrit la structure des isogénies $\mathscr{A} \to \mathscr{B}$ dites horizontales, c'est-à-dire satisfaisant $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{B})$; d'autre part, le résultat suivant qui décrit la structure des autres isogénies, dites verticales.

Lemme 2.1.2 ([135, Lemma 2.1]). *Soit $\mathscr{A} \to \mathscr{B}$ une isogénie de noyau maximal isotrope isomorphe à $(\mathbb{Z}/\ell\mathbb{Z})^g$ avec $\mathscr{A}$ et $\mathscr{B}$ deux variétés abéliennes ordinaires absolument simples de dimension g définies sur un corps fini de caractéristique distincte du nombre premier ℓ. L'indice $[\mathrm{End}(\mathscr{A}) + \mathrm{End}(\mathscr{B}) : \mathrm{End}(\mathscr{A}) \cap \mathrm{End}(\mathscr{B})]$ est un diviseur de ℓ^{2g-1}.*

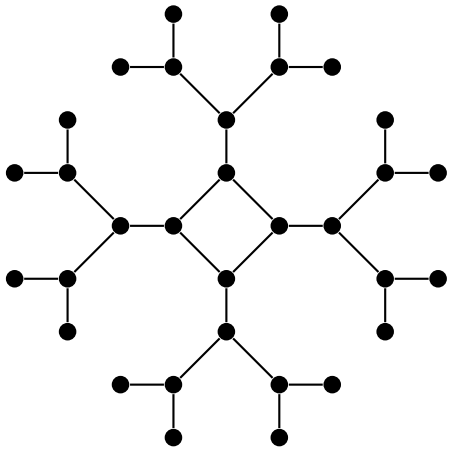


FIGURE 2.1 – Structure des composantes connexes des graphes d'isogénies des courbes elliptiques ordinaires sur les corps finis. Ici, le degré des isogénies est $\ell = 2$ (sommets de degré 1 ou $\ell + 1$) ; les deux idéaux premiers de norme ℓ sont d'ordre 4 dans le groupe de classes (longueur du cycle) ; et la valuation en ℓ du conducteur $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ est 3 (hauteur des arbres).

Lorsque $g = 1$, le corps $K = \mathbb{Q} \otimes \mathrm{End}(\mathscr{A})$ est quadratique imaginaire et ses ordres de la forme $\mathbb{Z} + u\mathcal{O}_K$; le lemme ci-dessus permet alors de partitionner les isogénies $\mathscr{A} \to \mathscr{B}$ en trois catégories :

1. $\mathrm{End}(\mathscr{B}) = \mathbb{Z} + \ell\,\mathrm{End}(\mathscr{A})$, isogénie dite ascendante ;
2. $\mathrm{End}(\mathscr{A}) = \mathbb{Z} + \ell\,\mathrm{End}(\mathscr{B})$, isogénie dite descendante ;
3. $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{B})$, isogénie dite horizontale.

Cette trichotomie est la base d'une description explicite du graphe d'isogénies [65, 83] dont la structure, communément qualifiée de volcan, est illustrée par la figure 2.1 ; voir aussi [88]. C'est principalement cette structure qu'exploite l'algorithme de KOHEL [65, §4.2] mais on ne peut s'en contenter pour obtenir un algorithme de complexité sous-exponentielle : il faut pour cela exploiter la théorie de la multiplication complexe via le théorème 1.1.6 afin de travailler plus finement avec les isogénies horizontales [119, 135].

2.2 Enjeux et applications

Parmi les grands enjeux liés à l'étude de la structure du graphes d'isogénies des variétés abéliennes ordinaires sur les corps finis et, en particulier, à son application au calcul des anneaux d'endomorphismes, on distingue les suivants.

Le calcul de l'anneau d'endomorphismes d'une variété abélienne donnée. Ce problème fait l'objet de la section suivante. Sa résolution permet d'exploiter d'un point de vue effectif les résultats de la théorie de la multiplication complexe. Déterminer l'emplacement d'une variété abélienne donnée dans sa composante connexe du graphe d'isogénies est un outil important en théorie algorithmique des nombres qui possède de nombreuses applications notamment au problème de la recherche d'isogénies mais aussi à l'énumération de certaines classes de variétés abéliennes et en particulier au calcul des polynômes modulaires et des polynômes de classes.

Le problème inverse : construire une variété abélienne d'anneau d'endomorphismes donné. La principale solution, connue sous le nom de « méthode CM », repose sur l'évaluation des polynômes de classes. Classiquement, le polynôme de Hilbert est défini par $H_{\mathcal{O}}(x) = \prod(x - j)$ où j parcours les j-invariants des courbes elliptiques sur $\overline{\mathbb{Q}}$ avec multiplication complexe par $\mathcal{O}$. Les polynômes de classes en sont une généralisation à d'autres invariants ou en dimension supérieure. Leur évaluation permet de construire des variétés abéliennes munies de certaines propriétés tel un cardinal premier ou encore un accouplement efficacement calculable [102] dont les applications notamment en cryptographie sont multiples [109, 150]. Deux approches existent pour les calculer : des techniques numériques [108] et des méthodes basées sur le théorème des restes chinois [121, 176] qui tirent parti des avancées sur le calcul des anneaux d'endomorphismes. Les avancées dans le cas $g = 2$ restent limitées [134, 132, 160] car entravées notamment par la structure moins explicite des corps CM quartique et du graphe d'isogénies [143, 158] ainsi que par la taille significative de ces objets en plus grande dimension.

Le calcul des polynômes modulaires. Comme pour les polynômes de classes, le polynôme modulaire classique, $\Phi_\ell(X, Y) = \prod(X - \alpha)$ où α parcours les j-invariants des courbes elliptiques ℓ-isogènes à celle de j-invariant Y, admet des extensions à d'autres invariants et en dimension supérieure. Leur évaluation joue notamment un rôle clef dans le cadre du comptage des points [40, 48]. Toujours comme pour les polynômes de classes, deux approches existent pour les calculer : des techniques numériques [107] et des méthodes basées sur le théorème des restes chinois [123, 176]. Leur utilité dans le cas $g = 2$ reste elle aussi limitée [104, 162].

Les sections suivantes décrivent mes travaux de l'article [135].

2.3 Treillis des ordres

Soit $\mathcal{A}$ une surface abélienne ordinaire absolument simple sur un corps fini k. Son anneau d'endomorphismes $\mathrm{End}(\mathcal{A})$ est un ordre de $K = \mathbb{Q}(\pi)$ stable par conjugaison complexe contenant $\mathbb{Z}[\pi, \overline{\pi}]$. Les tels ordres forment un treillis admettant $\mathcal{O}_K$ comme élément maximal et dont la taille peut être exponentielle en $\log(q)$ pour $q = |k|$.

Lemme 2.3.1 ([135, Lemma 6.1]). *On a l'inégalité* $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]] < 64q^2$.

Afin de déterminer $\mathrm{End}(\mathcal{A})$, l'idée principale est de parcourir ce treillis en exploitant l'implication $\mathcal{O} \subset \mathrm{End}(\mathcal{A}) \Rightarrow \mathrm{N}_\Phi(p_{\mathcal{O}}) \subset \Omega_{\mathrm{End}(\mathcal{A})}$ et en testant l'appartenance à $\Omega_{\mathrm{End}(\mathcal{A})}$ grâce aux isogénies via 1.1.6. On détermine ainsi un ordre $\mathcal{O}$ vérifiant les conditions du théorème 1.4.1 avec $\mathcal{O}' = \mathrm{End}(\mathcal{A})$ et on utilise enfin la méthode d'Eisenträger et Lauter [106, §6] pour déterminer $\mathrm{End}(\mathcal{A})$ localement en les nombres premiers où ces ordres peuvent différer. Cette approche est formalisée par l'algorithme suivant.

Algorithme 2.3.2 ([135, Alg. 6.2]).

ENTRÉE. *Une surface abélienne $\mathscr{A}/k$ ordinaire absolument simple.*

SORTIE. *Son anneau d'endomorphismes.*

1. *Calculer le polynôme caractéristique de son endomorphisme de* FROBENIUS.
2. *Factoriser son discriminant et en déduire $\mathcal{O} = \mathbb{Z}[\pi, \overline{\pi}]$.*
3. *Pour tout ordre minimal $\mathcal{O}' \supsetneq \mathcal{O}$:*
4. *Si $\mathrm{N}_\Phi(p_{\mathcal{O}}) \subset \Omega_{\mathrm{End}\,\mathscr{A}}$ affecter $\mathcal{O} \leftarrow \mathcal{O}'$ et retourner en 3.*
5. *Pour tout premier satisfaisant $\ell < 42$ ou $\ell \mid [\mathcal{O}_{K_0} : \mathbb{Z}[\pi + \overline{\pi}]]$:*
6. *Calculer l'ordre maximal $\mathcal{O}' \subset \mathrm{End}(\mathscr{A})$ vérifiant $[\mathcal{O}' : \mathbb{Z}[\pi, \overline{\pi}]] = \ell^\alpha$.*
7. *Affecter $\mathcal{O} \leftarrow \mathcal{O} + \mathcal{O}'$.*
8. *Renvoyer $\mathcal{O}$.*

L'algorithme de SCHOOF–PILA [36, 46] accompli l'étape 1 en temps polynomial en $\log(q)$. Celui de LENSTRA–POMERANCE [53] réalise l'étape 2 inconditionnellement en temps sous-exponentiel $L(q)^{\sqrt{6}+o(1)}$ pour $L(x) = \exp\sqrt{\log(x)\log(\log(x))}$. L'énumération des ordres de l'étape 3 s'effectue via les méthodes de [118, §3.2], [163, §3] et [153, Alg. 1]. L'étape 6 repose sur la méthode d'EISENTRÄGER et LAUTER [106, §6] dont la complexité est exponentielle en ℓ. Néanmoins, grâce aux travaux de la section 1.4, on peut démontrer le résultat suivant.

Proposition 2.3.3 ([135, Th. 7.1]). *Pour tout $\varepsilon > 0$, les puissances ℓ^α intervenant à l'étape 6 de l'algorithme 2.3.2 sont inférieures à $L(q)^\varepsilon$ pour presque toutes les variétés abéliennes $\mathscr{A}$.*

2.4 Groupes de classes via isogénies

L'étape 4 est le cœur de l'algorithme : on y exploite la théorie de la multiplication complexe et plus particulièrement le théorème 1.1.6 afin de ramener une question portant sur l'anneau d'endomorphismes à l'évaluation de simples isogénies. Pour ce faire, on construit dans un premier temps des idéaux friables de $p_{\mathcal{O}}$ via une technique à la BUCHMANN [43] avant, dans un second, temps de tester la condition $\mathrm{N}_\Phi(p_{\mathcal{O}}) \subset \Omega_{\mathrm{End}\,\mathscr{A}}$ proprement dite. Cela donne les deux algorithmes suivants.

Algorithme 2.4.1 ([135, Alg. 4.3]).

ENTRÉE. *Un ordre $\mathcal{O}$ de discriminant Δ d'un corps CM quartique.*

SORTIE. *Un idéal friable principal de $\mathcal{O}$.*

1. *Énumérer les premiers $\mathfrak{p}$ de $\mathcal{O}$ de norme au plus $L(\Delta)^\gamma$.*
2. *Choisir uniformément un idéal $\prod \mathfrak{p}^{x_\mathfrak{p}}$ avec $|x_\mathfrak{p}| < \log(\Delta)^{4+\varepsilon}$.*
3. *Calculer un représentant réduit $\mathfrak{a}$ de sa classe.*
4. *Si $\mathfrak{a}$ admet une factorisation $\prod \mathfrak{p}^{y_\mathfrak{p}}$:*
5. *Renvoyer l'idéal $\prod \mathfrak{p}^{x_\mathfrak{p} - y_\mathfrak{p}}$.*
6. *Retourner en 2.*

L'exposant γ considéré dans l'étape 1 a pour vocation à équilibrer le coût de construction des idéaux avec celui d'évaluation des isogénies correspondantes. Plus précisément, des résultats antérieurs [122, §6] montrent que l'étape 4 réussi avec probabilité $L(\Delta)^{-1/(4\gamma)+o(1)}$. La domination $\Delta = O(q^4)$ implique ainsi que la complexité de l'algorithme ci-dessus est de

$$L(q)^{\max\{2\gamma, 1/(2\gamma)\}+o(1)}$$

en temps probabiliste.

Algorithme 2.4.2 ([135, Alg. 5.1]).

ENTRÉE. *Une surface abélienne $\mathscr{A}$ et un ordre $\mathcal{O}$ contenant $\mathbb{Z}[\pi, \overline{\pi}]$.*

SORTIE. *La véracité de l'assertion $\mathrm{N}_\Phi(p_{\mathcal{O}}) \subset \Omega_{\mathrm{End}(\mathscr{A})}$.*

1. *Répéter $5g^2 \log_2(q)$ fois :*
2. *Calculer $\mathfrak{b} = \mathrm{N}_{\Phi^r}(\mathrm{N}_\Phi(\mathfrak{a}))$ pour $\mathfrak{a}$ obtenu par l'algorithme 2.4.1.*
3. *Calculer l'isogénie correspondante $\mathscr{A} \to \mathscr{A}/\bigcap_{\alpha\in\mathfrak{b}} \ker(\alpha)$.*
4. *Si son codomaine n'est pas isomorphe à $\mathscr{A}$, renvoyer* `faux`.
5. *Renvoyer* `vrai`.

L'évaluation de l'isogénie associée requiert $(\mathrm{N}\,\mathfrak{b})^{3+o(1)}$ opérations et une inégalité de convexité donne aisément $\mathrm{N}\,\mathfrak{b} \leqslant (\mathrm{N}\,\mathfrak{a})^4$. L'algorithme ci-dessus est donc de complexité $L(q)^{24\gamma+o(1)}$. On en déduit l'exposant optimal $\gamma = \sqrt{3}/12$. Ceci achève l'étape 4 et le résultat suivant en découle.

Théorème 2.4.3 ([135, Th. 7.2]). *L'algorithme 2.3.2 détermine l'anneau d'endomorphismes d'une surface abélienne ordinaire absolument simple en temps moyen $L(q)^{2\sqrt{3}+o(1)}$.*

Des records de calcul exploitant les techniques décrites ci-dessus ont été obtenus [135, §8] dans des cas hors de portée des méthodes précédemment connues : des calculs d'anneaux d'endomorphismes qui auraient auparavant nécessité un nombre d'opérations dépassant les 2^{90} sont réalisés par la présente méthode sur un ordinateur de bureau en quelques secondes seulement.

Notons enfin que, dans le cas particulier où la multiplication réelle est maximale, c'est-à-dire que l'anneau d'endomorphismes de $\mathscr{A}$ satisfait $\mathcal{O}_{K_0} \subset \mathrm{End}(\mathscr{A})$, et où le groupe de classes au sens restreint de l'anneau $\mathcal{O}_{K_0}$ est trivial, ces résultats ont depuis été renforcés même si la complexité asymptotique reste inchangée [155].

Chapitre 3

Applications aux corps finis

3.1 Revêtements exceptionnels

Soient X et Y deux variétés projectives absolument irréductibles définies sur un corps fini k. Un revêtement $X \to Y$ est dit exceptionnel s'il induit des isomorphismes $X(k') \to Y(k')$ pour une infinité d'extensions k' de k. Ces objets jouent un rôle important en géométrie arithmétique : ils permettent d'interpréter le théorème de l'image ouverte de Serre [27] ou encore de construire des relations entre certaines fonctions zêta [92].

Dans le cas le plus élémentaire où $X = Y = \mathbb{P}^1(k)$, la notion de revêtement exceptionnel est essentiellement équivalente à celle de fraction rationnelle de permutation [100] dont on rappelle la définition.

Définition 3.1.1. *Une fraction rationnelle $f \in k(x)$ sur un corps fini k est dite de permutation si elle induit une bijection de k dans lui-même.*

Le cas particulier des polynômes est l'objet de célèbres conjectures désormais démontrées.

Théorème 3.1.2 (conjecture de Carlitz [19, 55])**.** *Soit d un entier pair. Aucun corps fini de caractéristique impaire suffisamment grand n'admet de polynôme de permutation de degré d.*

Théorème 3.1.3 (conjecture de Schur [6, 25])**.** *Soit K un corps de nombre. Tout polynôme $f \in \mathcal{O}_K[x]$ induisant des permutations sur une infinité de corps résiduels est la composée de polynômes linéaires et de polynômes de Dickson.*

Les travaux d'extension de ces résultats à des contextes plus généraux, comme celui des fractions rationnelles ou encore des variétés X et Y arbitraires, sont à l'intersection de multiples domaines des mathématiques et font notamment intervenir la théorie de la multiplication complexe des courbes elliptiques [29, 59, 84].

Les fractions rationnelles de permutation jouent aussi un rôle clef en cryptographie, tout particulièrement dans le cas où X est une courbe elliptique et où Y est la droite projective : un revêtement exceptionnel $\mathscr{E} \to \mathbb{P}^1$ fournit alors une fonction de hachage vers la courbe elliptique. La construction de tels objets [110, 114] et son extension aux courbes de genre supérieur [115, 117, 128, 130] est délicate.

3.2 Construction de fractions rationnelles de permutation

Cette section décrit des travaux communs avec Mehdi Tibouchi [142, 147].

Notre contribution consiste en la description et l'analyse d'une procédure effective permettant, pour des degrés d et des corps finis k donnés, de construire de vastes familles de fractions rationnelles de permutation. Une implantation directe atteint les tailles cryptographique, telle $\log_2 |k| = 1023$. Cette procédure repose le résultat suivant.

Théorème 3.2.1 ([147, Th. 1]). *Soit $\varphi : \mathscr{E} \to \mathscr{E}'$ une isogénie de degré premier ℓ définie sur un corps fini k entre deux courbes elliptiques sous forme de Weierstrass ; notons $(u, v) \in \big(k(x)\big)^2$ l'unique couple vérifiant $\varphi\big((x, y)\big) = \big(u(x), y \cdot v(x)\big)$. Les assertions suivantes sont équivalentes :*

(i) La fraction rationnelle u n'a aucun pôle dans k.

(ii) Le noyau de φ est trivial sur l'extension quadratique de k.

(iii) Le revêtement $u : \mathbb{P}^1 \to \mathbb{P}^1$ est exceptionnel.

Autrement dit, étant donné un point P d'ordre premier ℓ sur une courbe elliptique $\mathscr{E}$ définie sur un corps fini k, si le sous-groupe $\langle P \rangle$ est rationnel mais qu'aucun de ses points n'est défini sur l'extension quadratique, alors la fraction rationnelle u est de permutation.

Par cyclicité, aucun point du sous-groupe $\langle P \rangle$ n'est défini sur l'extension quadratique si et seulement si P lui-même ne l'est pas. Reste à exhiber un critère efficace pour déterminer si le sous-groupe $\langle P \rangle$ est rationnel.

Lemme 3.2.2 ([147, Lem. 1]). *Soit P un point d'ordre premier ℓ d'une courbe elliptique $\mathscr{E}$ sous forme de Weierstrass définie sur un corps fini k. Soit τ un entier dont l'ordre dans $\mathbb{F}_\ell^\times/\{\pm 1\}$ est exactement le degré de l'extension $k(x(P))/k$. Le sous-groupe $\langle P \rangle$ est rationnel si et seulement si $x(P)$ et $x([\tau]P)$ sont conjugués par l'action du groupe de Galois.*

Afin de traduire ce critère concrètement, rappelons que la multiplication par l'entier $\sigma \geqslant 2$ sur la courbe elliptique $\mathscr{E}$ s'écrit explicitement

$$P = (x, y) \longmapsto [\sigma]P = \left(\frac{\phi_\sigma(x)}{\psi_\sigma(x)^2}, \frac{\omega_\sigma(x, y)}{\psi_\sigma(x)^3} \right)$$

et le polynôme de division $\psi_\sigma(x)$ a donc pour racines les premières coordonnées des points de $\mathscr{E}[\sigma]$. Soit $P \in \mathscr{E}[\ell]$ et soit $f(x)$ le facteur irréductible de $\psi_\ell(x)$ dont $x(P)$ est racine. D'après le lemme, le sous-groupe $\langle P \rangle$ est rationnel si et seulement si

$$f\left(\frac{\phi_\tau(x)}{\psi_\tau(x)^2} \right) = 0 \bmod f(x).$$

Le polynôme ayant pour racines les premières coordonnées des points de $\langle P \rangle$ est alors

$$g_\ell\big(f(x)\big) = \prod_\rho \operatorname{pgcd}\Big(\psi_\ell(x), \operatorname{res}_y\big(f(y), \psi_\rho(x) - \psi_\rho(x)^2 y\big) \Big).$$

où ρ parcours $\mathbb{F}_\ell^\times/\{\pm 1\}/\mu_{\deg(f)}$. On obtient ainsi l'algorithme suivant.

Algorithme 3.2.3 ([147, Alg. 1]).

ENTRÉE. *Une courbe elliptique $\mathscr{E}/k$ avec $|k| = p^\alpha$ où $p > 3$ et un premier $\ell \neq 2, 3, p$.*

SORTIE. *Les polynômes de noyau des isogénies vérifiant les assertions du théorème 3.2.1.*

1. *Déterminer un générateur ω de $\mathbb{F}_\ell^\star$.*
2. *Pour tout diviseur $d > 1$ de $\frac{\ell-1}{2}$:*
3. *Calculer $\tau = \omega^{\frac{\ell-1}{2d}}$.*
4. *Pour tout diviseur $f(x)$ de degré d de $\psi_\ell(x)$:*
5. *Si $f\left(\phi_\tau(x)/\psi_\tau(x)^2\right) = 0 \bmod f(x)$:*
6. *Calculer puis afficher $g_\ell\big(f(x)\big)$.*

Des techniques arithmétiques et algorithmiques classiques, pour lesquelles nous renvoyons à l'article original, permettent de réaliser efficacement chaque étape de calcul et notamment de ne pas reparcourir à l'étape 4 les facteurs des polynômes $g_\ell\big(f(x)\big)$ déjà calculés à l'étape 6. En découle le résultat suivant.

Théorème 3.2.4 ([147, Th. 1]). *L'algorithme 3.2.3 est de complexité probabiliste $\tilde{O}\left(\ell^{4+\varepsilon}(\log|k|^2)\right)$.*

Afin d'obtenir des revêtements exceptionnels, il ne reste plus qu'à sélectionner des courbes elliptiques $\mathscr{E}/k$ convenables puis de déduire des polynômes de noyau renvoyés par l'algorithme 3.2.3 les isogénies correspondantes.

Algorithme 3.2.5 ([147, Alg. 2]).

ENTRÉE. *Un corps k fini de caractéristique $p > 3$ et un premier $\ell \neq 2, 3, p$.*

SORTIE. *Des fractions rationnelles de permutation de degré ℓ sur k.*

1. *Calculer la réduction du polynôme modulaire $\Phi_\ell(X, Y) \in k[X, Y]$.*
2. *Tirer uniformément un élément $j \in k$.*
3. *Si $\Phi_\ell(X, j)$ n'a aucune racine, retourner en 2.*
4. *Soit $\mathscr{E}/k$ une courbe elliptique d'invariant j.*
5. *Pour tout polynôme affiché par l'algorithme 3.2.3 :*
6. *Calculer l'isogénie correspondante et afficher sa fraction rationnelle u.*

À l'étape 3, la probabilité de ne pas retourner à l'étape 2 est celle, pour la courbe elliptique $\mathscr{E}$, d'admettre une ℓ-isogénie rationnelle. Pour $|k| \to \infty$, cette courbe est presque sûrement ordinaire. Son graphe de ℓ-isogénies est alors non trivial si ℓ est décomposé dans $\mathbb{Q} \otimes \mathrm{End}(\mathscr{E})$, autrement dit, si $\Delta(\mathscr{E})$ est un carré non nul modulo ℓ, ce qui est le cas avec probabilité $\frac{\ell-1}{2\ell}$ sous heuristique.

La probabilité pour l'algorithme 3.2.3 d'afficher au moins un polynôme est minorée par celle, pour une ℓ-isogénie rationnelle, de n'admettre aucun point rationnel dans son noyau. Le revêtement des courbes modulaires $X_1(\ell) \to X_0(\ell)$ étant galoisien cyclique de degré $\frac{\ell-1}{2}$, le théorème de densité de Chebotarev [1, 7] montre que l'image de $X_1(\ell)(k) \to X_0(\ell)(k)$ est de densité $\frac{2}{\ell-1} + O(|k|^{-1/2})$. La probabilité considérée est donc asymptotiquement minorée par $1 - \frac{2}{\ell-1}$. On en déduit que les complexités asymptotique des algorithmes 3.2.3 et 3.2.5 sont identiques.

Théorème 3.2.6 ([147, Th. 2]). *Sous heuristique, l'algorithme 3.2.5 est de complexité probabiliste $\tilde{O}\left(\ell^{4+\varepsilon}(\log|k|)^2\right)$.*

Une implantation directe de ces algorithmes permet de construire, en quelques secondes seulement sur une machine de bureau, des fractions rationnelles de permutation sur des corps de taille cryptographique, tel $\log_2 |k| = 1023$.

3.3 Présentations itérées de corps finis

Soit $S \in \mathbb{Q}(x)$ une fraction rationnelle. Pour tout corps fini k où S admet bonne réduction, considérons la transformation, introduite par Cohen [23], définie par

$$T_S : \begin{cases} k[x] \longrightarrow k[x] \\ f(x) \longmapsto \text{numérateur}\big(f(S(x))\big) \end{cases}$$

et, pour tout $i \in \mathbb{N}$, notons $T_S^i = T_S \circ \cdots \circ T_S$ la composition de i copies de T_S.

Pour certains couples (S, f), les polynômes $T_S^i(f)$ sont tous irréductibles et définissent ainsi une tour d'extensions de k. Plus précisément, posons $d = \deg(f)$ et $e = \deg(S)$, cette dernière quantité désignant le maximum des degrés du numérateur et du dénominateur de la fraction rationnelle réduite S. Alors, le degré de $T_S^i(f)$ étant $d\,e^i$, ces polynômes induisent une présentation itérée [42] du corps

$$k^{[d\,e^\infty]} = \bigcup_{i=0}^{\infty} k^{[d\,e^i]}$$

où l'on dénote par $k^{[\ell]}$ l'extension de degré ℓ du corps fini k. Des extensions algébriques de la forme $k^{[d\,e^\infty]}$ ont été étudiées par Steinitz [3] dans l'objectif de décrire les clotures algébriques des corps finis.

Définition 3.3.1. *On dit qu'un couple $(S, f) \in \mathbb{Q}(x) \times k[x]$ induit une présentation itérée lorsque les polynômes $T_S^i(f)$ sont irréductibles pour tout $i \in \mathbb{N}$.*

Notre objectif est ici de caractériser de tels couples. Deux cas particuliers bien connus de la littérature concernent les fractions rationnelles

$$Q(x) = \frac{x^2+1}{x} \qquad \text{et} \qquad R(x) = \frac{x^2+1}{2x};$$

en effet, des approches *ad hoc* ont permis d'obtenir les résultats suivants.

Théorème 3.3.2 ([34, 45, 85])**.** *Soient k un corps fini de caractéristique paire et $f \in k[x]$ un polynôme unitaire irréductible de coefficients $(a_\ell)_{\ell=0}^n$. Si $\mathrm{tr}(a_{n-1}) = \mathrm{tr}(a_1/a_0) = 1$ où tr dénote la trace de $k/\mathbb{F}_2$, alors tous les polynômes $T_Q^i(f)$ sont irréductibles.*

Théorème 3.3.3 ([52])**.** *Soient k un corps fini de caractéristique impaire et $f \in k[x]$ un polynôme unitaire irréductible. Pour $|k| = 3 \bmod 4$, on suppose de plus $\deg(f)$ pair. Si $f(1)f(-1)$ n'est pas un carré dans k alors tous les polynômes $T_R^i(f)$ sont irréductibles.*

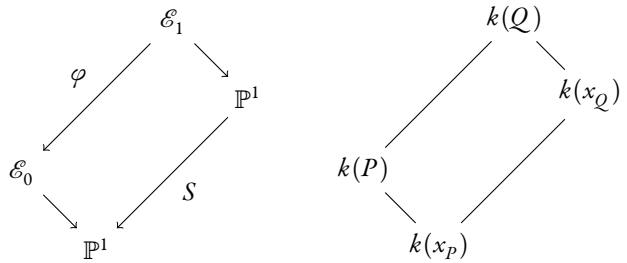
Plus récemment, le cas des fractions rationnelles de degré deux a fait l'objet d'études exhaustives [87, 96] et d'autres approches exploitant notamment la théorie de Galois des corps de fonctions ont permis d'étendre ces résultats et d'en obtenir quelques extensions [151, 166].

3.4 Construction de présentations itérées

Cette section décrit des travaux communs avec Alp Bassa et Roger Oyono [174].

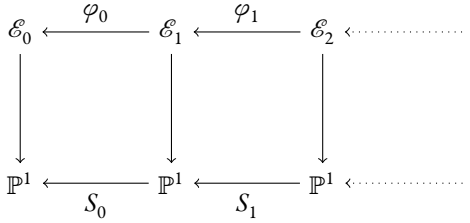
Nous caractérisons ici plusieurs familles de couples (S, f) induisant des présentations itérées. Cette caractérisation repose sur les isogénies des courbes elliptiques et plus particulièrement sur les propriétés galoisiennes de leur corps de définition.

Soit $\mathscr{E}_0 \xleftarrow{\varphi} \mathscr{E}_1$ une isogénie de courbes elliptiques sous forme de Weierstrass définie sur un corps fini k ; notons $S \in k(x)$ la fraction rationnelle qui en donne l'action sur la première coordonnée. Soient aussi $P \in \mathscr{E}_0(\overline{k})$ et $Q \in \varphi^{-1}(P)$ deux points ; leur première coordonnée satisfont ainsi $x_P = S(x_Q)$. Désignant par $f \in k[x]$ le polynôme minimal de x_P alors on obtient $f(S(x_Q)) = 0$, ce qui montre que le polynôme $T_S(f)$ est annulateur de x_Q. Il en est le polynôme minimal, donc irréductible, si son degré est précisément le bon, c'est-à-dire si on a l'égalité $[k(x_Q) : k(x_P)] = \deg(\varphi)$. Les diagrammes ci-dessous, commutatif à gauche et d'extensions de corps à droite, résument cette situation.



On observe que, lorsque le degré de l'isogénie φ est impair ou lorsque celui de l'extension $k(P)/k(x_P)$ est pair, alors l'hypothèse $[k(Q) : k(P)] = \deg(\varphi)$ ressort indemne par projection sur la première coordonnée et l'on a $\big[k(x_Q) : k(x_P)\big] = \deg(\varphi)$. Dans ce cas, le polynôme $T_S(f)$ est irréductible.

Afin d'itérer cette construction comme l'indique le diagramme commutatif ci-dessous, il s'agit d'obtenir un critère explicite garantissant que la condition $[k(Q) : k(P)] = \deg(\varphi)$ est préservée par composition avec φ.



Pour ce faire, montrons d'abord un résultat simple mais indispensable.

Lemme 3.4.1 ([174, Lem. 2.1]). *Soit $\mathscr{E}_0 \xleftarrow{\varphi} \mathscr{E}_1$ une isogénie séparable définie sur un corps fini k. Fixons un point $P \in \mathscr{E}_0(\overline{k})$. On suppose que tous les points du noyau $\ker(\varphi)$ sont $k(P)$-rationnels et on note π le $k(P)$-Frobenius de $\mathscr{E}_0$. Il existe un point $F \in \ker(\varphi)$ pour lequel tout point $Q \in \varphi^{-1}(P)$ vérifie $\pi^n(Q) = Q + nF$ quel que soit $n \in \mathbb{N}$.*

On en déduit le résultat suivant qui donne précisément le critère recherché.

Théorème 3.4.2 ([174, Th. 2.2]). *Soient $\mathscr{E}_0 \xleftarrow{\varphi_0} \mathscr{E}_1 \xleftarrow{\varphi_1} \mathscr{E}_2$ deux isogénies séparables de degrés respectifs ℓ_0 et ℓ_1 définies sur un corps fini k. Supposons que tous les facteurs premiers de ℓ_1 divisent ℓ_0. Supposons aussi que le noyau de la composée* $\ker(\varphi_0 \circ \varphi_1)$ *est cyclique et que tous ses points sont définis sur l'extension $k(P)$ pour un certain point $P \in \mathscr{E}_0(\overline{k})$. Alors, tous les points $Q \in (\varphi_0 \circ \varphi_1)^{-1}(P)$ vérifiant $[k(\varphi_1(Q)) : k(P)] = \ell_0$ vérifient aussi $[k(Q) : k(P)] = \ell_0\ell_1$.*

Ce résultat est particulièrement propice aux itérations lorsque les courbes elliptiques $\mathscr{E}_0 = \mathscr{E}_1 = \mathscr{E}_2$ sont identiques et que les endomorphismes $\varphi_0 = \varphi_1$ le sont aussi. On supposera dorénavant, afin de simplifier l'exposition, que cet endomorphisme est de degré impair. On obtient alors le résultat suivant.

Corollaire 3.4.3 ([174, Cor. 2.3]). *Soit $\mathscr{E}$ une courbe elliptique sous forme de Weierstrass, $\varphi : \mathscr{E} \to \mathscr{E}$ un endomorphisme séparable de degré impair défini sur un corps fini k et $P \in \mathscr{E}(\overline{k})$ un point. Supposons le sous-groupe* $\ker(\varphi \circ \varphi)$ *cyclique et tous ses points $k(P)$-rationnels. Notons S la fraction rationnelle donnant l'action de φ sur la première coordonnée et notons f le polynôme minimal de x_P sur k. Alors, si $T_S(f)$ est irréductible, tous les polynômes $T_S^i(f)$ le sont aussi ; le couple (S, f) induit ainsi une présentation itérée.*

Les fractions rationnelles ainsi obtenues d'endomorphismes $\varphi : \mathscr{E} \to \mathscr{E}$ par projection sur la première coordonnée et, plus généralement, par projection via un revêtement fini séparable $\mathscr{E} \to \mathbb{P}^1$, sont appelées fonctions de Lattès [5]. Notons par ailleurs que, dans le cas d'endomorphismes de degré premier, la condition de cyclicité sur $\ker(\varphi \circ \varphi)$ équivaut à ce que φ ne soit pas son propre dual.

Nos efforts se concentreront désormais sur la recherche d'endomorphismes satisfaisant les hypothèses de ce corollaire et ignorerons sciemment les points P pouvant y être associés : pour chaque endomorphisme identifiée, on se contentera, dans un premier temps, de savoir qu'un tel P existe ; dans un second temps, on évaluera la densité des polynômes irréductibles f concernés.

Remarquons enfin qu'étant donnée une homographie $h(x) = \frac{ax+b}{cx+d}$ avec $ad - bc \neq 0$, le couple (S, f) induit une présentation itérée si et seulement si c'est aussi le cas du couple $(h^{-1} \circ S \circ h, f)$. Ainsi, pour chaque isogénie φ identifiée, nous sélectionnerons et n'afficherons que le représentant de poids de Hamming le plus faible de la classe de conjugaison de S par les homographies.

Endomorphisme de Verschiebung. Soit $\mathscr{E}$ une courbe elliptique ordinaire définie sur un corps fini k. Son endomorphisme de Verschiebung $\widehat{\pi}$ est une isogénie séparable de degré $|k|$. Elle satisfait les conditions du théorème. Pour les petits corps finis, on énumère les courbes elliptiques ordinaires et calcule leurs endomorphismes de Verschiebung. On obtient ainsi la table 3.1 dont chaque fraction rationnelle S induit une présentation itérée pour une densité positive des polynômes irréductibles $f \in k[x]$.

Cycles d'isogénies horizontales. Restreignons nous à présent aux endomorphismes de degré premier avec la caractéristique ; ce ne sont autre que les cycles du graphe des isogénies de degré premier. La condition de cyclicité du noyau du carré impose que ces cycles ne contiennent pas simultanément une arête et sa duale. Pour les courbes ordinaires, on déduit de la structure explicite de ce graphe que les endomorphismes s'obtiennent par composition d'isogénies horizontales « au sommet du volcan ».

Considérons d'abord les endomorphismes de degré premier, c'est-à-dire les cycles de longueur un ou encore les boucles du graphe. Notant K le corps CM de la courbe $\mathscr{E}$, ces endomorphisme $\mathscr{E} \to \mathscr{E}$ correspondent, via la théorie de la multiplication complexe, aux idéaux premiers principaux de l'anneau $\mathcal{O}_K$. Tout tel idéal $\mathfrak{a}$ de norme ℓ induit une isogénie $\varphi_\mathfrak{a} : \mathscr{E} \to \mathscr{E}$.

q	S
3	$(x^3+x^2+x+2)/x^2$
5	$(2x^5+x)/(x^4+2)$
7	$(5x^7+x^4+6x)/(x^6+x^3+3)$
11	$(8x^{11}+x^9+7x^7+4x^3+10x)/(x^{10}+x^8+2x^4+7x^2+8)$

TABLE 3.1 – Pour le corps fini de cardinal q, la fraction rationnelle S est un représentant, sous l'action des homographies, des fonctions de LATTÈS déduites d'endomorphismes de Verschiebung de courbes elliptiques ordinaires.

q	ℓ	S
2	3	$(x^3+1)/x^2$
5	3	$x/(x^3+x^2+1)$
7	5	$(x^5+x^4+x^3+6x^2+x)/(x^4+x^3+4x^2+x+1)$
11	2	$x/(x^2+1)$
11	5	$(x^5+9x^4+10x^3+4x+1)/(x^5+x^3+9)$
17	5	$(15x^5+3x^3+x)/(x^5+3x^4+15x^3+x^2+1)$

TABLE 3.2 – Pour le corps fini de cardinal q, la fraction rationnelle S est un représentant, sous l'action des homographies, des fonctions de LATTÈS déduites d'endomorphismes de degré ℓ de courbes elliptiques ordinaires.

Pour en déduire des présentations itérées, on sélectionne de petits discriminants Δ puis on construit par la méthode CM des courbes elliptiques $\mathscr{E}$ dont l'anneau d'endomorphismes $\mathrm{End}(\mathscr{E})$ est exactement l'anneau des entiers $\mathcal{O}_K$ du corps quadratique imaginaire $K=\mathbb{Q}(\sqrt{\Delta})$. On calcule alors les isogénies de domaine $\mathscr{E}$ dont le degré ℓ est premier et décomposé comme produit de deux idéaux principaux dans $\mathrm{cl}(\mathcal{O}_K)$. Cela donne la table 3.2.

Considérons maintenant le cas plus général de cycles construits comme composition d'isogénies de multiples degrés premiers. Ceci correspond, via la théorie de la multiplication complexe, à la recherche de produits principaux d'idéaux premiers dans le groupe de classes de l'anneau d'endomorphismes. De telles constructions présentent toutefois le défaut d'accroître le degré de la fraction rationnelle S et donc de diminuer la densité de la présentation itérée. Nous renvoyons le lecteur à l'article original [174] pour davantage de précisions ainsi que pour d'autres constructions.

Construction en caractéristique nulle. Soit φ un endomorphisme de degré ℓ d'une courbe elliptique $\mathscr{E}$ définie sur un corps de nombres K. La fonction de LATTÈS qui s'en déduit par projection sur la première coordonnée, $S\in K(x)$, satisfait alors les conditions du corollaire 3.4.3 pour tous les corps résiduels k de K où elle admet bonne réduction.

Ces endomorphismes s'énumèrent aisément, les classes d'isomorphismes des courbes elliptiques $\mathscr{E}$ concernées correspondant aux racines du polynôme modulaire $\Phi_\ell(X,X)\in K[X]$. Par exemple, pour $K=\mathbb{Q}$ et $\ell=2$, on obtient le résultat classique suivant.

Proposition 3.4.4 ([60, Prop. 2.3.1]). *Seules trois classes d'isomorphismes de courbes elliptiques sur $\mathbb{Q}$ possèdent un endomorphisme de degré deux. Elles admettent pour représentants :*

$$\begin{aligned}
&\text{(i)} \quad E : y^2 = x^3 + x, \qquad j = 1728, \qquad \alpha = 1 + \sqrt{-1},\\
&\qquad [\alpha](x,y) = \left(\alpha^{-2}\left(x + \frac{1}{x}\right), \alpha^{-3} y \left(1 - \frac{1}{x^2}\right)\right);\\
&\text{(ii)} \quad E : y^2 = x^3 + 4x^2 + 2x, \quad j = 8000, \qquad \alpha = \sqrt{-2},\\
&\qquad [\alpha](x,y) = \left(\alpha^{-2}\left(x + 4 + \frac{2}{x}\right), \alpha^{-3} y \left(1 - \frac{2}{x^2}\right)\right);\\
&\text{(iii)} \quad E : y^2 = x^3 - 35x + 98, \quad j = -3375, \quad \alpha = \frac{1 + \sqrt{-7}}{2},\\
&\qquad [\alpha](x,y) = \left(\alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x + \alpha^2 - 2}\right), \alpha^{-3} y \left(1 + \frac{7(1-\alpha)^4}{(x + \alpha^2 - 2)^2}\right)\right).
\end{aligned}$$

Remarquons notamment que la fonction de Lattès déduite de l'endomorphisme (i) de la proposition ci-dessus n'est autre que la fraction rationnelle $Q(x)$ du théorème 3.3.2 ; on en déduit une extension de ce résultat aux corps finis de caractéristique impaire.

Densité des présentations itérées. Pour chaque fraction rationnelle S nous calculons la densité des polynômes irréductibles f de degré d sur le corps à q éléments pour lesquels le couple (S, f) induit une présentation itérée. Cela donne notamment la table 3.3. Noter que le théorème de densité de Chebotarev [1, 7] permet, grâce au corollaire 3.4.3, de calculer explicitement les densités asymptotiques des colonnes de cette table.

$S = \frac{x^2}{x+1}$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=2$	0	0	0	0	0
$q=3$	1/3	1/4	5/18	1/4	15/58
$q=5$	3/10	1/4	13/50	1/4	≈ 0.25
$q=7$	0	1/14	1/14	≈ 0.06	≈ 0.06
$q=11$	3/55	≈ 0.06	≈ 0.06	≈ 0.06	≈ 0.06
$q=13$	3/26	≈ 0.13	≈ 0.13	≈ 0.12	≈ 0.13

$S = \frac{x^2+1}{x}$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=2$	1	0	1/3	1/3	2/9
$q=3$	2/3	0	5/9	0	15/29
$q=5$	0	0	0	0	0
$q=7$	8/21	0	12/49	0	≈ 0.25
$q=11$	8/55	≈ 0.12	≈ 0.13	≈ 0.12	≈ 0.12
$q=13$	2/13	11/91	≈ 0.13	≈ 0.13	≈ 0.13

$S = \frac{1}{2}\frac{x^2+1}{x}$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=3$	2/3	0	5/9	0	15/29
$q=5$	3/5	1/2	13/25	1/2	≈ 0.50
$q=7$	4/7	0	25/49	0	≈ 0.50
$q=11$	6/11	0	≈ 0.50	0	≈ 0.50
$q=13$	7/13	1/2	≈ 0.50	1/2	≈ 0.50
$q=17$	9/17	1/2	≈ 0.50	1/2	≈ 0.50

$S = \alpha^{-2}\left(x - \frac{7(1-\alpha)^4}{x+\alpha^2-2}\right)$	$d=2$	$d=3$	$d=4$	$d=5$	$d=6$
$q=11$	16/55	13/55	≈ 0.26	≈ 0.25	≈ 0.25
$q=23$	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=29$	8/29	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=37$	≈ 0.26	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=43$	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25
$q=53$	≈ 0.26	≈ 0.25	≈ 0.25	≈ 0.25	≈ 0.25

TABLE 3.3 – Pour certaines fractions rationnelles S, densités des polynômes irréductibles f de degré d sur le corps à q éléments pour lesquels le couple (S, f) induit une présentation itérée.

Chapitre 4

Théorie de l'information

4.1 Minimisation du risque empirique

Soit une famille d'algorithmes $f_\theta : X \to Y$ paramétrée par une variable $\theta \in \mathscr{M} \subset \mathbb{R}^d$. Fixons aussi une fonction symétrique séparable $\ell : Y^2 \to \mathbb{R}_+$ et une partie finie $Z \subset X \times Y$. La déviation des algorithmes par rapport au jeu de données Z est quantifiée par le risque empirique

$$L : \theta \in \mathscr{M} \longmapsto \frac{1}{|Z|} \sum_{(x,y)\in Z} \ell\big(f_\theta(x), y\big).$$

La minimisation du risque empirique (ERM) est un problème central en apprentissage supervisé [51]. Attaquons-le, non pas de front en recherchant $\theta \in \mathscr{M}$ en terme absolu, mais de côté en sélectionnant $\theta \in \mathscr{M}$ suivant une mesure de probabilité P ; l'espérance du risque empirique est alors

$$R : P \in \Delta \longmapsto \int L(\theta)\, d\,P(\theta)$$

où Δ dénote l'ensemble des mesures de probabilité sur la tribu borélienne de $\mathscr{M}$ et où on suppose implicitement L mesurable. Pour limiter les phénomènes de surajustement et obtenir de bonnes garanties en généralisation, le problème consistant à minimiser R est typiquement régularisé par l'entropie relative à une mesure Q dite de référence ou *a priori*.

Problème 4.1.1 (ERM-RER). *Étant donnés une mesure $Q \in \Delta$ et un réel $\lambda \in \mathbb{R}_+^\star$ déterminer une mesure $P \in \Delta$ absolument continue par rapport à Q minimisant la quantité*

$$R(P) + \lambda D(P\|Q).$$

Rappelons que l'entropie relative, aussi connue sous le nom de divergence de Kullback–Leibler [11], d'une mesure P absolument continue par rapport à une mesure Q est

$$D(P\|Q) = \int \frac{d\,P}{d\,Q}(\theta) \log\left(\frac{d\,P}{d\,Q}(\theta)\right) d\,\theta$$

où $\frac{d\,P}{d\,Q}$ dénote la dérivée de Radon–Nikodym [8].

Le problème ERM-RER tel qu'énoncé ci-dessus intervient naturellement en apprentissage supervisé [89] mais aussi en physique statistique [95, 140], en théorie des jeux [90, Chap. 6] ainsi qu'en théorie de l'information [97]. Il s'apparente à deux variantes distinctes : lorsque la mesure de référence Q est une mesure de comptage, on parle de régularisation par entropie discrète et, lorsque c'est la mesure de Lebesgue, on parle de régularisation par entropie différentielle.

4.2 Généralisation aux mesures σ-finies

Cette section décrit des travaux communs avec Samir Perlaza, Iñaki Esnaola, Alain Jean-Marie et Stefano Rini [164, 171].

Le problème ERM-RER est ici généralisé aux mesures de référence σ-finies, unifiant ainsi les trois théories existantes concernant le cas des mesures de probabilité, des mesures de comptage et de la mesure de Lebesgue. Notons Δ^σ l'ensemble des mesures σ-finies sur la tribu borélienne de $\mathscr{M}$ et désignons toujours par Δ sa partie formée des mesures de probabilité.

Problème 4.2.1 (ERM-RER). *Étant donnés une mesure $Q \in \Delta^\sigma$ et un réel $\lambda \in \mathbb{R}_+^\star$ déterminer une mesure $P \in \Delta$ absolument continue par rapport à Q minimisant la quantité*

$$R(P) + \lambda D(P\|Q).$$

Nous conservons délibérément l'appellation ERM-RER pour cette version généralisée du problème 4.1.1. La théorie complète fait l'objet du rapport [164] ; seuls ses aspects particulièrement originaux vis-à-vis des trois spécialisations déjà connues ont été publiés [171]. Montrons tout d'abord que ce problème admet une unique solution sous la forme d'une mesure de Gibbs.

Théorème 4.2.2 ([164, Th. 3.1]). *Soit $\lambda \in \mathbb{R}_+^\star$ et soit $Q \in \Delta^\sigma$ une mesure par rapport à laquelle la fonction*

$$K(\lambda) : \theta \in \mathscr{M} \longmapsto \exp\left(-\frac{1}{\lambda} L(\theta)\right)$$

est intégrable. Le problème ERM-RER admet comme une unique solution la mesure P_Q^λ vérifiant

$$\frac{dP_Q^\lambda}{dQ}(\theta) = \frac{K(\lambda)(\theta)}{\int K(\lambda)(\upsilon) dQ(\upsilon)}$$

pour tout θ dans le support de Q.

Les réels λ pour lesquels $K(\lambda)$ est intégrable forment un intervalle $]0, \alpha[$ qui n'est autre que $\mathbb{R}_+^\star$ dans le cas particulier où Q est une mesure de probabilité. Si $\alpha = \infty$, pour $\lambda \to \infty$, la mesure P_Q^λ converge fortement vers la mesure de référence Q, ce qui est attendu, le terme de régularisation du problème ERM-RER devenant alors prépondérant. La situation est plus intéressante en $\lambda \to 0$: considérons le risque infimum des parties non négligeables

$$\delta_Q = \inf\left\{\lambda \in \mathbb{R}_+^\star : Q\left(L^{-1}([0,\lambda])\right) > 0\right\}.$$

Proposition 4.2.3 ([164, Lem. 3.6–10]). *Lorsque $\lambda \to 0$, la mesure optimale P_Q^λ se concentre sur la partie $\mathscr{L} = L^{-1}(\delta_Q)$. Plus précisément, si $\mathscr{L}$ est non négligeable, alors P_Q^λ converge fortement vers*

$$\frac{\mathbb{1}_{\mathscr{L}} \cdot Q}{Q(\mathscr{L})}.$$

Notons que le cas des mesures de référence Q dites cohérentes, c'est-à-dire vérifiant $\delta_Q = 0$, est d'intérêt particulier car l'ensemble limite $\mathscr{L}$ est alors exactement celui minimisant le risque empirique sans régularisation.

Afin d'évaluer la performance dans le cas moyen d'algorithmes sélectionnés suivant la mesure optimale P_Q^λ, on introduit la partie

$$\mathscr{N}_Q(\lambda) = \left\{\theta \in \mathscr{M} : L(\theta) \leqslant R\left(P_Q^\lambda\right)\right\}$$

pour laquelle on obtient le résultat suivant.

Théorème 4.2.4 ([164, Th. 7.1–3]). *La fonction $\mathscr{N}_Q : \mathbb{R}_+^\star \to \mathfrak{P}(\mathscr{M})$ est croissante et, en $\lambda \to 0$, sa mesure satisfait*

$$P_Q^\lambda\left(\mathscr{N}_Q(\lambda)\right) \to 1.$$

De manière plus surprenante, nous parvenons à démontrer rigoureusement une hypothèse qui était souvent admise comme heuristique dans les travaux antérieurs, y compris dans le cas où Q est une mesure de probabilité.

Théorème 4.2.5 ([164, §8]). *Soit Θ une variable aléatoire induisant la mesure P_Q^λ. Son risque empirique $L(\Theta)$ est une variable aléatoire sous gaussienne.*

Ce type de résultats possède notamment d'importantes conséquences théoriques [145].

Mentionnons enfin un résultat fort, stipulant que la sélection d'algorithmes suivant la probabilité P_Q^λ offre une garantie de type PAC [33] pour le problème sans régularisation, instanciée par le théorème suivant. Aucun résultat de ce type n'était auparavant paru dans la littérature, y compris lorsque la mesure de référence est supposée être une mesure de probabilité.

Théorème 4.2.6 ([164, Th. 9.1]). *Pour tout $\delta > \delta_Q$ et tout $\varepsilon \in]0,1[$, il existe un réel λ pour lequel*

$$P_Q^\lambda\left(L^{-1}([0,\delta])\right) > 1 - \varepsilon.$$

Tous ces travaux étendent et renforcent simultanément les résultats précédemment limités aux spécialisations du problème ERM-RER dans le cas où la mesure de référence est une mesure de probabilité, une mesure de comptage ou la mesure de Lebesgue.

Perspectives et projets de recherche

Aspects effectifs des surfaces abéliennes

Le développement des aspects effectifs des courbes elliptiques, initié dans les années 1980, a largement porté ses fruits, tant en ce qui concerne les retombées en mathématiques fondamentales, que les avancées en théorie algorithmique des nombres ou encore les applications en cryptographie. Comparativement, l'extension de ces travaux à la classe plus générale d'objets mathématiques que sont les variétés abéliennes reste limitée aujourd'hui encore.

Le premier volet de ce programme de recherche vise à réduire le fossé qui s'est creusé entre l'état de l'art des variétés abéliennes et celui des courbes elliptiques concernant leurs aspects effectifs. Pour ce faire, nous proposons trois objectifs visant chacun à attaquer un problème précis et sélectionnés pour leur potentiel en termes d'impact, de retombées et d'applications concrètes.

Structures algébriques sous-jacentes. Ce premier objectif consiste à développer des outils algébriques adaptés à l'étude et à l'analyse des variétés abéliennes. Explicitons trois directions de recherche particulièrement porteuses.

L'un des obstacles entravant une bonne maîtrise des graphes d'isogénies réside en la complexité de la structure du treillis des ordres des corps CM : ces treillis sont localement linéaire lorsque la multiplication réelle est maximale, ce qui est notamment le cas en dimension un et explique en partie les avancées dans ce cadre. Une meilleure représentation de ces ordres, empruntant par exemple les techniques de Bhargava [91], permettrait de décrire plus explicitement leur treillis. Une application très concrète serait la conception d'un algorithme de complexité polynomiale permettant, étant donné un ordre $\mathcal{O}$, d'énumérer les ordres $\mathcal{O}'$ immédiatement au dessus de $\mathcal{O}$ en un premier donné ℓ, c'est-à-dire vérifiant $[\mathcal{O}' : \mathcal{O}] \in \{\ell, \ell^2, \dots, \ell^{2g-1}\}$ et tels qu'aucun ordre intermédiaire ne soit inclus entre $\mathcal{O}$ et $\mathcal{O}'$.

Parallèlement à l'obtention de telles représentations, une étude fine des propriétés arithmétiques de l'indice $[\mathrm{End}(\mathcal{A}) : \mathbb{Z}[\pi, \overline{\pi}]]$ et du groupe $\mathfrak{C}(\mathcal{O})$ serait pertinente. Cela généraliserait les travaux de Cohen et Lenstra pour les groupes de classes [31] et permettrait une compréhension ne serait-ce que heuristique de ces objets. Une application directe serait notamment l'obtention de meilleures bornes de complexité pour de nombreux algorithmes exploitant ces objets dans le cadre de la théorie de la multiplication complexe en dimension supérieure ou égale à deux.

Enfin, l'analyse du groupe de classes polarisé entamée pourrait être davantage poussée afin d'en déduire une extension du célèbre résultat de Jao, Miller et Venkatesan [111] concernant les propriétés de mixité des graphes d'isogénies des courbes elliptiques ordinaires. En découlerait directement des résultats sur la difficulté du problème du logarithme discret, notamment une réduction du type cas le pire vers cas moyen.

Structure du graphe d'isogénies. Le graphe d'isogénies représente un enjeu tout particulier de par sa pertinence en cryptographie et sa situation au centre de divers théories mathématiques. On envisage deux approches afin de parfaire sa maîtrise.

La première viserait à décrire explicitement les composantes verticales des graphes d'isogénies en terme d'opérateurs de Hecke. Un travail a été débutté dans ce sens [146] mais reste encore inachevé. Une application directe de toute avancée dans ce domaine consisterait à améliorer l'efficacité de la méthode CRT afin de calculer les polynômes des classes [106, 98, 129] : cette méthode sélectionne aléatoirement des variétés abéliennes afin d'en trouver dans la classe d'isogénies ciblée, puis cherche des isogénies successives permettant d'accroître l'anneau d'endomorphismes jusqu'au cas maximal.

Indépendamment, la description de ce graphe pourrait être davantage explicitée pour certaines sous classes, comme cela est déjà le cas concernant les variétés abéliennes avec multiplication réelle maximale ou encore les isogénies de type $(\ell, \ell, \ldots, \ell)$. Pareillement, des restrictions à d'autres sous graphes peuvent être envisagées dans l'objectif de calculer certains facteurs des polynômes des classes ou, plus généralement, de subdiviser tout problème général en sous problèmes algorithmiquement plus attaquables. Il s'agit pour cela de munir les variétés abéliennes de structures supplémentaires puis de se restreindre à certaines classes de ces structures. Pour n'en citer que deux, les corps de définition des points de la ℓ-torsion et l'accouplement de Weil fournissent deux telles structures dont les liens avec la structure du graphes d'isogénies ont déjà été partiellement exploités [116, 158].

Endomorphismes de variétés abéliennes générales. La grande majorité des efforts de recherche actuels porte sur les variétés abéliennes simples et ordinaires. Cette restriction est légitimement justifiée par le fait qu'il s'agit là du cas générique : l'espace de modules de ces variétés est de même dimension que celui des variétés abéliennes générales. Les variétés abéliennes non simples ou non ordinaires fournissent néanmoins des espaces de modules de dimension strictement positive dont les particularités peuvent s'avérer utiles notamment dans le cadre de constructions cryptographiques.

Notons d'ailleurs qu'en dimension un les courbes elliptiques supersingulières n'ont cessé de faire l'actualité cryptographique : pour les méfaits de leurs accouplements [49, 58] puis leurs bienfaits [75, 80, 78], pour la mixité de leurs graphes d'isogénies [105], pour un espoir post-quantique [120, 131] puis son déchirement [167, 169, 172]. Leurs extensions en dimension supérieure, que ce soit en les variétés supersingulières ou superspéciales, ont attiré bien moins d'attention.

Il serait donc pertinent d'étendre l'état de l'art des surfaces abéliennes au cas non simples et au cas non ordinaires. Ces travaux concerneraient notamment le calcul des anneaux d'endomorphismes et ses avancées récentes pour les courbes elliptiques supersingulières [157, 165]. Ils déboucheraient sur une compréhension unifiée des structures algébriques pertinentes dont les propriétés particulières pourraient servir de socle à la conception de nouveaux algorithmes ou systèmes cryptographiques, à l'instar de [152].

Deux outils joueront un rôle clef afin d'atteindre ces trois objectifs :

- les surfaces abéliennes à multiplication réelle maximale, qui présentent de grandes similitudes avec le cas de la dimension un, notamment en ce qui concerne la théorie de la multiplication complexe ; elles ne seront ici toutefois pas considérées comme une fin mais comme un tremplin, toute surface abélienne étant isogène à une surface abélienne à multiplication réelle maximale ;
- les bibliothèques logicielles [35, 66, 94], dont le développement va de pair avec toutes les avancées de nature expérimentale en théorie algorithmique des nombres et, bien évidemment, l'établissement de records de calcul.

Applications à l'algorithmique des corps finis

Les deux applications des isogénies et de la théorie de la multiplication complexe à l'algorithmique des corps finis présentées au chapitre 3 de ce mémoire offrent, à elles seules, un grand potentiel de développement. Mentionnons quelques directions de recherche particulièrement pertinentes.

Obtention de résultats de complétude. Une première question particulièrement intéressante serait de quantifier la densité asymptotique des revêtements exceptionnels et des présentations itérées de degré donné que les méthodes du chapitre 3 permettent de construire. L'objectif utopique serait évidemment l'obtention d'un résultat de complétude démontré inconditionnellement. Une approche plus réaliste serait de s'appuyer sur des heuristiques, soutenues par des expérimentations numériques, afin de borner la densité des objets ainsi construits.

Extension aux modules elliptiques. Les modules elliptiques de Drinfeld [28] fournissent un analogue à la théorie de la multiplication complexe pour les corps de fonctions. Leurs propriétés algébriques et analytiques ont été largement étudiées, notamment dans le cadre des conjectures de Langlands, et présentent des similitudes frappantes avec la théorie des courbes elliptiques définies sur les corps finis. Le développement de leurs aspects algorithmiques est relativement nouveau [154, 156] mais progresse rapidement au point qu'il est envisageable d'y étendre les méthodes du chapitre 3.

Extension aux surfaces abéliennes. L'espace de modules des surfaces abéliennes étant de dimension trois, il fournit un cadre naturel offrant des degrés de liberté supplémentaires afin de réaliser une plus grande variété de constructions qu'avec les courbes elliptiques, s'agissant aussi bien de revêtements exceptionnels que de présentations itérées. On peut ainsi envisager imposer des contraintes additionnelles visant à obtenir des constructions plus riches.

Certains outils algorithmiques nécessaires à la réalisation de ces travaux sont bien connus, notamment les polynômes de division de Cantor [57] ou encore les formules explicites d'isogénies en dimension supérieure [125, 137, 138, 161] ; d'autres seront développés dans le cadre du premier volet du présent programme de recherche portant sur les aspects effectifs des surfaces abéliennes. Deux étapes joueront un rôle particulièrement critique : premièrement, expliciter le lien entre les isogénies de variétés abéliennes $\mathscr{A} \to \mathscr{A}'$, données comme variétés jacobiennes $\mathscr{A} = \mathrm{Jac}(\mathscr{H})$ et $\mathscr{A}' = \mathrm{Jac}(\mathscr{H}')$, et les revêtements de courbes algébriques $\mathscr{H} \to \mathscr{H}'$; deuxièmement, étudier finement les propriétés arithmétiques, géométriques et galoisiennes de ces courbes ainsi que des plongements $\mathscr{H} \to \mathscr{A}$ et $\mathscr{H}' \to \mathscr{A}'$.

Notons que de récents travaux caractérisant les endomorphismes des surfaces abéliennes définis sur les corps de nombres [127] permettent d'envisager une généralisation de la construction de présentations itérées dans ce contexte.

Autres applications. Les techniques mentionnées ci-dessus trouveront aussi de multiples applications au delà de celles faisant l'objet du chapitre 3. Mentionnons notamment la construction d'objets en quelque sorte opposés aux revêtements exceptionnels : les fractions rationnelles de petite image. D'intérêt cryptographique [133], ce problème a déjà été attaqué grâce aux courbes elliptiques et aux outils classiques de la théorie de la multiplication complexe [144]. C'est un candidat naturel à l'application des méthodes mentionnées ci-dessus.

Applications en cryptographie

En aval de nombreuses thématiques de recherche présentées ci-avant se trouvent des problématiques relevant du domaine de la cryptographie. Dans cette section, il s'agit cependant de considérer des applications directes à la construction et à l'analyse de systèmes cryptographiques.

Difficulté du problème du logarithme discret. L'expérience montre que la sécurité de systèmes cryptographiques, y compris des plus respectés [30, 120, 131], n'est jamais à l'abri d'une dévaluation irrémédiable suite à d'importantes avancées sur les problèmes mathématiques sous-jacents [56, 167, 169, 172]. Dans ce contexte, tout indicateur de sécurité est précieux, comme notamment les réductions du cas moyen au cas le pire des instances de certains problèmes concernant les réseaux euclidiens [63]. Pour le problème du logarithme discret des variétés abéliennes, ces indicateurs restent toutefois partiels [93].

Les courbes elliptiques supersingulières sont propices à de telles réductions car leurs graphes d'isogénies sont de Ramanujan [41, 47, 69], les marches aléatoires y convergent donc rapidement vers la distribution uniforme ; les avancées restent toutefois entravées par la non commutativité de leurs anneaux d'endomorphismes et son degré plus élevé que celui de l'endomorphisme de Frobenius. Ces verrous pourraient néanmoins être dépassés par des restrictions à certaines sous-structures, par exemple, les intersections de plusieurs tels anneaux qui possèdent une structure plus simple tout en préservant une quantité importante d'information.

Les variétés abéliennes ordinaires possèdent un graphe d'isogénies dont les composantes horizontales sont des espaces principalement homogènes pour certains groupes de classes ; leurs composantes verticales sont quant à elles fortement contraintes : tout grand premier ℓ divisant le conducteur $[\mathcal{O}_K : \mathbb{Z}[\pi, \overline{\pi}]]$ forme une barrière à la connexité effective de la classe d'isogénies. Pour y remédier on peut envisager l'obtention de bornes explicites sur la distribution des degrés de ces isogénies, par des méthodes heuristiques ou de théorie analytique des nombres ; on peut aussi envisager de rétablir la connexité via d'autres morphismes tels l'accouplement de Tate ou encore la descente de Weil, exploitant ainsi les variétés abéliennes de dimension supérieures à l'instar de [173].

Construction de systèmes cryptographiques. L'enjeu est ici d'exploiter les structures offertes par les surfaces abéliennes afin de construire des systèmes cryptographiques riches. Les accouplements jouent notamment un rôle important pour la construction de systèmes de chiffrement semi homomorphe. La réalisation de tels systèmes repose sur la sélection de paramètres [102] et la construction de variétés adaptées [106, 98, 129], deux techniques qui possèdent encore un vaste potentiel d'amélioration. Une direction évidente serait de les étendre au cas des anneaux d'endomorphismes non maximaux, *a minima* dans le cas réel maximal. Toute diversité supplémentaire que cela permettra d'obtenir en terme d'instances de ces systèmes permettra de renforcer leur sécurité ou de les exploiter pour construire des primitives plus riches.

Résistance aux ordinateurs post-quantiques. Ces dernières années ont vues se succéder de rapides avancées constructives et destructives dans le domaine de la cryptographie post-quantique grâce aux isogénies des courbes elliptiques. De récents travaux [167, 169, 172] ont culminé en l'anéantissement d'un système phare [120, 131] dont la sécurité semblait jusqu'alors solidement établie. Malgré ce traumatisme, les isogénies restent un outil pertinent pour la construction de cryptosystèmes post-quantiques.

Des proposition alternatives devront ainsi voir leur efficacité améliorée [148] et leur sécurité évaluée [170, 168]. Ceci souligne le besoin de consolider et d'accélérer le développement et l'analyse des outils algorithmiques liés aux isogénies et plus généralement aux variétés abéliennes.

Bibliographie

[1] Ferdinand Georg Frobenius. « Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe ». *Sitzungsberichte der Deutschen Akademie der Wissenschaften zu Berlin* (1895), pages 689-703.

[2] David Hilbert. « Mathematische Probleme ». *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* 1900 (1900), pages 253-297.

[3] Ernst Steinitz. « Algebraische Theorie der Körper ». *Journal für die reine und angewandte Mathematik* 137 (1910), pages 167-309. doi : 10.1515/crll.1910.137.167.

[4] Ruggiero Torelli. « Sulle varietà di Jacobi ». *Rendiconti della reale accademia nazionale dei Lincei* 22.5 (1913), pages 98-103.

[5] Samuel Lattès. « Sur l'itération des substitutions rationnelles et les fonctions de Poincaré ». *Comptes rendus de l'académie des sciences de Paris* 166 (1918), pages 26-28.

[6] Issai Schur. « Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen ». *Sitzungsberichte der Preussischen Akademie der Wissenschaften* (1923), pages 123-134.

[7] Nikolaï Grigorievitch Tschebotareff. « Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören ». *Mathematische Annalen* 95.1 (1926), pages 191-228. doi : 10.1007/BF01206606.

[8] Otto Marcin Nikodym. « Sur une généralisation des intégrales de M. J. Radon ». *Fundamenta Mathematicae* 15 (1930), pages 131-179. doi : 10.4064/fm-15-1-131-179.

[9] Max Deuring. « Die Typen der Multiplikatorenringe elliptischer Funktionenkörper ». *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 14 (1941), pages 197-272. doi : 10.1007/BF02940746.

[10] André Weil. « Sur les courbes algébriques et les variétés qui s'en déduisent ». *Actualités scientifiques et industrielles* 1041. Publications de l'institut de mathématique de l'université de Strasbourg 7 (1945).

[11] Solomon Kullback et Richard Leibler. « On information and sufficiency ». *Annals of Mathematical Statistics* 22.1 (1951), pages 79-86. doi : 10.1214/aoms/1177729694.

[12] Kurt Heegner. « Diophantische Analysis und Modulfunktionen ». *Mathematische Zeitschrift* 56 (1952), pages 227-253. doi : 10.1007/BF01174749.

[13] André Weil. « Zum Beweis des Torellischen Satzes ». *Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse* 1.IIa (1957), pages 33-53.

[14] Claude Chevalley. « Une démonstration d'un théorème sur les groupes algébriques ». *Journal de mathématiques pures et appliquées* 39 (1960), pages 307-317.

[15] Jun-Ichi Igusa. « Arithmetic variety of moduli for genus two ». *Annals of Mathematics* 72.3 (1960), pages 612-649. doi : 10.2307/1970233.

[16] Goro Shimura et Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Tome 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, 1961.

[17] Alan Baker. « Linear forms in the logarithms of algebraic numbers ». *Mathematika* 13.2 (1966), pages 204-216. doi : 10.1112/S0025579300003971.

[18] John Torrence Tate. « Endomorphisms of abelian varieties over finite fields ». *Inventiones mathematicae* 2.2 (1966), pages 134-144. doi : 10.1007/BF01404549.

[19] David Ryan Hayes. « A geometric approach to permutation polynomials over a finite field ». *Duke Mathematical Journal* 34.2 (1967), pages 293-305. doi : 10.1215/S0012-7094-67-03433-3.

[20] Jean-Pierre Serre. « Complex multiplication ». *Algebraic Number Theory*. Sous la direction de John William Scott Cassels et Albrecht Fröhlich. Academic Press, 1967. Chapitre 13, pages 292-296.

[21] Tetsuji Shioda. « On the graded ring of invariants of binary octavics ». *American Journal of Mathematics* 89.4 (1967), pages 1022-1046. doi : 10.2307/2373415.

[22] Harold Mead Stark. « A complete determination of the complex quadratic fields of class-number one ». *Michigan Mathematical Journal* 14.1 (1967), pages 1-27. doi : 10.1307/mmj/1028999653.

[23] Stephen D. Cohen. « On irreducible polynomials of certain types in finite fields ». *Mathematical Proceedings of the Cambridge Philosophical Society* 66.2 (1969), pages 335-344. doi : 10.1017/S0305004100045023.

[24] William Charles Waterhouse. « Abelian varieties over finite fields ». *Annales scientifiques de l'École normale supérieure* 2.4 (1969), pages 521-560.

[25] Michael David Fried. « On a conjecture of Schur ». *Michigan Mathematical Journal* 17 (1970), pages 41-55. doi : .1307/mmj/1029000374.

[26] Jacques Vélu. « Isogénies entre courbes elliptiques ». *Comptes rendus de l'académie des sciences de Paris*. A 273 (1971), pages 238-241.

[27] Jean-Pierre Serre. « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques ». *Inventiones mathematicae* 15.4 (1972), pages 259-331. doi : 10.1007/BF01405086.

[28] Vladimir Gershonovich Drinfeld. « Elliptic modules ». *Matematicheskii Sbornik. Novaya Seriya* 94(136).4(8) (1974), pages 594-627. doi : 10.1070/SM1974v023n04ABEH001731.

[29] Michael David Fried. « Galois groups and complex multiplication ». *Transactions of the American Mathematical Society* 235 (1978), pages 141-163. doi : 10.2307/1998211.

[30] Ronald Linn Rivest, Adi Shamir et Leonard Max Adleman. « A method for obtaining digital signatures and public-key cryptosystems ». *Communications of the ACM* 21.2 (1978), pages 120-126. doi : 10.1145/359340.359342.

[31] Henri Cohen et Hendrik Willem Lenstra. « Heuristics on class groups of number fields ». *Number Theory Noordwijkerhout — Journées arithmétiques 1983*. Sous la direction d'Hendrik Jager. Tome 1068. Lecture Notes in Mathematics. Springer, 1984, pages 33-62. doi : 10.1007/BFb0099440.

[32] David Mumford. *Tata lectures on theta, II*. Tome 43. Progress in Mathematics. Birkhäuser, 1984. isbn : 3-7643-3110-0.

[33] Leslie Gabriel Valiant. « A theory of the learnable ». *Communications of the ACM* 27.11 (1984), pages 1134-1142. doi : 10.1145/1968.1972.

[34] Rom Rubenovich Varshamov. « A general method of synthesis for irreducible polynomials over Galois fields ». *Proceedings of the USSR Academy of Sciences* 275.5 (1984), pages 1041-1044. url : http://mi.mathnet.ru/eng/dan/v275/i5/p1041.

[35] *PARI/GP*. A computer algebra system designed for fast computations in number theory. The PARI Group. 1985. URL : http://pari.math.u-bordeaux.fr/.

[36] René SCHOOF. « Elliptic curves over finite fields and the computation of square roots mod p ». *Mathematics of Computation* 44.170 (1985), pages 483-494. DOI : 10.1090/S0025-5718-1985-0777280-6.

[37] Victor Saul MILLER. « Use of elliptic curves in cryptography ». *Advances in Cryptology — CRYPTO 1985*. Sous la direction d'Hugh C. WILLIAMS. Tome 218. Lecture Notes in Computer Science. Springer, 1986, pages 417-426. DOI : 10.1007/3-540-39799-X_31.

[38] Jacques DIXMIER. « On the projective invariants of quartic plane curves ». *Advances in Mathematics* 64.3 (1987), pages 279-304. DOI : 10.1016/0001-8708(87)90010-7.

[39] Neal I. KOBLITZ. « Elliptic curve cryptosystems ». *Mathematics of Computation* 48.177 (1987), pages 203-209. DOI : 10.1090/S0025-5718-1987-0866109-5.

[40] Arthur Oliver Lonsdale ATKIN. « The number of points on an elliptic curve modulo a prime ». 1988.

[41] Alexander LUBOTZKY, Ralph Saul PHILLIPS et Peter Clive SARNAK. « RAMANUJAN graphs ». *Combinatorica* 8 (1988), pages 261-277. DOI : 10.1007/BF02126799.

[42] Joel Vincent BRAWLEY et George Ernest SCHNIBBEN. *Infinite Algebraic Extensions of Finite Fields*. Tome 95. Contemporary Mathematics. American Mathematical Society, 1989. ISBN : 0-8218-5101-2.

[43] Johannes BUCHMANN. « A subexponential algorithm for the determination of class groups and regulators of algebraic number fields ». *Séminaire de théorie des nombres, Paris*. Sous la direction de Catherine GOLDSTEIN. Tome 91. Progress in Mathematics. Birkhäuser, 1989, pages 27-41.

[44] Neal I. KOBLITZ. « Hyperelliptic cryptosystems ». *Journal of Cryptology* 1.3 (1989), pages 139-150. DOI : 10.1007/BF02252872.

[45] Helmut MEYN. « On the construction of irreducible self-reciprocal polynomials over finite fields ». *Applicable Algebra in Engineering, Communication and Computing* 1.1 (1990), pages 43-53. DOI : 10.1007/BF01810846.

[46] Jonathan PILA. « FROBENIUS maps of abelian varieties and finding roots of unity in finite fields ». *Mathematics of Computation* 55.192 (1990), pages 745-763. DOI : 10.1090/S0025-5718-1990-1035941-X.

[47] Arnold Koster PIZER. « RAMANUJAN graphs and HECKE operators ». *Bulletin of the American Mathematical Society* 23.1 (1990), pages 127-137. URL : https://projecteuclid.org/euclid.bams/1183555725.

[48] Noam David ELKIES. « Explicit isogenies ». 1991.

[49] Alfred MENEZES, Tatsuaki OKAMOTO et Scott VANSTONE. « Reducing elliptic curve logarithms to logarithms in a finite field ». *IEEE Transactions on Information Theory* 39.5 (1991), pages 1639-1646. DOI : 10.1109/18.259647.

[50] Jean-François MESTRE. « Construction de courbes de genre 2 à partir de leurs modules ». *Effective methods in algebraic geometry — MEGA 1990*. Sous la direction de Teo MORA et Carlo TRAVERSO. Tome 94. Progress in Mathematics. Birkhäuser, 1991, pages 313-334.

[51] Vladimir Naumovich VAPNIK. « Principles of risk minimization for learning theory ». *Advances in Neural Information Processing Systems — NIPS 1991*. Sous la direction de John Earl MOODY, Stephen José HANSON et Richard P. LIPPMANN. Tome 4. Association for Computer Machinery, 1991, pages 831-838. ISBN : 1-55860-222-4.

[52] Stephen D. COHEN. « The explicit construction of irreducible polynomials over finite fields ». *Designs, Codes and Cryptography* 2 (1992), pages 169-174. DOI : 10.1007/BF00124895.

[53] Hendrik Willem LENSTRA et Carl POMERANCE. « A rigorous time bound for factoring integers ». *Journal of the American Mathematical Society* 5.3 (1992), pages 483-516. DOI : 10.1090/S0894-0347-1992-1137100-0.

[54] Leonard Max Adleman et Jonathan DeMarrais. « A subexponential algorithm for discrete logarithms over all finite fields ». *Mathematics of Computation* 61.203 (1993), pages 1-15. doi : 10.1006/jsco.2001.0470.

[55] Michael David Fried, Robert Guralnick et Jan Saxl. « Schur covers and Carlitz's conjecture ». *Israel Journal of Mathematics* 82 (1993), pages 157-225. doi : 10.1007/BF02808112.

[56] Arjen Klaas Lenstra et Hendrik Willem Lenstra, éditeurs. *The Development of the Number Field Sieve*. Tome 1554. Lecture Notes in Mathematics. Springer, 1993. isbn : 3-540-57013-6.

[57] David Geoffrey Cantor. « On the analogue of the division polynomials for hyperelliptic curves ». *Journal für die reine und angewandte Mathematik* 447 (1994), pages 91-145. doi : 10.1515/crll.1994.447.91.

[58] Gerhard Frey et Hans-Georg Rück. « A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves ». *Mathematics of Computation* 62.206 (1994), pages 865-874. doi : 10.2307/2153546.

[59] Michael David Fried. « Global construction of general exceptional covers ». *Finite Fields : Theory, Applications, and Algorithms*. Sous la direction de Gary Lee Mullen et Peter Jau-Shyong Shiue. Tome 168. Contemporary Mathematics. American Mathematical Society, 1994, pages 69-100. doi : 10.1090/conm/168/01690.

[60] Joseph Hillel Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Tome 151. Graduate Texts in Mathematics. Springer, 1994. doi : 10.1007/978-1-4612-0851-8.

[61] Richard Lawrence Taylor et Andrew Wiles. « Ring-theoretic properties of certain Hecke algebras ». *Annals of Mathematics* 141.3 (1995), pages 553-572. doi : 10.2307/2118560.

[62] Andrew Wiles. « Modular elliptic curves and Fermat's last theorem ». *Annals of Mathematics* 141.3 (1995), pages 443-551. doi : 10.2307/2118559.

[63] Miklós Ajtai. « Generating hard instances of lattice problems ». *Symposium on Theory of Computing — STOC 1996*. Sous la direction de Gary L. Miller. Association for Computing Machinery, 1996, pages 99-108. doi : 10.1145/237814.237838.

[64] Jean-Marc Couveignes. « Computing ℓ-isogenies using the p-torsion ». *Algorithmic Number Theory — ANTS-II*. Sous la direction d'Henri Cohen. Tome 1122. Lecture Notes in Computer Science. Springer, 1996, pages 59-65. doi : 10.1007/3-540-61581-4_41.

[65] David Russell Kohel. « Endomorphism rings of elliptic curves over finite fields ». Thèse de doctorat. University of California at Berkeley, 1996. url : http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf.

[66] Wieb Bosma, John Cannon et Catherine Playoust. « The Magma algebra system : the user language ». *Journal of Symbolic Computation* 24.3–4 (1997), pages 235-265. doi : 10.1006/jsco.1996.0125.

[67] Jean-Marc Couveignes. *Hard homogeneous spaces*. 1997. IACR Cryptology ePrint archive, 2006/291.

[68] Alfred Menezes et Yi-Hong Wu. « The discrete logarithm problem in GL(n, q) ». *Ars Combinatoria* 47 (1997), pages 23-32.

[69] Arnold Koster Pizer. « Ramanujan graphs ». *Computational Perspectives on Number Theory*. Proceedings of a conference in honor of A. O. L. Atkin. Tome 7. AMS/IP Studies in Advanced Mathematics. American Mathematical Society, 1998, pages 159-178.

[70] Steven D. Galbraith. « Constructing isogenies between elliptic curves over finite fields ». *London Mathematical Society Journal of Computation and Mathematics* 2 (1999), pages 118-138. doi : 10.1112/S1461157000000097.

[71] Alice Gee. « Class invariants by Shimura's reciprocity law ». *Journal de théorie des nombres de Bordeaux* 11.1 (1999), pages 45-72.

[72] Paul van Wamelen. « Examples of genus-two CM curves defined over the rationals ». *Mathematics of Computation* 68.225 (1999), pages 307-320. DOI : 10.1090/S0025-5718-99-01020-0.

[73] Paul van Wamelen. « Proving that a genus-2 curve has complex multiplication ». *Mathematics of Computation* 68.228 (1999), pages 1663-1677. DOI : 10.1090/S0025-5718-99-01101-1.

[74] Pierrick Gaudry et Robert Harley. « Counting points on hyperelliptic curves over finite fields ». *Algorithmic Number Theory — ANTS-IV*. Sous la direction de Wieb Bosma. Tome 1838. Lecture Notes in Computer Science. Springer, 2000, pages 313-332. DOI : 10.1007/10722028_18.

[75] Ryuichi Sakai, Kiyoshi Ohgishi et Masao Kasahara. « Cryptosystems based on pairing ». *Symposium on Cryptography and Information Security — SCIS 2000*. IEICE, 2000, C20.

[76] Takakazu Satoh. « The canonical lift of an ordinary elliptic curve over a finite field and its point counting ». *Journal of the Ramanujan Mathematical Society* 15.4 (2000), pages 247-270.

[77] Leonard Max Adleman et Ming-Deh Huang. « Counting points on curves and abelian varieties over finite fields ». *Journal of Symbolic Computation* 23.3 (2001), pages 171-189. DOI : 10.1006/jsco.2001.0470.

[78] Dan Boneh et Matthew Keith Franklin. « Identity-based encryption from the Weil pairing ». *Advances in Cryptology — CRYPTO 2001*. Sous la direction de Joe Kilian. Tome 2139. Lecture Notes in Computer Science. Springer, 2001, pages 213-229. DOI : 10.1007/3-540-44647-8_13.

[79] Christophe Breuil, Brian Conrad, Fred Diamond et Richard Lawrence Taylor. « On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises ». *Journal of the American Mathematical Society* 14.4 (2001), pages 843-939. DOI : 10.1090/S0894-0347-01-00370-8.

[80] Clifford Cocks. « An identity-based encryption scheme based on quadratic residues ». *Cryptography and Coding — IMA-CC 2001*. Sous la direction de Bahram Honary. Tome 2260. Lecture Notes in Computer Science. Springer, 2001, pages 360-363. DOI : 10.1007/3-540-45325-3_32.

[81] Kiran Sridhara Kedlaya. « Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology ». *Journal of the Ramanujan Mathematical Society* 16.4 (2001), pages 323-338.

[82] Naoki Murabayashi et Atsuki Umegaki. « Determination of all $\mathbb{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces ». *Journal of Algebra* 235.1 (2001), pages 267-274. DOI : 10.1006/jabr.2000.8453.

[83] Mireille Fouquet et François Morain. « Isogeny volcanoes and the SEA algorithm ». *Algorithmic Number Theory — ANTS-V*. Sous la direction de Claus Fieker et David Russell Kohel. Tome 2369. Lecture Notes in Computer Science. Springer, 2002, pages 47-62. DOI : 10.1007/3-540-45455-1_23.

[84] Robert Guralnick, Peter Müller et Jan Saxl. « The rational function analogue of a question of Schur and exceptionality of permutation representations ». *Memoirs of the American Mathematical Society* 162.773 (2002). DOI : 10.1090/memo/0773.

[85] Melsik K. Kyuregyan. « Recurrent methods for constructing irreducible polynomials over GF(2^s) ». *Finite Fields and their Applications* 8.1 (2002), pages 52-68. DOI : 10.1006/ffta.2001.0323.

[86] Reinhard Schertz. « Weber's class invariants revisited ». *Journal de théorie des nombres de Bordeaux* 14.1 (2002), pages 325-343.

[87] Melsik K. Kyuregyan. « Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics ». *Finite Fields and their Applications* 9.1 (2003), pages 39-58. DOI : 10.1016/S1071-5797(02)00005-9.

[88] Andrew Victor Sutherland. *Isogeny volcanoes*. Sous la direction d'Everett William Howe et Kiran Sridhara Kedlaya. 2003. doi : 10.2140/obs.2013.1.507.

[89] Olivier Catoni. *Statistical Learning Theory and Stochastic Optimization. École d'été de probabilités de Saint-Flour XXXI*. Tome 1851. Lecture Notes in Mathematics. Springer, 2004. isbn : 3-540-22572-2.

[90] Hobart Peyton Young. *Strategic Learning and its Limits*. Oxford University Press, 2004. isbn : 0-19-926918-1.

[91] Manjul Bhargava. « The density of discriminants of quartic rings and fields ». *Annals of Mathematics* 162.2 (2005), pages 1031-1063. doi : 10.4007/annals.2005.162.1031.

[92] Michael David Fried. « The place of exceptional covers among all diophantine relations ». *Finite Fields and their Applications* 11.3 (2005), pages 367-433. doi : 10.1016/j.ffa.2005.06.005.

[93] David Jao, Stephen David Miller et Ramarathnam Venkatesan. « Do all elliptic curves of the same order have the same difficulty of discrete log ? » : *Advances in Cryptology — ASIACRYPT 2005*. Sous la direction de Bimal Roy. Tome 3788. Lecture Notes in Computer Science. Springer, 2005, pages 21-40. doi : 10.1007/11593447_2.

[94] William Arthur Stein et al. *Sage Mathematics Software*. The Sage Development Team. 2005. url : http://www.sagemath.org/.

[95] Olivier Catoni. *Pac-Bayesian Supervised Classification : The Thermodynamics of Statistical Learning*. Tome 56. Lecture Notes - Monograph Series. Institute of Mathematical Statistics, 2006. isbn : 0-940600-72-2. doi : 10.1214/074921707000000391.

[96] Melsik K. Kyuregyan. « Recurrent methods for constructing irreducible polynomials over $\mathbb{F}_q$ of odd characteristics, II ». *Finite Fields and their Applications* 12.3 (2006), pages 357-378. doi : 10.1016/j.ffa.2005.07.002.

[97] Tong Zhang. « Information theoretical upper and lower bounds for statistical estimation ». *IEEE Transactions on Information Theory* 52.4 (2006), pages 1307-1321. doi : 10.1109/TIT.2005.864439.

[98] David Mandell Freeman et Kristin Estella Lauter. « Computing endomorphism rings of Jacobians of genus-2 curves over finite fields ». *Algebraic Geometry and its Applications — SAGA 2007*. Sous la direction de Jean Chaumine, James Hirschfeld et Robert Rolland. Tome 5. Number Theory and its Applications. World Scientific, 2007, pages 29-66. doi : 10.1142/9789812793430_0002.

[99] Eyal Zvi Goren et Kristin Estella Lauter. « Class invariants for quartic CM fields ». *Annales de l'institut Fourier* 57.2 (2007), pages 457-480. doi : 10.5802/aif.2264.

[100] Robert Michael Guralnick, Thomas John Tucker et Michael Ernest Zieve. « Exceptional covers and bijections on rational points ». *International Mathematics Research Notices* 2007, rnm004 (2007). doi : 10.1093/imrn/rnm004.

[101] Toshiaki Ohno. « The graded ring of invariants of ternary quartics I. Generators and relations ». 2007.

[102] David Mandell Freeman. « A generalized Brezing–Weng method for constructing pairing-friendly ordinary abelian varieties ». *Pairing-Based Cryptography — PAIRING 2008*. Sous la direction de Steven D. Galbraith et Kenny G. Paterson. Tome 5209. Lecture Notes in Computer Science. Springer, 2008, pages 146-163. doi : 10.1007/978-3-540-85538-5_11.

[103] Alan George Beattie Lauder et Daqing Wan. « Counting points on varieties over finite fields of small characteristic ». *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography*. Sous la direction de Joseph Peter Buhler et Peter Stevenhagen. Tome 44. Mathematical Sciences Research Institute Publications. Cambridge University Press, 2008, pages 579-612.

[104] Reinier Bröker et Kristin Estella Lauter. « Modular polynomials for genus 2 ». *London Mathematical Society Journal of Computation and Mathematics* 12 (2009), pages 326-339. doi : 10.1112/S1461157000001546.

[105] Denis Xavier Charles, Eyal Zvi Goren et Kristin Estella Lauter. « Cryptographic hash functions from expander graphs ». *Journal of Cryptology* 22.1 (2009), pages 93-113. doi : 10.1007/s00145-007-9002-x.

[106] Kirsten Eisenträger et Kristin Estella Lauter. « A CRT algorithm for constructing genus-2 curves over finite fields ». *Arithmetic, Geometry and Coding Theory — AGCT 2010*. Sous la direction de François Rodier et Serge Vladut. Tome 21. Séminaires et congrès. Société Mathématique de France, 2009, pages 161-176.

[107] Andreas Enge. « Computing modular polynomials in quasi-linear time ». *Mathematics of Computation* 78.267 (2009), pages 1809-1824. doi : 10.1090/S0025-5718-09-02199-1.

[108] Andreas Enge. « The complexity of class polynomial computation via floating point approximations ». *Mathematics of Computation* 78.266 (2009), pages 1089-1107. doi : 10.1090/S0025-5718-08-02200-X.

[109] David Mandell Freeman, Michael Scott et Edlyn Teske. « A taxonomy of pairing-friendly elliptic curves ». *Journal of Cryptology* 23.2 (2009), pages 224-280. doi : 10.1007/s00145-009-9048-z.

[110] Thomas Icart. « How to hash into elliptic curves ». *Advances in Cryptology — CRYPTO 2009*. Sous la direction de Shai Halevi. Tome 5677. Lecture Notes in Computer Science. Springer, 2009, pages 301-316. doi : 10.1007/978-3-642-03356-8_18.

[111] David Jao, Stephen David Miller et Ramarathnam Venkatesan. « Expander graphs based on GRH with an application to elliptic curve cryptography ». *Journal of Number Theory* 129.6 (2009), pages 1491-1504. doi : 10.1016/j.jnt.2008.11.006.

[112] Markus Wagner. « Über Korrespondenzen zwischen algebraischen Funktionenkörper ». Thèse de doctorat. Technische Universität Berlin, 2009. url : http://www.math.tu-berlin.de/~wagner/Diss.pdf.

[113] Gaetan Bisson, Romain Cosset et Damien Robert. *AVIsogenies*. A library for computing isogenies between abelian varieties. Agence pour la protection des programmes, 2010, IDDN.FR.001.440011.000.R.P.2010.000.10000. url : https://www.math.u-bordeaux.fr/~damienrobert/avisogenies/.

[114] Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam et Mehdi Tibouchi. « Efficient indifferentiable hashing into ordinary elliptic curves ». *Advances in Cryptology — CRYPTO 2010*. Sous la direction de Tal Rabin. Tome 6223. Lecture Notes in Computer Science. Springer, 2010, pages 237-254. doi : 10.1007/978-3-642-14623-7_13.

[115] Pierre-Alain Fouque et Mehdi Tibouchi. « Deterministic encoding and hashing to odd hyperelliptic curves ». *Pairing-Based Cryptography - PAIRING 2010*. Sous la direction de Marc Joye, Atsuko Miyaji et Akira Otsuka. Tome 6487. Lecture Notes in Computer Science. Springer, 2010, pages 265-277. doi : 10.1007/978-3-642-17455-1_17.

[116] Sorina Ionica et Antoine Joux. « Pairing the volcano ». *Algorithmic Number Theory — ANTS-IX*. Sous la direction de Guillaume Hanrot, François Morain et Emmanuel Thomé. Tome 6197. Lecture Notes in Computer Science. Springer, 2010, pages 201-218. doi : 10.1007/978-3-642-14518-6_18.

[117] Jean-Gabriel Kammerer, Reynald Lercier et Guénaël Renault. « Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time ». *Pairing-Based Cryptography - PAIRING 2010*. Sous la direction de Marc Joye, Atsuko Miyaji et Akira Otsuka. Tome 6487. Lecture Notes in Computer Science. Springer, 2010, pages 278-297. doi : 10.1007/978-3-642-17455-1_18.

[118] Gaetan Bisson. *Endomorphism Rings in Cryptography*. Eindhoven University of Technology & Institut national polytechnique de Lorraine, 2011. ISBN : 90-386-2519-7. DOI : 10.6100/IR714676.

[119] Gaetan Bisson et Andrew Victor Sutherland. « Computing the endomorphism ring of an ordinary elliptic curve over a finite field ». *Journal of Number Theory* 131.5 (2011) : *Elliptic Curve Cryptography*. Sous la direction de Neal I. Koblitz et Victor Saul Miller, pages 815-831. DOI : 10.1016/j.jnt.2009.11.003.

[120] David Jao et Luca De Feo. « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies ». *Post-Quantum Cryptography — PQCRYPTO 2011*. Sous la direction de Bo-Yin Yang. Tome 7071. Lecture Notes in Computer Science. Springer, 2011, pages 19-34. DOI : 10.1007/978-3-642-25405-5_2.

[121] Andrew Victor Sutherland. « Computing Hilbert class polynomials with the Chinese remainder theorem ». *Mathematics of Computation* 80.273 (2011), pages 501-538. DOI : 10.1090/S0025-5718-2010-02373-7.

[122] Gaetan Bisson. « Computing endomorphism rings of elliptic curves under the GRH ». *Journal of Mathematical Cryptology* 5.2 (2012), pages 101-113. DOI : 10.1515/jmc.2011.008.

[123] Reinier Bröker, Kristin Estella Lauter et Andrew Victor Sutherland. « Modular polynomials via isogeny volcanoes ». *Mathematics of Computation* 81.278 (2012), pages 1201-1231. DOI : 10.1090/S0025-5718-2011-02508-1.

[124] Reynald Lercier et Christophe Ritzenthaler. « Hyperelliptic curves and their invariants : geometric, arithmetic and algorithmic aspects ». *Journal of Algebra* 372 (2012), pages 595-636. DOI : 10.1016/j.jalgebra.2012.07.054.

[125] David Lubicz et Damien Robert. « Computing isogenies between abelian varieties ». *Compositio Mathematica* 148.5 (2012), pages 1483-1515. DOI : 10.1112/S0010437X12000243.

[126] Marco Streng. *An explicit version of Shimura's reciprocity law for Siegel modular functions*. 2012. Cornell University arXiv repository, 1201.0020.

[127] Reinier Bröker, Kristin Lauter et Marco Streng. « Abelian surfaces admitting an (ℓ, ℓ)-endomorphism ». *Journal of Algebra* 394 (2013), pages 374-396. DOI : 10.1016/j.jalgebra.2013.07.011.

[128] Reza Rezaeian Farashahi, Pierre-Alain Fouque, Igor Shparlinski, Mehdi Tibouchi et José Felipe Voloch. « Indifferentiable deterministic hashing to elliptic and hyperelliptic curves ». *Mathematics of Computation* 82 (2013), pages 491-512. DOI : 10.1090/S0025-5718-2012-02606-8.

[129] Kristin Estella Lauter et Damien Robert. « Improved CRT algorithm for class polynomials in genus 2 ». *Algorithmic Number Theory Symposium — ANTS-X*. Sous la direction d'Everett William Howe et Kiran Sridhara Kedlaya. Tome 1. The Open Book Series 1. Mathematical Sciences Publishers, 2013, pages 437-461. DOI : 10.2140/obs.2013.1.437.

[130] Jean-Marc Couveignes et Reynald Lercier. « The geometry of some parameterizations and encodings ». *Advances in Mathematics of Communications* 8.4 (2014), pages 437-458. DOI : 10.3934/amc.2014.8.437.

[131] Luca De Feo, David Jao et Jérôme Plût. « Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies ». *Journal of Mathematical Cryptology* 8.3 (2014), pages 209-247. DOI : 10.1515/jmc-2012-0015.

[132] Andreas Enge et Emmanuel Thomé. « Computing class polynomials for abelian surfaces ». *Experimental Mathematics* 23.2 (2014), pages 129-145. DOI : 10.1080/10586458.2013.878675.

[133] Minkyu Kim, Jung Hee Cheon et In-Sok Lee. « Analysis on a generalized algorithm for the strong discrete logarithm problem with auxiliary inputs ». *Mathematics of Computation* 83 (2014), pages 1993-2004. DOI : 10.1090/S0025-5718-2014-02813-5.

[134] Marco Streng. « Computing Igusa class polynomials ». *Mathematics of Computation* 83 (2014), pages 275-309. doi : 10.1090/S0025-5718-2013-02712-3.

[135] Gaetan Bisson. « Computing endomorphism rings of abelian varieties of dimension two ». *Mathematics of Computation* 84.294 (2015), pages 1977-1989. doi : 10.1090/S0025-5718-2015-02938-X.

[136] Florian Bouyer et Marco Streng. « Examples of CM curves of genus two defined over the reflex field ». *London Mathematical Society Journal of Computation and Mathematics* 18.1 (2015), pages 507-538. doi : 10.1112/S1461157015000121.

[137] Romain Cosset et Damien Robert. « Computing (ℓ, ℓ)-isogenies in polynomial time on Jacobians of genus-2 curves ». *Mathematics of Computation* 84 (2015), pages 1953-1975. doi : 10.1090/S0025-5718-2014-02899-8.

[138] Jean-Marc Couveignes et Tony Ezome. « Computing functions on Jacobians and their quotients ». *London Mathematical Society Journal of Computation and Mathematics* 18.1 (2015), pages 555-577. doi : 10.1112/S1461157015000169.

[139] Andreas Enge et Marco Streng. *Schertz style class invariants for quartic CM fields*. 2016. Cornell University arXiv repository, 1610.04505.

[140] Lenka Zdeborová et Florent Krzakala. « Statistical physics of inference : thresholds and algorithms ». *Advances in Physics* 65.5 (2016), pages 453-552. doi : 10.1080/00018732.2016.1211393.

[141] Gaetan Bisson et Marco Streng. « On polarised class groups of orders in quartic CM-fields ». *Mathematical Research Letters* 24.2 (2017), pages 247-270. doi : 10.4310/MRL.2017.v24.n2.a1.

[142] Gaetan Bisson et Mehdi Tibouchi. « 同種写像を用いた置換有理関数の生成手法 ». *Symposium on Cryptography and Information Security — SCIS 2017*. IEICE, 2017, 3B2-3.

[143] Ernest Hunter Brooks, Dimitar Jetchev et Benjamin Wesolowski. « Isogeny graphs of ordinary abelian varieties ». *Research in Number Theory* 3.28 (2017). doi : 10.1007/s40993-017-0087-5.

[144] Igor Shparlinski et Andrew Victor Sutherland. « Finding elliptic curves with a subgroup of prescribed size ». *International Journal of Number Theory* 13.1 (2017), pages 133-152. doi : 10.1142/S1793042117500099.

[145] Aolin Xu et Maxim Raginsky. « Information-theoretic analysis of generalization capability of learning algorithms ». *Advances in Neural Information Processing Systems — NIPS 2017*. Sous la direction d'Isabelle Guyon, Ulrike von Luxburg, Samy Bengio, Hanna Megan Wallach, Rob Fergus, S. V. N. Vishwanathan et Roman Garnett. Tome 30. Association for Computer Machinery, 2017, pages 2521-2530. isbn : 1-5108-6096-7.

[146] Gaetan Bisson et Dimitar Jetchev. « Isogeny graphs of ordinary abelian surfaces and endomorphism rings ». *L-Functions and Algebraic Varieties. A conference in memory of Alexey Zykin*. Moscow Independent University, 2018. url : https://www.mathnet.ru/php/conference.phtml?confid=1347.

[147] Gaetan Bisson et Mehdi Tibouchi. « Constructing permutation rational functions from isogenies ». *SIAM Journal on Discrete Mathematics* 32.3 (2018), pages 1741-1749. doi : 10.1137/17M1135736.

[148] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny et Joost Renes. « CSIDH : an efficient post-quantum commutative group action ». *Advances in Cryptology — ASIACRYPT 2018*. Sous la direction de Thomas Peyrin et Steven Galbraith. Tome 11274. Lecture Notes in Computer Science. Springer, 2018, pages 395-427. doi : 10.1007/978-3-030-03332-3_15.

[149] Pınar Kiliçer, Hugo Labrande, Reynald Lercier, Christophe Ritzenthaler, Jeroen Sijsling et Marco Streng. « Plane quartics over $\mathbb{Q}$ with complex multiplication ». *Acta Arithmetica* 185.2 (2018), pages 127-156. doi : 10.4064/aa170227-16-3.

[150] Razvan Barbulescu et Sylvain Duquesne. « Updating key size estimations for pairings ». *Journal of Cryptology* 32 (2019), pages 1298-1336. doi : 10.1007/s00145-018-9280-5.

[151] Alp Bassa et Ricardo Menares. « The R-transform as a power map and its generalisations to higher degree ». (2019). url : https://arxiv.org/abs/1909.02608.

[152] Wouter Castryck, Thomas Decru et Benjamin Smith. *Hash functions from superspecial genus-2 curves using Richelot isogenies*. 2019. url : https://arxiv.org/abs/1903.06451.

[153] Stefano Marseglia. « Computing the ideal class monoid of an order ». *Journal of the London Mathematical Society* 101.3 (2019), pages 984-1007. doi : 10.1112/jlms.12294.

[154] Yossef Musleh et Éric Schost. « Computing the characteristic polynomial of a finite rank-two Drinfeld module ». *Symbolic and Algebraic Computation — ISSAC 2019*. Sous la direction de James Davenport, Dongming Wang, Manuel Kauers et Russell Bradford. Association for Computing Machinery, 2019, pages 307-314. doi : 10.1145/3326229.3326256.

[155] Caleb Springer. « Computing the endomorphism ring of an ordinary abelian surface over a finite field ». *Journal of Number Theory* 202 (2019), pages 403-457. doi : 10.1016/j.jnt.2019.01.013.

[156] Perlas Caranay, Matthew Greenberg et Renate Scheidler. « Computing modular polynomials and isogenies of rank-two Drinfeld modules over finite fields ». *75 Years of Mathematics of Computation*. Sous la direction de Susanne Cecelia Brenner, Igor Shparlinski, Chi-Wang Shu et Daniel B. Szyld. Tome 754. Contemporary Mathematics. American Mathematical Society, 2020, pages 283-313. doi : 10.1090/conm/754/15148.

[157] Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison et Jennifer Park. « Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs ». *Algorithmic Number Theory Symposium — ANTS-XIV*. Sous la direction de Steven D. Galbraith. Tome 4. The Open Book Series 1. Mathematical Sciences Publishers, 2020, pages 215-232. doi : 10.2140/obs.2020.4.215.

[158] Sorina Ionica et Emmanuel Thomé. « Isogeny graphs with maximal real multiplication ». *Journal of Number Theory* 207 (2020), pages 385-422. doi : 10.1016/j.jnt.2019.06.019.

[159] Reynald Lercier, Christophe Ritzenthaler et Jeroen Sijsling. « Reconstructing plane quartics from their invariants ». *Discrete & Computational Geometry* 63 (2020), pages 73-113. doi : 10.1007/s00454-018-0047-4.

[160] Chloe Martindale. « Hilbert modular polynomials ». *Journal of Number Theory* 213 (2020), pages 464-498. doi : 10.1016/j.jnt.2019.11.019.

[161] Enea Milio. « Computing isogenies between Jacobians of curves of genus 2 and 3 ». *Mathematics of Computation* 89 (2020), pages 1331-1364. doi : 10.1090/mcom/3486.

[162] Enea Milio et Damien Robert. « Modular polynomials on Hilbert surfaces ». *Journal of Number Theory* 216 (2020), pages 403-459. doi : 10.1016/j.jnt.2020.04.014.

[163] Claus Fieker, Tommy Hofmann et Sogo Pierre Sanon. « On the computation of the endomorphism rings of abelian surfaces ». *Journal of Number Theory* 229 (2021), pages 39-52. doi : 10.1016/j.jnt.2021.04.024.

[164] Samir Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie et Stefano Rini. *Empirical risk minimization with generalized relative entropy regularization*. Rapport scientifique 9454. Institut national de recherche en informatique et en automatique, 2021. url : https://hal.inria.fr/INRIA-RRRT/hal-03560072.

[165] Benjamin Wesolowski. « The supersingular isogeny path and endomorphism ring problems are equivalent ». (2021), pages 1100-1111. doi : 10.1109/FOCS52979.2021.00109.

[166] Alp Bassa et Ricardo Menares. « Galois theory and iterative construction of irreducible polynomials ». (2022). En préparation.

[167] Wouter Castryck et Thomas Decru. *An efficient key recovery attack on SIDH*. 2022. IACR Cryptology ePrint archive, 2022/975.

[168] Tako Boris Fouotsa. *SIDH with masked torsion point images*. 2022. IACR Cryptology ePrint archive, 2022/1054.

[169] Luciano Maino et Chloe Martindale. *An attack on SIDH with arbitrary starting curve*. 2022. IACR Cryptology ePrint archive, 2022/1026.

[170] Tomoki Moriya. *Masked-degree SIDH*. 2022. IACR Cryptology ePrint archive, 2022/1019.

[171] Samir Perlaza, Gaetan Bisson, Iñaki Esnaola, Alain Jean-Marie et Stefano Rini. « Empirical risk minimization with relative entropy regularization : optimality and sensitivity analysis ». *International Symposium on Information Theory — ISIT 2022*. IEEE, 2022, pages 684-689. doi : 10.1109/ISIT50566.2022.9834273.

[172] Damien Robert. *Breaking SIDH in polynomial time*. 2022. IACR Cryptology ePrint archive, 2022/1038.

[173] Damien Robert. *Some applications of higher dimensional isogenies to elliptic curves*. 2022. IACR Cryptology ePrint archive, 2022/1704.

[174] Alp Bassa, Gaetan Bisson et Roger Oyono. *Iterative constructions of irreducible polynomials from isogenies*. 2023. Cornell University arXiv repository, 2302.09674.

[175] Pınar Kiliçer et Marco Streng. « The CM class number one problem for curves of genus 2 ». *Research in Number Theory* 9.15 (2023). doi : 10.1007/s40993-022-00417-7.

[176] Antonin Leroux. *Computation of Hilbert class polynomials and modular polynomials from supersingular elliptic curves*. 2023. Cornell University arXiv repository, 2301.08531.