Christophe **Levrat**

Chercheur post-doctoral en mathématiques & cryptographie

Table des matières

Intérêts scientifiques

- cohomologie étale et cohomologie galoisienne des courbes et surfaces
- comptage de points des variétés sur les corps finis
- algorithmique des variétés algébriques : diviseurs, revêtements, jacobiennes de courbes
- cryptographie asymétrique : courbes elliptiques, couplages et formes multilinéaires
- calcul multipartite, partage de secrets, preuves zero-knowledge

Christophe Levrat

88 boulevard Arago
75014 Paris
France

(+33) 7 86 83 13 72

christophe.levrat
@telecom-paris.fr

Langues

Français (bilingue)
Allemand (bilingue)
Anglais (niveau C2)

Programmation

Go
Python

Calcul formel

Magma
Sage
Maple

Expérience

2022- **Chercheur post-doctoral** — Télécom Paris, LTCI, équipe C²
Responsable : M. Rambaud

2019-2022 **Doctorant** — Sorbonne Université, IMJ-PRG
Directeurs : F. Orgogozo, D. Madore

2020-2022 **Organisation du séminaire des thésards** — Sorbonne Université

04-07 2018 **Stage de recherche** — INRIA Saclay, équipe GRACE
Tours de courbes de Shimura
Encadrant : M. Rambaud

Enseignement

2024 **TD et TP informatiques** — ENSTA Paris
Mathématiques discrètes pour la protection de l'information (14h)

2022-2024 **Cours et TP informatiques** — Télécom Paris
Analyse numérique et optimisation (30h), Théorie des langages (15h), Algorithmes et fondements de l'informatique (12h)

2019-2022 **TD et colles** — Sorbonne Université
Maths pour les sciences (L1, 54h), Algèbre linéaire (L2, 36h), Théorie des groupes (L3, 72h), Colles (L2/L3, 40h)

Exposés (conférences)

juillet 2023 — **JA2023** — Nancy, France
Journées Arithmétiques
Curves are algebraic K(π,1): theory and practice

juin 2023 — **AGC²T** — CIRM, France
Arithmetic, Geometry, Cryptography and Coding Theory
Computing the cohomology of π_1-modules trivialised by hyperelliptic covers

février 2023 — **COGNAC** — CIRM, France
Conference On alGebraic varieties over fiNite fields and Algebraic geometry Codes
Computing the cohomology of constructible sheaves on curves

Exposés (séminaires)

février 2024 — **Séminaire CANARI** — INRIA Bordeaux
ℓ-adic point counting on surfaces: nearly almost halfway there?

mai 2023 — **Séminaire Géométrie et Algèbre Effectives** — IRMAR, Rennes
Point counting, dividing in the Jacobian, and étale cohomology

mars 2023 — **Séminaire de l'équipe GRACE** — Inria Saclay
Cohomologie étale des courbes et comptage de points sur les surfaces

octobre 2022 — **Seminar on Algebraic Geometry and Ramification** — en ligne
Computing the étale cohomology of constructible sheaves on curves

novembre 2019 — **Séminaire des doctorants du LAREMA** — Angers
Pourquoi calculer la cohomologie étale ?

Poster

avril 2023 — **Journées nationales du GDR IM** — Université Paris Cité
On the complexity of computing étale cohomology

Diffusion de la science

avril 2023 — **Pré-conférences "Un texte, un mathématicien"**
Préparation au cycle de conférences à la BNF organisé par la SMF et Animath

2021-2022 — **Rencontres avec des collégiens stagiaires** — Sorbonne Université

Formation et diplômes

2022 **Qualification aux fonctions de MCF** CNU section 25

2022 **Doctorat** Sorbonne Université - Paris VI
Thèse soutenue le 30 septembre 2022 devant le jury composé de MM: Couvreur, Kahn, Lombardo, Madore, Orgogozo, Randriam
Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe

2019 **M2** Mathématiques Fondamentales Sorbonne Université - Paris VI
Mémoire : *Cohomologie étale et comptage de points*
Mention B

2018 **Master** Mathématiques et applications UVSQ / Université Paris-Saclay
Algèbre appliquée à la cryptologie et au calcul formel
Projet de programmation : *Pairing the volcano*
Mémoire : *Tours de courbes de Shimura*
Mention TB, rang : 1

2016 **Licence** Mathématiques Université de Lorraine
Mémoire : Symbole de Legendre et réciprocité quadratique
Mention TB, rang : 1

2012 **Baccalauréat scientifique** Lycée La Malgrange
Mention TB

Résumé des travaux de recherche

Travaux en mathématiques

Mes travaux de recherche portent jusqu'à présent sur l'algorithmique des courbes algébriques, en particulier le calcul de groupes de cohomologié étale en vue de l'application au comptage de points sur les surfaces algébriques. L'algorithmique des courbes et de leurs jacobiennes joue un rôle de plus en plus important en cryptographie, et les outils de géométrie algébrique utilisés (notamment dans la cryptanalyse de SIDH [Castryck, Decru, '22]) sont de plus en plus pointus.

• Thèse (soutenue le 30 septembre 2022) :
Calcul effectif de la cohomologie des faisceaux constructibles sur le sité étale d'une courbe
Le travail de ma thèse est centré autour du calcul algorithmique de complexes de cohomologie étale, en vue de l'utilisation ultérieure dans des algorithmes de comptage de points sur les surfaces. En particulier, il est question de faisceaux constructibles sur une courbe définie sur un corps algébriquement clos. Les résultats principaux de la thèse sont une expression explicite du complexe de cohomologie d'un tel faisceau muni de son action galoisienne, ainsi que la description d'un algorithme calculant ce complexe de cohomologie, assorti d'une majoration de sa complexité. La thèse contient de plus une étude de différentes représentations algorithmiques des faisceaux constructibles, ainsi que des descriptions concrètes de certaines opérations sur ces faisceaux. La praticabilité des différents algorithmes est illustrée par des exemples concrets, traités à l'aide des logiciels de calcul formel SageMath et Magma. Ces travaux ont mené aux deux articles suivants, qui seront soumis en juin-juillet.

1. Prépublication (soumise) :
Computing the cohomology of constructible étale sheaves on curves

Cet article généralise les résultats de la thèse aux courbes à singularités quelconques, ainsi qu'aux corps de dimension cohomologique 1 : cela inclut le cas des courbes sur les corps finis, qui a un intérêt en cryptographie (voir projet de recherche). Une stratégie pour réduire la complexité dans le cas des courbes sur les corps finis est présentée, de même qu'une description des difficultés restant à surmonter pour aboutir à un algorithme de comptage de points sur les surfaces. Ces travaux ont été présentés aux conférences COGNAC (février 2023) et AGC^{2}T (juin 2023) au CIRM.

2. Prépublication (à soumettre prochainement) :
Curves are K(π,1): theoretical and practical aspects

La cohomologie étale d'un faisceau lisse sur courbe algébrique géométriquement connexe X est celle du $\pi_1(X)$-module associé. Dans cet article, nous démontrons ce résultat – déjà bien connu dans le cas particulier des courbes courbes lisses irréductibles sur un corps algébriquement clos – dans le cas des courbes (possiblement singulières) avec un point rationnel sur un corps et donnons explicitement des revêtements de X dont les groupes de cohomologie permettent de calculer ceux des faisceaux localement constants sur X. Ceci permet en particulier de décrire explicitement les cup-produits dans la cohomologie de la courbe en termes de cup-produits de cohomologie des groupes finis. Ces travaux ont été présentés aux Journées Arithmétiques à Nancy en juillet 2023.

Travaux en cryptographie

J'ai participé à plusieurs travaux de recherche en cryptographie, plus spécifiquement en calcul multipartite (MPC). J'ai notamment travaillé dans ce cadre sur les protocoles de partage de secret et les protocoles de preuve à divulgation nulle de connaissance (zero-knowledge). Ces travaux ont été assortis d'implémentations en go avec la librairie gnark-crypto. Cette librairie représente l'état de l'art en termes d'implémentation de combinaisons linéaires et de couplages sur les courbes elliptiques. Deux de ces projets ont mené aux prépublications suivantes.

1. Prépublication (avec Matthieu Rambaud et Antoine Urban) : *Breaking the* $t < n/3$ *Consensus Bound: Asynchronous Dynamic Proactive Secret Sharing under Honest Majority*

Cet article présente un protocole de partage de secret dynamique proactif en réseau asynchrone, dans lequel un comité "sortant" de joueurs détenant chacun une part d'un secret transmet de nouvelles parts de ce même secret à un comité "entrant" (cette opération est appelée *refresh*). L'originalité de ce protocole est de permettre n'importe quel nombre $t<n/2$ de corruptions parmi les n joueurs du comité sortant. Mes contributions personnelles à l'article sont en particulier la mise au point d'une méthode optimisée de vérification en batch de preuves zero-knowledge considérées dans le refresh, l'implémentation en go du calcul et de la vérification de ces preuves, ainsi que la comparaison du temps d'exécution avec des preuves NIZK existantes (le temps de vérification est divisé par environ 50 par rapport à l'état de l'art).

2. Prépublication (avec Matthieu Rambaud) :
Proofs of non-Supermajority: the missing link for two-phase BFT with responsive view-change and linear complexity
Cet article présente les preuves de non-supermajorité (PnS) : un type de protocole permettant à des joueurs, dont certains sont corrompus, et ayant chacun une valeur v, de rapporter cette valeur à un prouveur ; celui-ci, étant donné un certain nombre de telles valeurs, peut alors construire une preuve succincte qu'au moins un certain nombre de joueurs honnêtes ont une valeur inférieure à la plus grande valeur rapportée. L'article présente un protocole de consensus (BFT) basé sur les PnS, ainsi que différentes instanciations de PnS, notamment une à base de multisignatures BLS. J'ai réalisé l'implémentation en go, notamment une accélération des signatures agrégées à base de couplages (on obtient une division par 50 du temps de calcul par rapport à l'état de l'art).

Activités d'enseignement

Depuis le début de ma thèse, j'ai effectué des enseignements variés :

- à tous les niveaux de bac+1 à bac+4 ;
- à des publics divers, allant de futurs ingénieurs mécaniciens à des futurs mathématiciens ;
- sous différents formats : cours, TD, colles, TP informatiques ;
- en présence et en visioconférence.

TD à Sorbonne Université (2019-2022

• Mathématiques pour les études scientifiques I (L1, 54h) : Au sein de cette UE destinée à l'ensemble des étudiants en licence scientifique, j'ai enseigné à des étudiants dans un parcours spécifique d'ingénierie mécanique. L'enseignement portait principalement sur l'analyse réelle : intégration, développements limités, équations différentielles linéaires... ainsi que sur les polynômes et les nombres complexes.

• Algèbre linéaire et bilinéaire IIb (L2, 18h) : Cet enseignement, destiné aux étudiants en licence monodisciplinaire de mathématiques, portait sur les aspects théoriques de la réduction des endomorphismes. J'ai enseigné, entièrement à distance avec BigBlueButton, les critères usuels de diagonalisation et trigonalisation, les réductions de Dunford et de Jordan.

• Algèbre (L3, 2x36h) : J'ai effectué ces TD deux années de suite, une fois partiellement à distance, et une fois entièrement en présentiel. J'étais en charge du groupe des étudiants en licence monodisciplinaire intensive, qui se destinent majoritairement à un master recherche. Cette UE, qui portait essentiellement sur la théorie des groupes, était également l'occasion d'aborder des notions plus avancées comme les catégories et foncteurs.

Colles à Sorbonne Université (2019-2022)

J'ai également donné des colles en L2 et L3 à Sorbonne Université ; ressemblant à celles habituellement dispensées en classes prépa, ces colles sont l'occasion pour les étudiants de se confronter à leurs difficultés, et de voir sous un angle différent les notions abordées en cours et en TD.

• Algèbre linéaire et bilinéaire IIa (L2, 3x10h) : J'ai donné ces colles 3 années de suite, tantôt sur place, tantôt à distance. Cette UE comportait des rappels d'algèbre linéaire, ainsi que diverses méthodes pratiques de réduction des endomorphismes. Ces colles m'ont permis de mieux cerner les difficultés rencontrées par les étudiants en double licence maths-physique ou maths-info, et d'apprendre à varier les explications données en fonction du mode de pensée de chaque étudiant.

• Topologie et calcul différentiel (L3, 10h) : Ces colles à distance, données à des étudiants de double licence maths-physique, portaient essentiellement sur la topologie des espaces métriques, ainsi que sur la différentiabilité.

Cours et TP à Télécom Paris (2022-2023)

• Analyse numérique et optimisation (bac+4, 30h) : Cette UE donne une introduction aux techniques usuelles d'analyse numérique, ainsi qu'à l'optimisation linéaire et non linéaire. J'ai enseigné dans cette UE deux années de suite, et encadré des TP en java visant à implémenter l'algorithme du simplexe ainsi qu'une méthode de descente du gradient.

• Théorie des langages (bac+3, 15h) : Ce cours, dispensé au second semestre à tous les élèves de première année de Télécom, comporte une partie sur les automates et langages rationnels, une partie sur les grammaires hors contexte et langages algébriques, et une partie sur les notions de calculabilité et complexité.

Diffusion de la science

• Au cours de ma thèse, j'ai participé à l'activité "interview d'un chercheur" proposée aux collégiens effectuant leur stage de troisième à Sorbonne Université. Elle consiste en un dialogue d'une heure avec des stagiaires, afin de leur présenter les différents métiers de la recherche, et également de leur donner une image des mathématiques pratiquées à l'université. Ces échanges, toujours très francs, permettent de déconstruire certains préjugés liés à la recherche ou aux mathématiques, et d'encourager les élèves à s'intéresser à cette discipline et aux débouchés des études qui lui sont associées.

• En avril 2023, j'ai participé à la préparation de classes de lycée aux conférences du cycle "Un texte, un mathématicien" organisé par la Société Mathématique de France, la Bibliothèque Nationale de France, et l'association Animath. Cette préparation consiste en une séance d'une ou deux heures avec une classe de lycée, qui est l'occasion non seulement de présenter le sujet de la conférence et quelques outils mathématiques pour la comprendre, mais surtout de parler des applications des mathématiques et des métiers qui y sont associés.

Organisation de séminaires

J'ai fait partie, de 2020 à 2022, de l'équipe d'organisation du Séminaire des Thésards de l'IMJ-PRG. Ce séminaire, qui a lieu toutes les deux semaines tantôt à Sorbonne Université, tantôt à l'Université Paris Cité, permet à tous les doctorants du laboratoire, quelle que soit leur thématique de prédilection ou leur avancement dans la thèse, de présenter leur sujet de recherche et, le cas échéant, leurs résultats. J'ai participé aux aspects usuels de l'organisation d'un séminaire : recherche d'orateurs, réservation de salles, organisation d'un pot suivant l'exposé... mais également à une tradition propre au Séminaire des Thésards : la répétition des exposés par les orateurs la semaine précédant leur intervention. Ce processus permet d'une part de rassurer les orateurs dont c'est souvent le premier exposé de recherche, et également de leur donner un retour franc sur leur prestation et leur façon de présenter. Cette expérience m'a permis de me confronter à de nombreuses problématiques liées aux exposés de séminaire, allant de la gestion du tableau à la nécessité d'adapter le contenu de l'exposé au public présent dans la salle.