Curriculum Vitae

Christophe Levrat

1 Résumé

1.1 Informations personnelles

- Nom : Christophe Nicolas LEVRAT
- Date de naissance : 22/06/1994
- Lieu de naissance : Regensburg (Allemagne)
- Nationalités : Française, Allemande

1.2 Expérience professionnelle

2024 –	Post-doctorant dans l'équipe GRACE Directeurs : Alain Couvreur, Hugues Randriam	INRIA Saclay
2022-2024	Post-doctorant dans l'équipe C^2 Directeur : Matthieu Rambaud	LTCI, Télécom Paris
2019-2022	Doctorant dans l'équipe Théorie des Nombres Directeurs : David Madore, Fabrice Orgogozo	IMJ-PRG, Sorbonne Université
2018	Stagiaire dans l'équipe GRACE Encadrant : Matthieu Rambaud	INRIA Saclay

1.3 Formation et diplômes

2022	Qualification aux fonctions de Maître de Conférences	CNU section 25
2022	Thèse de doctorat Titre : Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe Soutenue le 30 septembre 2022 Jury : MM Couvreur, Kahn, Lombardo, Madore, Orgogozo, Randriambololona	Sorbonne Université
2019	Master mathématiques fondamentales Mémoire : Cohomologie étale et comptage de points Mention B	Sorbonne Université
2018	Master Algèbre appliquée Projet de programmation : Pairing the volcano Mémoire : Tours de courbes de Shimura Mention TB, rang : 1	Université Paris-Saclay
2016	Licence Mathématiques Mention TB, rang : 1	Université de Lorraine
2012	Baccalauréat général, série scientifique Mention TB	Lycée La Malgrange

2 Liste des travaux de recherche

2.1 Articles publiés ou acceptés pour publication

1. *A Divide-and-Conquer Sumcheck Protocol*
Christophe Levrat, Tanguy Medevielle, Jade Nardi
à paraître dans IACR Communications in Cryptology, Vol. 2, No.1 (2025).
2. *Curves are algebraic $K(\pi, 1)$: theoretical and practical aspects*
Christophe Levrat
Bulletin of the London Mathematical Society, Vol. 56, No. 12 (2024) : pp 3601-3622.
doi : <https://doi.org/10.1112/blms.13153>
3. *Computing the cohomology of constructible étale sheaves on curves*
Christophe Levrat
Journal de Théorie des Nombres de Bordeaux, Vol. 36, No. 3 (2024) : pp 1085-1122.
doi : <https://doi.org/10.5802/jtnb.1309>

2.2 Prépublications

1. *Highway to Hull : An Algorithm Solving the General Matrix Code Equivalence Problem*
Alain Couvreur, Christophe Levrat
2. *Breaking the $t < n/3$ Consensus Bound : Asynchronous Dynamic Proactive Secret Sharing under Honest Majority*
Christophe Levrat, Matthieu Rambaud, Antoine Urban
eprint : <https://eprint.iacr.org/2022/619>
3. *Practical Non-interactive Multi-signatures, and a Multi-to-Aggregate Signatures Compiler*
Christophe Levrat, Matthieu Rambaud
eprint : <https://eprint.iacr.org/2024/1081>
4. *Proofs of non-Supermajority : the missing link for two-phase BFT with responsive view-change and linear complexity*
Christophe Levrat, Matthieu Rambaud
eprint : <https://eprint.iacr.org/2020/1480>

2.3 Article en préparation

1. *Effective Artin-Schreier-Witt theory for curves*
Christophe Levrat, Rubén Muñoz--Bertrand

3 Communications

3.1 Conférences

- Journées Codage et Cryptographie Pornichet
A Divide-and-Conquer Sumcheck Protocol avril 2025
- Journées arithmétiques Nancy
Curves are algebraic $K(\pi,1)$: Theoretical and practical aspects juillet 2023
- Conférence AGC²T CIRM
Computing the cohomology of π_1 -modules trivialized by a hyperelliptic cover juin 2023
- Conférence COGNAC CIRM
Computing the cohomology of constructible étale sheaves on curves février 2023

3.2 Séminaires

- Séminaire de l'équipe Crypto Université de Versailles
A new algorithm solving the matrix code equivalence problem mars 2025
- Séminaire de l'équipe ATI Aix-Marseille Université
Actually computing the étale cohomology of curves novembre 2024
- Séminaire de théorie des nombres. Université de Besançon
Cohomologie étale des courbes octobre 2024
- Séminaire de l'équipe AGC3 Université Paris 8
A history of Diophantine equations in cryptography mai 2024
- Séminaire de l'équipe CANARI INRIA Bordeaux
 ℓ -adic point counting on surfaces : nearly almost halfway there ? février 2024
- Séminaire Géométrie et Algèbre Effectives Université de Rennes
Point counting, dividing in the Jacobian, and étale cohomology mai 2023
- Séminaire de l'équipe GRACE INRIA Saclay
Cohomologie étale des courbes et comptage de points sur les surfaces mars 2023
- Seminar on Algebraic Geometry and Ramification (en ligne)
Computing the étale cohomology of constructible sheaves on curves octobre 2022
- Séminaire des thésards Université d'Angers
Pourquoi calculer la cohomologie étale ? novembre 2019

3.3 Groupes de travail

- Retraite de l'ANR BARRACUDA Université Paris 8
Construction de revêtements d'Artin-Schreier de courbes janvier 2025
- Groupe de travail GODZILLA INRIA Saclay
Introduction to algebraic curves juillet 2024
- Retraite de l'ANR BARRACUDA IHP
Cohomologie étale des courbes et surfaces janvier 2024
- Groupe de travail sur la conjecture de Weil pour les nombres de Tamagawa ENS Paris
Groupes algébriques mars 2020
Introduction à la cohomologie étale octobre 2019

4 Rapport sur l'enseignement effectué

Depuis le début de ma thèse, j'ai effectué des enseignements variés, à l'université et en école d'ingénieur. J'ai donné des cours, TD, TP et colles de mathématiques ou d'informatique, à des niveaux allant de bac+1 à bac+4. J'ai également choisi d'enseigner durant chaque année de post-doctorat. Mes enseignements sont résumés dans le tableau ci-dessous, et décrits en détail par la suite.

Année	Lieu	Matière	Niveau	Heures	CM	TD	TP	Colles	Respo UE
24,25	EN	Mathématiques pour la protection de l'information	M1	24h		✓	✓		
24	P8	Théorie de l'information	M1	30h	✓	✓	✓		✓
24	TP	Algorithmique et fondements de l'informatique	L3	14h	✓		✓		
23	TP	Théorie des langages	L3	15h	✓				
22,23	TP	Analyse numérique et optimisation	M1	30h	✓		✓		
20-22	SU	Algèbre linéaire et bilinéaire IIa	L2	30h				✓	
21	SU	Topologie et calcul différentiel	L3	10h				✓	
21	SU	Algèbre linéaire et bilinéaire IIb	L2	18h				✓	
20,21	SU	Théorie des groupes	L3	72h		✓			
19	SU	Mathématiques pour les études scientifiques	L1	54h		✓			

EN = ENSTA Paris, P8 = Université Paris 8, TP = Télécom Paris, SU = Sorbonne Université.

4.1 Cours, TD, TP à l'Université Paris 8 (2024)

- Théorie de l'information (M1, 30h) : J'ai été responsable de cette UE qui fait partie du master Arithmétique, Codage, Cryptographie de l'Université Paris 8. J'étais chargé de l'ensemble de l'enseignement, ainsi que la production du matériel pédagogique (feuilles de TD/TP). Il s'agit d'un cours sur les notions d'entropie et d'information mutuelle, le codage des sources sans mémoire ou markoviennes, ainsi que le codage de canal, assorti de séances de TD et TP informatique. Ce cours est l'occasion d'insister sur le développement d'une théorie mathématique décrite par Claude Shannon dans un contexte historique particulier, et qui a encore des applications aujourd'hui.

4.2 TD/TP à l'ENSTA Paris (2024-2025)

- Mathématiques discrètes pour la protection de l'information (14h) : Cette unité donne essentiellement une introduction à la théorie des corps finis à des élèves-ingénieurs n'ayant pas eu de cours d'algèbre depuis les classes préparatoires. J'ai encadré les séances d'exercices et les séances de programmation C visant à implanter les opérations de base du corps à 256 éléments.

4.3 Cours et TP à Télécom Paris (2022-2024)

- Théorie des langages (bac+3, 15h) : J'ai donné des cours magistraux dans cette UE, dispensée au second semestre à tous les élèves de première année de Télécom. Elle 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.
- Algorithmique et fondements de l'informatique (bac+3, 14h) : J'ai encadré dans cette UE des TP en Python sur la théorie des graphes, et donné des cours sur la théorie des langages ainsi que la théorie de la complexité.

- 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 dispensé des cours magistraux 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.

4.4 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.

4.5 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 préparatoires, 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.

5 Autres responsabilités et activités

5.1 Organisation de séminaires

(2020-2022) Séminaire des Thésards de l'IMJ-PRG 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 scientifiques, allant de la gestion du tableau à la nécessité d'adapter le contenu de l'exposé au public présent dans la salle.

5.2 Encadrement d'étudiant

J'encadre actuellement le TER de Raphael Leonardi, étudiant en L3 magistère d'informatique à l'Université Paris-Saclay. Son TER porte sur le protocole Bulletproofs [Bün+18] de preuve de connaissance d'un antécédent, lié par un engagement, d'un élément par une forme bilinéaire donnée. J'encadrerai de mai à juillet 2025 son stage de L3, qui consistera en l'évolution des différentes versions du protocole de chiffrement post-quantique HQC [Mel+18], récemment sélectionné par le NIST pour être l'un des standards de chiffrement post-quantique.

5.3 Médiation et diffusion de la science

(2023) Pré-conférences "Un texte, un mathématicien" En avril 2023, j'ai participé à la préparation de deux classes de lycée des villes de Pantin et Bobigny aux conférences du cycle "Un texte, un mathématicien" (désormais dénommé "Un texte, une aventure mathématique") 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. Étant sur le point de choisir leur orientation pour les études supérieures, ces élèves ont de nombreux questionnements – et malheureusement aussi des inquiétudes – liés aux filières d'études faisant intervenir les mathématiques. Ces séances permettaient entre autres de rassurer les élèves quant à leur légitimité à s'engager dans ces cursus.

(2021-2022) Activité "interview d'un chercheur" Au cours de ma thèse, j'ai participé à l'activité "interview d'un chercheur" proposée aux collégien.ne.s effectuant leur stage de classe de troisième à Sorbonne Université. Elle consiste en un dialogue d'une heure avec les 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.

Références

- [Bün+18] Benedikt BÜNZ et al. “Bulletproofs : Short proofs for confidential transactions and more”. In : *2018 IEEE symposium on security and privacy (SP)*. IEEE. 2018, p. 315-334.
- [Mel+18] Carlos Aguilar MELCHOR et al. “Hamming quasi-cyclic (HQC)”. In : *NIST PQC Round 2.4* (2018), p. 13.