Maxime BROS

7, rue des Écoles
87 000 Limoges
France
06 43 88 66 52
maxime_bros@unilim.fr
Né le 03/10/1992 à Besançon
Permis B et véhicule

Doctorant en Mathématiques et Informatique
Titulaire d'un Master en Mathématiques Appliquées
(Spécialité Cryptographie, Université de Limoges)

Expérience professionnelle

2019-2022 (en cours) **Doctorat en Mathématiques et Informatique à Xlim (Limoges) (UMR CNRS numéro 7252)**, *Encadré par* ***Philippe Gaborit et Vincent Neiger***, Attaques algébriques sur les cryptosystèmes en métrique rang.

Mars 2019 (6 mois) **Stage de recherche à Xlim**, *Encadré par* ***Philippe Gaborit, Olivier Ruatta et Vincent Neiger***, Évaluation de la complexité des attaques algébriques (par calcul de bases de Gröbner) sur les cryptosystèmes en métrique rang.

Juin 2018 (1 mois) **Stage de recherche à Xlim**, *Encadré par* ***Christophe Clavier***, Attaques par canaux auxiliaires (CPA, DPA et recherches de distingueurs pour la méthode Scatter), Rédaction d'un article en cours).

2016–2017 puis 2019 **Tuteur en Mathématiques**, *CDD auprès de l'Université de Bourgogne puis enseignant particulier*, Niveau Licence et prépa-intégrée, Statistiques et Analyse de données, Analyse et Algèbre.

Formation

2017–2019 **Master 1 et 2 de Mathématiques Appliquées : parcours Cryptologie (CRYPTIS)**, *Université de Limoges*.

- **Major de promotion et mention Très Bien en Master 1 et 2.**
  Moyennes générales : 16.5/20 en Master 1 et 17.5/20 en Master 2.
- **Délégué de la promotion Mathématiques et membre de la Commission de Perfectionnement des Masters.**
- **Titulaire d'une bourse au mérite de la région Aquitaine de 3000 €.**
- *Cours suivis* : Complexité et Calculabilité, Algèbre (Arithmétique, Théorie des Nombres, Corps Finis et courbes elliptiques), Réseaux et Systèmes, Algorithmique et Programmation, Statistiques, Calcul Formel (Note obtenue au projet (théorie + pratique + soutenance) : 20/20), Sécurité Informatique, Codes correcteurs, Systèmes Polynomiaux, Cryptographie à clé secrète et publique, Mécanismes cryptographiques, Développement de logiciels cryptographiques, Cryptographie post-quantique basée sur les réseaux et les codes et Cryptographie quantique).
- *Mémoire de recherche (1er semestre M2) :* « Attaques par Cryptanalyse Algébrique sur MinRank » sous la direction d'Olivier Ruatta (Note obtenue : 17/20).
- *Mémoire de recherche (M1) :* « Blockchain technology : analysis of the privacy of Bitcoin and zero-knowledge proof in the Zcash network » sous la direction de Phan Duong Hieu (Note obtenue : 17/20).

2016–2017 **Niveau Master 1 de Mathématiques Fondamentales**, *Université de Bourgogne*, Dijon.

- *Mémoire de recherche :* « Démonstration combinatoire du Théorème de Wigner (sur le spectre des matrices aléatoires de grandes tailles) et recherche d'une vitesse de convergence pour les fonctions de répartition empiriques »
  (Note obtenue (rapport + soutenance) : 15/20)

2015–2016 **Licence 3 de Mathématiques**, *Université de Bourgogne*, Dijon.

- *Options choisies* : Variable complexe, Probabilités, Analyse Fonctionnelle.
- *Mémoire :* « Démonstration de la Loi Faible des Grands Nombres par La Vallée Poussin, théorème de Moivre-Laplace et application à la méthode Monte-Carlo et au théorème de Stone-Weierstrass » (Note obtenue (rapport + soutenance) : 18.5/20)

2013–2014 **Niveau Licence 3 en Informatique**, *Université de Bourgogne*, Dijon.

Intérêt particulier pour le Langage Formel, le λ-Calcul et les modèles mathématiques du traitement d'image (tatouages, compression, etc.)

2012–2013 **Admission à l'École Normale Supérieure de Lyon et de Paris (Ulm)**, *Licence 3 Informatique*.

Titulaire d'une bourse de mérite Paris-Sciences-Lettres (PSL) d'un montant de 1200 € par mois (accordée en Septembre 2012 à l'ENS de Paris Ulm)

Cours suivis :

- **Algorithmique** avec Jacques Stern, Claire Mathieu et Damien Vergnaud.
- **Compilation** avec Jean-Christophe Filliâtre.
- **Langages Formels, Calculabilité et Complexité** avec Eugène Asarin.
- **Système Digital** avec Jean Vuillemin.
- **Structures et Algorithmes Aléatoires** avec Anne Bouillard.

2010–2012 **Licence 1 et 2 d'Informatique**, *Université de Franche-Comté*, Besançon.

Major de promotion en Licence 2.

2010 **Baccalauréat Série Scientifique - Europe Anglais**, *Lycée C.- N. Ledoux*, Besançon.

Mention Très Bien - Félicitations du Jury (18.02 / 20)

Présentations, séminaires ou conférences

Intervention lors des Journées des Matrices Structurées 2019 à Limoges.

- *Sujet :* "Generalized Sparse Matrices and Applications to Decoding and Cryptography".
- *Dates :* 23-24 Mai 2019.
- *Durée :* 30 minutes.

Conférences de vulgarisation sur les liens entre Cryptologie et Mathématiques.

- *Dates :* Printemps 2018.
- *Durée et lieu :* 1 heure 30 minutes, à l'Université de Limoges et dans 2 lycées de Haute-Vienne.
- *Public :* mélange entre des classes de Seconde et de Terminale.

Compétences en Cryptologie et Sécurité de l'Information

- Cryptosystèmes antiques et histoire de la Cryptographie moderne (de la machine Enigma à la cryptographie post-quantique, en passant par l'AES).
- Connaissances avancées des chiffrements DES, AES (que j'ai implémentés en C) et des fonctions de hachage MD5, SHA1 et SHA256. Je dispose aussi de connaissances sur leur cryptanalyse : cryptanalyse différentielle, attaque square à 6 tours de l'AES, etc.
- Cryptographie à clé publique (RSA, El-Gamal, Paillier), signatures DSA, ECDSA et One-Time-Signature basée sur les fonctions de hachages, zero-knowledge-proof authentication et zero-knowledge-proof-of-work, connaissances sur les blockchains et sur les courbes elliptiques.
- Cryptographie post-quantique : cryptosystèmes basés sur codes correcteurs d'erreurs, en

métrique de Hamming et en métrique rang.
- Cryptanalyse algébrique : attaque par mise en équations puis résolution par base de Gröbner et calcul d'immunité algébrique.
- Attaque par canaux auxiliaires : DPA, CPA, Scatter.
- Intérêt particulier pour la génération de nombres pseudo-aléatoires et les tests statistiques de ces derniers. Je m'intéresse en particulier aux comportements "aléatoires" dans les corps finis.
- Stéganographie : intérêt particulier pour le tatouage d'image (par exemple par FFT : projet implémenté en 2013).
- Autres : quelques connaissances en machine learning (deep learning).

Langages informatiques maitrisés

Généraux, *C, Ocaml, Assembleur MIPS (code machine), C++, Python, Java*.
Mathématiques et calcul formel, *Ocaml, Maple, SAGE, MAGMA, R, Scilab*.
Web et Base de Données, *PHP, HTML, CSS, SQL*.
LaTeX, *Bibliothèque Maths, Tikz (graphique), Beamer*.

Langues

Français	Langue maternelle	
Anglais	Lu, parlé, écrit	*Niveau Courant*
Espagnol	Lu, parlé, écrit	*Niveau Intermédiaire*

Centres d'intérêts

Lecture	*Philosophie et littérature classique* : Descartes, Maupassant, Voltaire, Montesquieu, Freud. *Littérature mathématique* : Bernoulli, Euclide, Cormen-Leiserson-Rivest (algorithmique générale), D. Vergnaud et Stinson (cryptologie), Cox (systèmes polynomiaux), Lidl et Niederreiter (corps finis).
Cinéma et séries	Tout type de films et séries : du cinéma d'animation aux films d'action en passant par les films d'auteurs. Liste absolument non exhaustive : *Matrix, Black Mirror, Un homme d'exception, L'homme qui défiait l'infini, Le bureau des légendes, Stranger Things, Le magasin des suicides, Némo, Polisse, Un prophète, Persepolis, OSS 117, Ratatouille, Titanic, La vie d'Adèle, Manhattan,...*
Sport	Course à pied, natation et fitness.