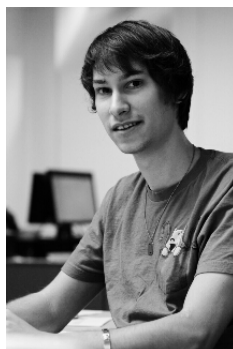


Florian BOURSE



INFORMATIONS PERSONNELLES

NATIONALITÉ : Française
DATE DE NAISSANCE : 2 juillet 1991
ADRESSE : 11 route départementale 50, 59990 Sebourg, France
TÉL. : +33 6 29 68 67 22
MÉL. : florian.bourse@ens.fr
PAGE PERSONELLE : <https://www.di.ens.fr/~fbourse/>

EXPERIENCE PROFESSIONNELLE

SEPTEMBRE 2022 –	Enseignement de l'informatique en CPGE MP2I/MPI Lycée Colbert – Tourcoing
SEPTEMBRE 2018 –	Professeur agrégé de mathématiques Titularisé le 1er septembre 2019
JANVIER 2018 – AOUT 2018	Chercheur postdoctoral chez Orange Labs, Cesson-Sévigné. Searchable Encryption
MARS 2014 – AOUT 2014	Stage dans l'équipe CRYPTO du département d'informatique de l'ÉNS. Functional Encryption
MARS 2013 – AOUT 2013	Stage INRIA-Microsoft Research. Balanced Graph Edge Partition

FORMATION

2018 – 2019 Diplôme universitaire Entrer dans le métier d'enseignant, ESPE de Valenciennes
2014 – 2017 Thèse dirigée par Michel Abdalla et David Pointcheval,
département d'informatique de l'École normale supérieure, Paris
Functional Encryption for Inner-Product Evaluations
2012 – 2014 Master Parisien de Recherche en Informatique, Université Paris Diderot - Paris 7, Paris
2011 – 2014 École normale supérieure, Paris
Études supérieure d'informatique et formation à la recherche
2009 – 2011 Classes préparatoires aux Grandes Écoles, Lycée Wallon, Valenciennes
*Section MPSI puis MP**

DIPLÔMES

- SEPT. 2021 Certification discipline non linguistique
Mathématiques en anglais
- SEPT. 2019 Diplôme universitaire à l'École Supérieure du Professorat et de l'éducation de Valenciennes
Entrer (enseignement au second degré)
- JUIL. 2018 Lauréat du concours de l'agrégation externe spéciale de mathématiques, 13e
- DÉC. 2017 Thèse de Doctorat de l'Université de recherche Paris Sciences et Lettres
Préparée à l'École normale supérieure
- SEPT. 2014 Diplôme de l'ÉNS
Master Parisien de Recherche en Informatique, mention Bien
- SEPT. 2012 Licence d'informatique, mention Bien
- JUIL. 2009 Baccalauréat, mention Bien

LANGUES

- FRANÇAIS : Langue maternelle
ANGLAIS : Courant
ALLEMAND : Intermédiaire

INFORMATIQUE

LANGAGES : Python, C/C++, C#, Java, Bash, OCaml, Haskell, HTML/CSS, JavaScript, LaTeX, SQL

PUBLICATIONS

Par souci de maintenabilité, la liste des publications est triée par ordre chronologique. Pour une liste triée par pertinence, [mon profil sur Google Scholar](#) vous permet d'accéder à une liste triée par nombre de citations.

- Florian Bourse, Malika Izabachène,
Plug-and-play sanitization for TFHE. ePrint.
- Michel Abdalla, Florian Bourse, Hugo Marival, David Pointcheval, Azam Soleimanian, Hendrik Waldner,
Multi-client inner-product functional encryption in the random-oracle model. SCN 2020.
- Florian Bourse, Olivier Sanders, Jacques Traoré,
Improved Secure Integer Comparison via Homomorphic Encryption. CT-RSA 2020.
- Florian Bourse, David Pointcheval, Olivier Sanders,
Divisible E-Cash from Constrained Pseudo-Random Functions. Asiacrypt 2019.
- Florian Bourse, Michele Minelli, Matthias Minihold, Pascal Paillier,
Fast Homomorphic Evaluation of Deep Discretized Neural Networks. Crypto 2018.
- Fabrice Benhamouda, Florian Bourse, Helger Lipmaa,
CCA-secure inner-product functional encryption from projective hash functions. PKC 2017.
- Florian Bourse, Rafael Del Pino, Michele Minelli, Hoeteck Wee,
FHE Circuit Privacy Almost For Free. Crypto 2016.

- Michel Abdalla, Florian Bourse, Angelo De Caro, David Pointcheval, *Better Security for Functional Encryption for Inner Product Evaluations*. ePrint.
- Michel Abdalla, Florian Bourse, Angelo De Caro, David Pointcheval, *Simple Functional Encryption Schemes for Inner Products*. PKC 2015.
- Florian Bourse, Marc Lelarge, and Milan Vojnovic, *Balanced Graph Edge Partition*. KDD 2014.
- Antoine Amarilli, Fabrice Ben Hamouda, Florian Bourse, Robin Morisset, David Naccache, Pablo Rauzy, *From Rational Number Reconstruction to Set Reconciliation and File Synchronization*. TGC 2012.

AUTRES PRÉSENTATIONS DANS DES SÉMINAIRES OU COLLOQUES

- 2021 - Séminaire du laboratoire de mathématiques de l'université de Valenciennes
Comment répondre à une question sans connaître la réponse ?
- 2018 - LATCA@BiCi: LATtice Crypto and Algorithms
Function privacy for GSW and efficient sign computation from TFHE
- 2018 - Séminaire Cryptologie & Sécurité - GREYC, Caen
Functional Encryption for Inner-Product Evaluations
- 2017 - Monthly lattice and crypto meeting - ENS Lyon
CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions
- 2016 - Monthly lattice and crypto meeting - ENS Lyon
FHE Circuit Privacy Almost for Free
- 2016 - Workshop HEAT: Homomorphic Encryption Applications and Technology
FHE Circuit Privacy Almost for Free
- 2015 - ESSA@BiCi: Encryption for Secure Search and other Algorithms
Functional Encryption for Inner-Product Evaluations
- 2014 - Séminaire des doctorants de l'ENS Ulm
Functional Encryption for Inner-Product Evaluations

VULGARISATION SCIENTIFIQUE

- Escher en temps réel : fenêtre sur l'infini - L'auto-assemblage algorithmique : un calcul aquatique
Nuit des sciences 2014
- Cryptris: un serious game autour de la cryptographie
Anniversaire 50 ans de l'INRIA; présenté aussi devant des groupes de collégiens et de lycéens à plusieurs reprises.

ACTIVITÉS EN MATIÈRE D'ADMINISTRATION ET AUTRES RESPONSABILITÉS

- Membre du comité de programme de CSCML 2023 (The International Symposium on Cyber Security, Cryptology and Machine Learning)
- Mission d'expertise des sujets de baccalauréat, spécialité NSI.
- Proposition de sujet pour les olympiades de mathématiques en première.

- Reviewer ou sous-reviewer pour plusieurs conférences et journaux (PKC, Eurocrypt, Crypto, Asi-acrypt, CCS, SCN, CANS, ICALP, ETRI Journal, et autres).

ENSEIGNEMENT

- 2022 – Informatique en CPGE, MP2I/MPI
- 2018 – 2021 Mathématiques dans l'enseignement secondaire
- 2018 – 2021 Interrogations orales en CPGE au lycée Henri Wallon, niveau MP et MP*
- 2014 – 2017 mission d'enseignement à l'Université Paris Diderot - Paris 7
- 2016 – 2017 *Introduction à la Programmation en Java* (IP1)
Introduction à la Programmation en C (IP-CPEI)
- 2015 – 2016 *Concepts Informatiques* (CI2)
Analyse de Données Structurées (ADS4)
- 2014 – 2015 *Base de Données* (BD3)
Internet et Outils (IO2)

CENTRES D'INTÉRÊT

- STRATÉGIE : Jeux de plateaux, jeux vidéos, sports
- INFORMATIQUE - SCIENCE DE L'INFORMATION : Internet, Big data, Cryptographie, Machine learning, énigmes
- DIDACTIQUE DES MATHÉMATIQUES : Histoire des mathématiques, vulgarisation scientifique