# Charles Bouillaguet

*né le 21 janvier 1984, nationalité française*

## Postes Précédents

2012– **MCF**, *Université de Lille (Laboratoire CRIStAL).*
2011–2012 **Post-doctorant**, *Université de Versailles/Saint-Quentin en Yvelines (Labo PRiSM).*
2008–2011 **Doctorant**, *Ecole Normale Supérieure*, Paris.
2004–2008 **Élève-fonctionnaire**, *Ecole Normale Supérieur de Cachan.*

## Principales Charges d'enseignement

2018– **TD/TP/CM Cryptographie en M2**, *Sorbonne Université.*
2015– **TD/TP de HPC en M1**, *Sorbonne Université.*
2017 **TD/TP de Bases de données**, *Univ. Lille.*
2014 **Tutorat sportif de haut niveau**, *Sorbonne Université.*
2014–2016 **TP de C et de méthodes numériques en L2**, *Sorbonne Université.*
2014–2019 **TD/TP de Python en L1**, *Sorbonne Université.*
2014–2015 **TP de calcul numérique**, *Polytech'Lille.*
2013–2017 **CM/TP de calcul haute performance en 5ème année**, *Polytech'Lille.*
2013– **TP/TD d'algorithmique en M1**, *Univ. Lille.*
2013– **CM/TD d'histoire et d'épistémologie en M1**, *Univ. Lille.*
2012– **CM/TP/TD de cryptographie en M1**, *Univ. Lille.*
2012–2013 **TP/TD d'algorithmique en L3**, *Univ. Lille.*
2012–2013 **TP/TD de logique en L2**, *Univ. Lille.*
2012–2013 **TP/TD de programmation fonctionnelle en L3**, *Univ. Lille.*
2011–2012 **TD d'algorithmique en L3**, *Ecole Normale supérieure*, Paris.
2009–2011 **TP de programmation en OCaml en MP***, *Lycée Louis-le-Grand*, Paris.
2007-2009 **TD de programmation en C en 1ère année**, *ENSTA*, Paris.
2007-2009 **TP de programmation en Maple en prépa**, *Lycée Lakanal*, Sceaux.

## Encadrement scientifique

2019 **Stage de M1**, *Julia Sauvage*, Cryptanalyse de PRNG.
2019 **Stage de M2**, *Mellila Bouam*, Implantation HPC (3XOR).
2019 **Stage de M2**, *Ryan Lefebvre*, Décomposition modulaire des graphes.
2015-2018 **Co-encadrement de thèse**, *Claire Delaplace*, avec Pierre-Alain Fouque.
2015 **Stage de M2**, *Claire Delaplace*, Algèbre linéaire creuse modulo $p$.
2013 **Stage de M2**, *Laurent Grémy*, Problème LPN .

*Université de Lille – 59655 – Villeneuve d'Ascq Cedex*
*+33 618 221 393* • *charles.bouillaguet@univ-lille.fr*
*https://cbouilla.github.io*

## Publications Scientifiques

| | |
|---|---|
| TOSC '18 | *Revisiting and Improving Algorithms for the 3XOR Problem*, avec C. Delaplace et P.-A. Fouque |
| PASCO '17 | *Parallel Sparse PLUQ Factorization modulo p*, avec C. Delaplace et M.-E. Voge |
| PQ Crypto '17 | *Fast Lattice-Based Encryption: Stretching Spring*, avec C. Delaplace, P.-A. Fouque et P. Kirchner |
| CASC '16 | *Sparse Gaussian Elimination modulo p: an Update*, avec C. Delaplace |
| J. crypto '16 | *New Second-Preimage Attacks on Hash Functions*, avec E. Andreeva, P.-A. Fouque, J. Hoch, J. Kelsey, A. Shamir et S. Zimmer |
| Asiacrypt '14 | *Cryptographic Schemes Based on the ASASA Structure: Black-Box, White-Box, and Public-Key (Extended Abstract)*, avecA. Biryukov et D. Khovratovich |
| Eurocrypt '13 | *Graph-Theoretic Algorithms for the "Isomorphism of Polynomials" Problem*, avec P.-A. Fouque et A. Véber |
| SAC '13 | *Provable Second Preimage Resistance Revisited*, avec B. Vayssière |
| SAC '13 | *Low-Data Complexity Attacks on AES*, avec P. Derbez, O. Dunkelman, P.-A. Fouque, N. Keller et V. Rijmen |
| Asiacrypt '11 | *Practical Key-recovery For All Possible Parameters of SFLASH*, avec P.-A. Fouque et G. Maccario-Rat |
| CRYPTO '11 | *Automatic Search of Attacks on round-reduced AES and Applications*, avec P. Derbez, P.-A. Fouque |
| SAC '11 | *New Insights on Impossible Differential Cryptanalysis*, avec O. Dunkelman, P.-A. Fouque et G. Leurent |
| PKC '11 | *Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial With One Secret Problem*, avec J.-C. Faugère, P.-A. Fouque et L. Perret |
| J. M. Crypt. | *A Family of Weak Keys in HFE and the Corresponding Practical Key-Recovery*, avec P.-A. Fouque, A. Joux et J. Treger |
| CHES '10 | *Fast Exhaustive Search for Polynomial Systems Over* $\mathbb{F}_2$, avec H.-C. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. Yang |
| SAC '10 | *Security Analysis of SIMD*, avec P.-A. Fouque et G. Leurent |
| SAC '10 | *Attacks on Hash Functions based on Generalized Feistel - Application to Reduced-Round Lesamnta and SHAvite-3*, avec O. Dunkelman, G. Leurent et P.-A. Fouque |
| FSE '10 | *Another Look at the Complementation Property*, avec O. Dunkelman et G. Leurent, P.-A. Fouque |
| SHA-3 candidate | *SIMD is a Message Digest*, avec G. Leurent et P.-A. Fouque |
| SAC '09 | *Herding, Second Preimage and Trojan Message Attacks Beyond MD*, avec E. Andreeva, J. Kelsey et O. Dunkelman |
| SAC '08 | *Analysis of the Collision Resistance of RadioGatún using Algebraic Techniques*, avec P.-A. Fouque |
| Eurocrypt '08 | *Second Preimage Attacks On Iterated Hash Functions*, avec E. Andreeva, P.-A. Fouque, J. Hoch, J. Kelsey, A. Shamir et S. Zimmer |
| VMCAI '07 | *Using First-Order Theorem Provers in the Jahob Data Structure Verification System Verification*, avec V. Kuncak, T. Wies, K. Zee et M. Rinard |

*Université de Lille – 59655 – Villeneuve d'Ascq Cedex*
*+33 618 221 393* • *charles.bouillaguet@univ-lille.fr*
*https://cbouilla.github.io*