Christopher Goyet

Mathématiques / Informatique

✉ *goyet.christopher@gmail.com*
Nationalité française
Permis B, A - véhiculé

Diplômes et Études

2014-2015 **Master2 MEEF**, *Métiers de l'enseignement, de l'éducation et de la formation*, ÉSPÉ de Nice.

2013–2014 **Agrégation de Mathématiques**, *Classement : 131ème.*

2009–2012 **Doctorat**, *Université Paris 6*, Thales/UPMC/LIP6/INRIA.
Sujet: Cryptanalyse algébrique par canaux auxiliaires. Directeur de thèse: Jean-Charles Faugère
Encadrant universitaire: Guénaël Renault - Encadrant industriel: Olivier Orcière

2008–2009 **Master2 Mathématiques**, *Université Nice Sophia-Antipolis*, *Mention Très Bien.*

2007–2008 **Master1 Mathématiques**, *UQÀM*, Montréal, *Bourse d'excellence.*
Programme d'échange inter-universitaire

2006–2007 **Licence Mathématiques**, *Université Nice Sophia-Antipolis*, *Mention Bien.*

2004–2006 **DEUG Mathématiques-Informatique**, *Université Nice Sophia-Antipolis.*

2003–2004 **Prépa BCPST**, *Lycée Thiers*, Marseille.

2003 **Baccalauréat S Spé Maths**, *Lycée Lorgues*, *Mention Bien.*

Expériences professionnelles

2015–2017 **Professeur Agrégé de Mathématiques**, *Lycée Guillaume Apollinaire*, Nice.

2014–2015 **Professeur Agrégé de Mathématiques**, *Collège Antoine Risso*, Nice.

10/2009–10/2012 **Ingénieur cryptologue**, *Thales communications*, Colombes, France.
Laboratoire chiffre, doctorat convention CIFRE (Power Analysis, Algebraic Cryptanalysis, Groebner Attacks)

02/2011–05/2011 **Enseignant vacataire**, *Université Paris Descartes*, Paris 5.
TD numération et logique - niveau L1 (MLI230B)

02/2010–05/2010 **Enseignant vacataire**, *UPMC*, Université de Paris 6.
TP calcul scientifique en C - niveau L2 (LI217)

03/2009–06/2009 **Stage Master 2**, *INRIA Sophia Antipolis/Laboratoire J.A. Dieudonné/Équipe GALAAD.*
Sujet: Ordre total de réductibilité d'un pinceau de courbes algébriques planes.
Directeurs: Bernard Mourain, Laurent Busé

Compétences

Informatique bureautique (Word, Excel, LibreOffice), LaTeX, Internet, connaissances en architecture système et réseau(programmation, sécurité), bases de données, algorithmique, calcul formel, vérification formelle de preuves

Certifications C2i2e

Langages C, Java, Scheme, HTML, Assembleur, Python, MAGMA, Coq

Langue Anglais intermédiaire

Centres d'intérêt

Sports arts martiaux, équitation, canyoning, snowboard, VTT, escalade, poker, échecs

Autres littérature, musique(guitare), cinéma, astronomie, électronique, mécanique, navigation de plaisance

Publications

[1] Claude Carlet, Jean-Charles Faugère, Christopher Goyet, and Guénaël Renault. Analysis of the Algebraic Side Channel Attack. *Journal of Cryptographic Engineering*, pages 1–18, 2012.

[2] Jean-Charles Faugère, Christopher Goyet, and Guénaël Renault. Algebraic Side Channel Analysis. In *COSADE'11: The 2nd International Workshop on Constructive Side-Channel Analysis and Secure Design*, pages 1–6, Fraunhofer SIT, 2011.

[3] Jean-Charles Faugère, Christopher Goyet, and Guénaël Renault. Attacking (EC)DSA Given Only an Implicit Hint. In *Conference on Selected Areas of Cryptography*, Lecture Notes in Computer Science, pages 1–12, Ontario, 2012. Springer Berlin / Heidelberg.

Exposés

04/2012 **Séminaire "Protection de l'information" du LAGA**, An Analysis of Algebraic Side Channel Attacks, Université Paris 8, Saint-Denis, France.

04/2011 **Journées Codage et Cryptographie 2011**, An Analysis of Algebraic Side Channel Attacks, Oléron, France.

02/2011 **Conférence COSADE 2011**, A new criterion for Effective Algebraic Side Channel Attacks, Darmstadt, Allemagne.

12/2010 **Séminaire SALSA**, *LIP6/UPMC/INRIA*, A new criterion for Effective Algebraic Side Channel Attacks, Université Paris 6, France.