Aurélien Greuet

Docteur en mathématiques
Ingénieur R&D cryptographie

56 boulevard de Verdun
92400 Courbevoie
+33.6.24.83.44.50
aureliengreuet@protonmail.com
http://aureliengreuet.free.fr/
Né le 28 octobre 1985 (32 ans)

Expérience

Août 2014– **Ingénieur R&D en cryptographie**, *IDEMIA (ex-Oberthur Technologies)*.

- Développement d'algorithmes cryptographiques embarqués résistants aux attaques physiques pour produits bancaires, mobiles et identités
- Recherche et innovation : crypto post-quantique, homomorphique, side-channel
- Assembleur ARM, 8051, 80251 / C / applet Java Card
- Cours et TP de cryptographie sur carte à puce en Master 2 à l'ISFA Lyon et Paris 6
- Encadrement de stage de fin d'étude : étude crypto post-quantique, implémentation HFEv- sur carte à puce

2013 – 2014 **Professeur agrégé détaché pour exercer les fonctions d'ATER**.
IUT A de Lille 1, département informatique / Laboratoire d'Informatique Fondamentale de Lille

- Recherche en calcul formel et optimisation
- Enseignement en DUT Info 2e année : algèbre, Java, programmation système, BDD

2010 – 2013 **Thèse de mathématiques et applications des mathématiques**.

Sujet Optimisation polynomiale et variétés polaires : théorie, algorithmes et implantations

Directeurs Vincent Cossart, Laboratoire de Mathématiques, Université de Versailles
Mohab Safey El Din, Laboratoire d'Informatique de Paris 6, Inria/LIP6/UPMC.

- Enseignements en mathématiques à l'université de Versailles niveaux L1, L2, L3, M2

2012–2013 **Membre du conseil de l'école doctorale Sciences et Technologie de Versailles**.

Octobre 2012 **Organisation d'un séminaire scientifique inter-disciplinaire**, *Université de Versailles*.

Juin 2012 **Animation d'un stage MathC2+ mathématique/algorithmique**, *Microsoft France*.
Algorithmique et calcul formel, applications à la cryptographie et à la cryptanalyse, 1reS et 1reSTI

2009–2010 **Master 2 Maths-Info Algèbre appliquée à la cryptographie et au calcul formel**, *Université de Versailles Saint-Quentin*.
Mention Bien, rang : 1er, Stage avec Mohab Safey El Din, Inria/LIP6/UPMC

2008–2010 **Colles de mathématiques**, *Lycées Hoche et Janson de Sailly*, Prépa MPSI et ECS2.

2007–2009 **Agrégation de mathématiques option calcul formel**, *Université Paris 6*, Reçu 171e.

2005–2007 **Licence/Maîtrise de mathématiques**, *Université Paris 6*, Mention Bien/Assez Bien.

2003–2005 **Classes préparatoires MPSI et MP**, *Lycée Saint-Louis*, Paris.

Juin 2003 **Baccalauréat S**, *Lycée Jean Racine*, Montdidier (80), Mention Bien.

Publications

2016 **Faster Evaluation of SBoxes via Common Shares**, J.-S. Coron, A. Greuet, E. Prouff, R. Zeitoun, *[CHES 2016]*.

2014 **Probabilistic and Exact Algorithm for the Global Optimization of a Polynomial over a Real Algebraic Set**, A. Greuet, M. Safey El Din *[SIAM Journal on Optimization]*.

2012 **Global optimization of polynomials restricted to a smooth variety using sums of squares**, A. Greuet, F. Guo, M. Safey El Din, L. Zhi *[Journal of Symbolic Computation]*.

2011 **Deciding reachability of the infimum of a multivariate polynomial**, Aurélien Greuet, Mohab Safey El Din. *[ISSAC 2011]*.

Exposés en conférences internationales - séjours invités

- Orateur invité à l'Asian Symposium on Computer Mathematics, Chinese Academy of Sciences, Pékin, Chine, Octobre 2012
- Jeune chercheur invité au Fields Institute Workshop on Hybrid Methodologies for Symbolic-Numeric Computation, Université de Waterloo, Canada, Novembre 2011
- International Symposium on Symbolic and Algebraic Computation (ISSAC), San Jose, Californie, Juin 2011
- Séjour invité de deux semaines au Mathematics Mechanization Research Center, Chinese Academy of Sciences, Pékin, Chine, Décembre 2010

Exposés en séminaires

- Séminaire de géométrie algorithmique, *Loria, Nancy,* mars 2014
- Séminaire de calcul formel et complexité, *université de Rennes 1,* mars 2014
- Séminaire de géométrie, *université de Savoie,* décembre 2013
- Seminaire d'algèbre et géométrie réelle. *Konstanz, Allemagne,* juillet 2013
- Journée des doctorants, *université de Versailles,* octobre 2012
- Séminaire de calcul formel, *université de Limoges,* octobre 2011
- Séminaire d'algèbre et géométrie, *université de Versailles,* avril 2011
- Séminaire SALSA, *université de Paris 6,* février 2011
- Séminaire ALGO, *Inria Paris-Rocquencourt,* janvier 2011

Informatique

OS	Linux, Mac OS X	Programmation	Assembleur ARM, 8051 et 80251, C, Applets Java Card
Sciences	Maple, Sage	Typographie	LaTeX

Langues

Français	Langue maternelle	Anglais	Lu, parlé, écrit

Divers

Loisirs	Arts martiaux, course à pied