Yann Rotella

Cryptographe

+33 6 16 41 00 19
yann@rotella.fr
https://www.rotella.fr
né le 19 août 1992, nationalité française

Curriculum Vitae

Parcours

2018 – Aujourd'hui — **PostDoc**, *Université de Radboud*, Nimègue, Pays-Bas, Digital Security Department.
Encadrant: Joan Daemen.

2015 – 2018 — **Doctorat en Informatique**, *Laboratoire INRIA de Paris, Sorbonne Université, EDITE de Paris - ED130, 19 septembre 2018*, SECRET,
Directrice : Anne Canteaut.
Rapporteurs: Joan Daemen et Henri Gilbert.
Jury: Pierre-Alain Fouque, Sihem Mesnager, María Naya-Plasencia, Sondre Rønjom, Antoine Joux.
Mathématiques discrètes appliquées à la cryptographie symétrique.

2014 – 2015 — **M2 Recherche Master Parisien de Recherche en Informatique (MPRI)**, *Université Paris Diderot*, Paris, *Cryptographie, Algorithmique et Combinatoire.*
Mémoire: les représentations équivalentes d'un LFSR et leur impact en cryptanalyse, sous la direction d'Anne Canteaut.
mention Bien.

2012 – 2015 — **Diplôme d'ingénieur à Télécom ParisTech**, *2015*,
Parcours *Cryptographie et Théorie de l'Information* et *Mathématiques, Informatique Théorique et Recherche Opérationnelle*.

2010 – 2012 — **Classe préparatoire MPSI - MP***, *Lycée Saint Louis*, Paris.

juin 2010 — **Baccalauréat Scientifique, mention Très Bien**, *Lycée Théophile Gautier*, Tarbes.

Prix

2018 — **Prix de la meilleure thèse de l'EDITE de Paris 2018**.

Publications dans des conférences et journaux internationaux avec comité de lecture

novembre 2018 — **Cryptanalysis of MORUS**, *Tomer Ashur, Maria Eichlseder, Martin M. Lauridsen, Gaëtan Leurent, Brice Minaud, Yann Rotella, Yu Sasaki et Benoit Viguier*, ASIACRYPT 2018, pages 35-64.
Springer.

novembre 2018 — **On the concrete security of Goldreich's pseudorandom generator**, *Geoffroy Couteau, Aurélien Dupin, Pierrick Méaux, Mélissa Rossi et Yann Rotella*, ASIACRYPT 2018, pages 96-124.
Springer.

mars 2018 — **State-recovery attacks on modified Ketje Jr**, *Thomas Fuhr, María Naya-Plasencia et Yann Rotella*, IACR Transactions on Symmetric Cryptology 2018(1), pages 29-56.

septembre 2017 **Boolean functions with restricted input and their robustness; application to the FLIP cipher**, *Claude Carlet, Pierrick Méaux et Yann Rotella*, IACR Transactions on Symmetric Cryptology 2017(3), pages 192-227.

août 2017 **Proving resistance against invariant attacks: How to choose the round constants**, *Christof Beierle, Anne Canteaut, Gregor Leander et Yann Rotella*, CRYPTO 2017, pages 647-678.
Springer, Heidelberg.

août 2016 **Cryptanalysis of the FLIP family of stream ciphers**, *Sébastien Duval, Virginie Lallemand et Yann Rotella*, CRYPTO 2016, pages 457-475.
Springer, Heidelberg.

mars 2016 **Attacks against filter generators exploiting monomial mappings**, *Anne Canteaut et Yann Rotella*, Fast Software Encryption 2016, pages 78-98.
Springer, Heidelberg.

Enseignement

2017 – 2018 **Initiation à l'algorithmique**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TD, 40h.
Complexité, Logique, Tris, Arbres.

2016 – 2017 **Algorithmes et Structures de Données**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TP, 17.5h.
Listes, Tableaux, Hachage, Arbres, Allocation dynamique en C.

2016 – 2017 **Machines et Représentations**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TP, 20h.
Architecture des machines, Représentation des informations et des programmes, Execution simple.

2016 – 2017 **Structures Discrètes**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TP, 21h.
Logique propositionnelle, Induction, Ensembles, Automates finis.

2016 – 2017 **Représentations et Méthodes numériques**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TD, 40h.
Nombres entiers et flottants, Représentations et algorithmes associés, Résolution de systèmes linéaires.

2015 – 2016 **Représentations et Méthodes numériques**, *L2, 30 élèves, Sorbonne Université*, Monitorat, TP, 20h.
Nombres entiers et flottants, Représentations et algorithmes associés, Résolution de systèmes linéaires.

2015 – 2016 **Ateliers de Recherche Encadrés**, *L1, 30 élèves, Sorbonne Université*, Monitorat, projet, 40h.
Projet de recherche en python, Simulations et Premiers programmes.

Administration

2016 – 2018 **AGOS Paris**, *Elu à l'Association pour la Gestion des Oeuvres Sociales de l'Inria de Paris*, Organisation d'événements pour le personnel du centre, 30h par an.

Médiation Scientifique

décembre 2017 **Intervention Alkindi, concours de cryptographie**, *lycée de la Vallée de Chevreuse.*

octobre 2017 **Intervention "Raconte moi ta thèse"**, *Institut Henri Poincaré, Paris.*

mai 2017 **Présentation Cryptographie équipe SECRET pour les 50 ans de l'Inria**, *Le 104, Paris.*

février 2017 **Intervention et TDs en prépa sur la cryptographie**, *Lycée Théophile Gautier, Tarbes.*

mai 2016 **Participation à Futur en Seine, présentation de la cryptographie**, *Paris.*

avril 2016 **Interventions scientifiques dans des écoles primaires**, *Paris.*

Autres

2015 – 2019 **Sous-relecteur pour les comités de programmes suivants:** , *DCC (Design Codes and Cryptography), CRYPTO 2018, ASIACRYPT 2018, ISIT, EUROCRYPT 2019.*

Présentations et Séminaires

janvier 2019 **On the concrete security of Goldreich's Pseudorandom Generator**, *Séminaire équipe CARAMBA*, Inria de Nancy.

janvier 2019 **Choosing Round Constants in Lightweight Block Ciphers**, *Séminaire Université de Versailles Saint Quentin en Yvelines*, Versailles.

septembre 2018 **Mathématiques discrètes appliquées à la cryptographie symétrique**, *Soutenance de thèse*, Jussieu, Paris.

juin 2018 **Attaques algébriques revisitées**, *Séminaire Codage, Cryptographie et Algorithmes*, Paris.

mars 2018 **Boolean functions with restricted input and their robustness; application to the FLIP cipher**, *Fast Software Encryption 2018*, Bruges.

janvier 2018 **New directions in attacks against stream ciphers**, *Séminaire à l'Ecole polytechnique de Lausanne (EPFL)*, Lausanne.

octobre 2017 **Attacks against Filter Generators Exploiting Monomial Mappings (version améliorée)**, *Séminaire GT Bac*, Télécom ParisTech, Paris.

avril 2017 **Attaques par invariant: comment s'en protéger?**, *Journées Codage et Cryptographie*, La Bresse.

mai 2016 **Des nouvelles attaques sur les registres filtrés exploitant la structure des corps finis**, *Séminaire Université de Versailles Saint Quentin en Yvelines*, Versailles.

mars 2016 **Cryptanalyse du chiffrement à flot FLIP**, *Séminaire ANR BLOC*, Inria de Paris.

mars 2016 **Attacks against Filter Generators Exploiting Monomial Mappings**, *Fast Software Encryption 2016*, Bochum.

octobre 2015 **Attaques exploitant les représentations équivalentes des LFSR filtrés**, *Journées Codage et Cryptographie*, La londe les Maures.

Langues

Français **Natif**.

Anglais **Courant**, *(CECR C1).*

Allemand **Courant**, *(CECR B2+).*

Compétences

Programmation **C/C++, Java, Python, Caml, Matlab**.

Environnements **Linux (Ubuntu), Windows, MAC OS**.

Outils **Emacs, GCC, Eclipse**.

Bureautique **Suite Microsoft Office, LaTeX**.

Expériences antérieures

mars – septembre 2015 — **Stage de recherche en cryptographie**, *INRIA Paris Rocquencourt*, SECRET, Directrice : Anne Canteaut..
Stage en cryptographie symétrique, sur les chiffrements à flots, plus particulièrement les registres filtrés, leurs représentations équivalentes et l'impact en cryptanalyse.

février – mai 2014 — **Projet Holographie Numérique 3D**.
Projet sous la tutelle de Renaud Gabet. Utilisation d'une matrice à cristaux liquide (SLM), génération d'hologrammes numériques et optimisation des algorithmes sous Matlab.

juin 2013 — **Stage humanitaire au Sénégal**, *avec l'Association FIDEI; un mois de formation d'élèves et d'enseignnants aux bases de l'informatique.*

2012 – 2013 — **Le "Google Bike"**, *Projet scolaire de 6 mois en groupe.*
Développé en Java, impliquant du traitement de la vidéo (interpolation d'images), gestion de lunettes à réalité augmentée.

Divers

Vie associative — **Responsable de la cafétéria de Télécom ParisTech**, *Gestion d'une équipe de 15 personnes.*

Président de Télécom LudoTech, *Organisation d'évênements ludiques (Jeux de plateau et jeux de rôles).*

1999 – 2010 — **Conservatoire**, *Etudes musicales (Violoncelle, solfège et chant).*

2004 – 2010 — **Théâtre**.

Loisirs

Sports — **Badminton, Tennis, Escalade, Ski, Snowboard, Randonnée (haute montagne), Alpinisme**.

Goûts — **Biérologie, Fromages, Jeux de société, Cinéma**.