Yann Rotella

Cryptographer

+33 6 16 41 00 19
yann@rotella.fr
https://www.rotella.fr
Born on August 19, 1992, french

Curriculum Vitae

Professionnal career

2018 – Today **PostDoc**, *Radboud University*, Nijmegen, The Netherlands, Digital Security Department.
Supervisor: Joan Daemen.

2015 – 2018 **PhD in Computer Science**, *INRIA de Paris Laboratory, Sorbonne University, EDITE de Paris - ED130, September 19, 2018*, SECRET,
Supervisor: Anne Canteaut.
Thesis reporters: Joan Daemen and Henri Gilbert.
Jury: Pierre-Alain Fouque, Sihem Mesnager, María Naya-Plasencia, Sondre Rønjom and Antoine Joux.
Discrete Mathematics applied to Symmetric Cryptography.

2014 – 2015 **Master Research: Master Parisian for Research in Computer Science (MPRI)**, *Paris Diderot University*, Paris, *Cryptography, algorithmics and Combinatorics.*
Thesis: Equivalent representations of an LFSR and their impact in cryptanalysis, supervised by Anne Canteaut.
High Honors

2012 – 2015 **Ingineer Diploma at Telecom ParisTech**, *2015*,
Courses *Cryptography and Information theory* and *Mathematics, Theoretical Computer Science and Operational Research.*

2010 – 2012 **Preparatory Class for entrance to Grandes Ecoles MPSI - MP***, *Lycée Saint Louis*, Paris.

June 2010 **High School Diploma**, *Lycée Théophile Gautier*, Tarbes.
Very High Honors

Prizes

2018 **Prize for the best thesis of the doctoring school EDITE de Paris 2018**.

Publications in international peer reviewed journals and conferences

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

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

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

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

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

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

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

Teaching

2017 – 2018 **Initiation to Algorithms**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Tutorials, 40h.
Complexity, Logic, Sorts, Trees.

2016 – 2017 **Algorithms and Data Structures**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Practical Work, 17.5h.
Lists, Tables, Hash, Trees, Dynamic allocation in C.

2016 – 2017 **Machines and Representations**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Practical Work, 20h.
Machine architecture, Representation of Information and Programs, Simple execution.

2016 – 2017 **Discrete Structures**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Practical Work, 21h.
Propositional Logic, Induction, Sets, Finite Automaton.

2016 – 2017 **Representations and Numerical Method**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Tutorials, 40h.
Integer and Floats, Representations and associated Algorithms, Resolution of linear systems.

2015 – 2016 **Representations and Numerical Method**, *Second year of Bachelor, 30 students, Sorbonne University*, Monitorat, Practical Work, 40h.
Integer and Floats, Representations and associated Algorithms, Resolution of linear systems.

2015 – 2016 **Research Project in Dynamic Systems**, *First year of Bachelor, 30 students, Sorbonne University*, Monitorat, Project, 40h.
Research Project in Python, Simulations and first Programms.

Administration

2016 – 2018 **AGOS Paris**, *Elected at "Association pour la Gestion des Oeuvres Sociales" of Inria de Paris*, Organization of events for Inria's staff, 30h per year.

Scientific Intervention

December 2017 **Intervention for Alkindi, Cryptography Contest**, *lycée de la Vallée de Chevreuse.*

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

May 2017 **Presentation of Cryptography (team SECRET) for 50th birthday of Inria**, *Le 104, Paris.*

February 2017 **Intervention and Tutorials in preparatory class on Cryptography**, *Lycée Théophile Gautier, Tarbes.*

May 2016 **Participation to "Futur en Seine", Presentation of Cryptography**, *Paris.*

April 2016 **Scientific interventions in primary schools**, *Paris.*

Others

2015 – 2019 **Sub-reviewer for the following program committee**, *DCC (Design Codes and Cryptography), CRYPTO 2018, ASIACRYPT 2018, ISIT, EUROCRYPT 2019.*

Presentations and Seminars

January 2019 **On the concrete security of Goldreich's Pseudorandom Generator**, *Seminair team CARAMBA*, Inria de Nancy.

January 2019 **Choosing Round Constants in Lightweight Block Ciphers**, *Seminar University of Versailles Saint Quentin en Yvelines, PRISM Laboratory*, Versailles.

September 2018 **Discrete Mathematics applied to Symmetric Cryptography**, *PhD Defense*, Jussieu, Paris.

June 2018 **Algebraic Attacks Revisited**, *Seminar Coding, Cryptography and Algorithms*, Paris.

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

January 2018 **New directions in attacks against stream ciphers**, *Seminar at Ecole polytechnique de Lausanne (EPFL)*, Lausanne.

October 2017 **Attacks against Filter Generators Exploiting Monomial Mappings (extended)**, *Seminar GT Bac*, Telecom ParisTech, Paris.

April 2017 **Innvariant attacks: How to protect?**, *Coding and Cryptography days*, La Bresse.

May 2016 **News attacks on Filtered Register exploiting Finite Fields Structure**, *Seminar University of Versailles Saint Quentin en Yvelines, PRISM Laboratory*, Versailles.

March 2016 **Cryptanalysis of the stream cipher FLIP**, *ANR BLOC Seminar*, Inria de Paris.

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

October 2015 **Attacks exploiting equivalent representations of Filtered LFSR**, *Coding and Cryptography days*, La londe les Maures.

Languages

French **Native**.

English **Fluent**, *(CECR C1)*.

German **Fluent**, *(CECR B2+)*.

Computer Skills

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

Environments **Linux (Ubuntu), Windows, Mac OS**.

Tools **Emacs, GCC, Eclipse**.

Others **Microsoft Office, LaTeX**.

Previous experience

March – September 2015 — **Research Internship in Cryptography**, *INRIA Paris Rocquencourt*, SECRET, Supervisor: Anne Canteaut..
Internship in Symmetric Cryptography on Stream Ciphers, on filtered registers and their equivalent representations and their impact on Cryptanalysis.

February – May 2014 — **Numerical 3D Holographic Project**.
Project directed by Renaud Gabet. Using Liquid Crystal Matrix (SLM) in order to generate Digital Holograms and Optimizing Matlab Algorithms.

June 2013 — **Humanitarian internship (Sénégal)**, *FIDEI association:one month of Computer Science courses.*

2012 – 2013 — **"Google Bike"**, *6 months project.*
Coded in Java, involving image interpolation and augmented reality glasses.

Various

Associative life — **Telecom ParisTech cafeteria manager**, *Management of a team of 15 people.*

Telecom LudoTech president, *Organization of events (Board games and role plays).*

1999 – 2010 — **Conservatory**, *Music School (Cello, music theory and vocal).*

2004 – 2010 — **Theater**.

Hobbies

Sports — **Badminton, Tennis, Climbing, Ski, Snowboard, Hiking (High mountain), Mountaineering**.

likes — **Beerology, Cheese, Board Games, Cinema**.