# Gaëtan Leurent

*Cryptographer*

*Centre de recherche Inria de Paris — EPI Secret*
*2 rue Simone Iff*
*F-75012 Paris*
☎ *+33.1.80.49.42.24*
✉ *gaetan.leurent@inria.fr*
*https://who.rocq.inria.fr/Gaetan.Leurent*


## Research Topics

**Symmetric cryptography**: hash functions, block ciphers, stream ciphers, modes. Cryptanalysis, design, and implementation.

## Positions

2013– **Researcher**, *Inria*, Paris-Rocquencourt, France.
Starting Research Position (2013–2018), Chargé de Recherche (since 2018)

2012–2013 **Postdoctoral researcher**, *University Catholique de Louvain-la-Neuve*, Belgique.
Grant on the ERC project CRASH

2010–2012 **Postdoctoral researcher**, *University of Luxembourg*, Luxembourg.
AFR grant from the Fonds National de la Recherche (Co-funded by Marie Curie Actions)

2007–2010 **Ph.D. student**, *ENS*, Paris.
Grant from Direction Générale de l'Armement

## Education

2006–2010 **Ph.D. in Computer Science**, *École Normale Supérieure (ENS)*, Paris.
Title: *Design and Analysis of Hash Functions*
Supervision: David Pointcheval *(Supervisor)* and Pierre-Alain Fouque *(Scientific Advisor)*

2004–2006 **Master's Degree in Computer Science**, *ENS*, Paris.
Dissertation: *Study and automation of Wang's attack against MD4*.

## Publication record

Publications **40+ conference publications**, 50+ co-authors
(6 Crypto, 4 Eurocrypt, 5 Asiacrypt, 12 FSE, 2 CHES, 1 CCS, 1 NDSS, 4 CT-RSA, 8 SAC)

H-index 21 (1300+ citations), *according to Google Scholar*

## Services to the Community

Program Committee **CHES 2019**, **FSE 2019**, **Asiacrypt 2018**, **FSE 2018**, SAC 2018, SCN 2018, SAC 2017, **Crypto 2017**, **FSE 2017**, Financial Crypto 2017, Indocrypt 2016, **FSE 2016**, SAC 2016, ACISP 2016, Indocrypt 2015, **FSE 2015**, SCN 2014, **Eurocrypt 2013**, SAC 2013, CANS 2013, Africacrypt 2013, SAC 2012, CANS 2011

Organizing Committee **Euro S&P 2017**, 300 attendees (posters chair)
**WCC 2015**, 150 attendees (co-organizer)

Other **IACR Transactions** LaTeX template

Local committees Member of the CUMI-R (Comité d'utilisation des moyens informatiques recherche)
Member of the CSD (Comité de suivi doctoral)

## Students supervision

**Ferdinand Sibleyras** — **Master** (2017), **Ph.D.** (2017–2020)
Ph.D. funded with a DGA-Inria grant.

**Sébastien Duval** — **Master** (2014), **Ph.D.** (2015–2018). Co-supervision with Anne Canteaut.
Ph.D. funded with a grant from the doctoral school.
Third prize of the doctoral school EDITE (750 students).

## Training Schools

February 2018 — **COST Training School on Symmetric Cryptography and Blockchain**, *Torremolinos*, Spain.
How Not to Use a Blockcipher

## Popularization

Popular science mag. — **La fagilité inattendue du chiffrement symétrique**, *La Recherche*, November 2018.
G. Leurent & M. Naya-Plasencia

Radio show — **Mot de passe partout**, *Service public (France Inter)*, April 2015.

## Vulnerabilities reported

CVE-2016-2183/6329 — **Sweet32 attack**, K. Bhargavan & G. Leurent.

CVE-2015-7575 — **SLOTH attack**, K. Bhargavan & G. Leurent.

CVE-2007-1558 — **Collision attack against APOP**, G. Leurent.

## Collaborations

2017–2019 — **PI of Associate Team CHOCOLAT** with Thomas Peyrin, *NTU*, Singapore.

January 2016 — **Visit to the team of Gregor Leander**, *RU Bochum*, Germany, 1 week.

June 2014 — **Visit to the team of Thomas Peyrin**, *NTU*, Singapore, 4 weeks.

2005 — **Master's internship with Carlos Cid**, *Royal Holloway*, U.K., 5 months.

## Software Developments

ARXtools — Toolkit for analysis of ARX constructions, and construction of differential characteristics.

Hash functions — Implementation of SIMD, Blake, and SCREAM with vector instructions on x86, PowerPC and ARM. Integrated in eBASH.

## Awards

January 2016 — **Distinguished paper award**, *NDSS 2016*.
*Transcript Collision Attacks: Breaking Authentication in TLS, IKE and SSH*
K. Bhargavan & G. Leurent

March 2015 — **1st place in the Streebog Competition**, *Organized by the Russian Technical Committee for Standardization (500 000 Rubles prize)*.
*The Usage of Counter Revisited: Second-Preimage Attack on New Russian Standardized Hash Function*
J. Guo, J. Jean, G. Leurent, T. Peyrin & L. Wang

March 2015 — **2nd place in the Underhanded Crypto Contest**.
*Backdoored Implementation of Stern's Zero-Knowledge Identification Protocol*
G. Leurent

## Keynote Talks

TCCM-CACR 2016 — **Workshop of the Technical Committee on Cryptologic Mathematics, Chinese Association for Cryptologic Research**, *Yinchuan*, China, August 2016.
Breaking Symmetric Cryptosystems Using Quantum Period Finding

SAC 2015 — **22nd Conference on Selected Areas in Cryptography (SAC)**, *Sackville*, Canada, August 2015.
Generic Attacks against MAC Algorithms

TCCM-CACR 2013 — **Workshop of the Technical Committee on Cryptologic Mathematics, Chinese Association for Cryptologic Research**, *Tianjin*, China, August 2013.
New Generic attacks on Hash-based MACs

## Workshops and Seminars

LWD 2018 — **Lightweight Crypto Day 2018**, *Tel Aviv*, Israel, April 2018.
Security Issues with Small Block Sizes

University of Oxford — **Mathematical Institute Cryptography Seminar**, *Oxford*, United Kingdom, May 2016.
Breaking Symmetric Cryptosystems using Quantum Period Finding

Tsinghua University — **Institute for Advanced Study Cryptology Seminar**, *Beijing*, China, August 2013.
New Generic attacks on Hash-based MACs

SKLOIS — **SKLOIS seminar (State Key Laboratory of Information Security)**, *Beijing*, China, December 2012.
Differential Attacks against ARX Designs

## Design of Cryptographic Schemes

CAESAR candidate — **SCREAM**, *Authenticated Encryption*.
V. Grosso, G. Leurent, F.-X. Standaert, K. Varici, F. Durvaux, L. Gaspar & S. Kerckhof

FSE 2014 — **LS-designs : Bitslice encryption for efficient masked software implementations**, *Light-weight block ciphers Robin and Fantomas*.
V. Grosso, G. Leurent, F.-X. Standaert & K. Varıcı

FSE 2014 — **SPRING : Fast Pseudorandom Functions from Rounded Ring Products**, *Lattice-based PRF*.
A. Banerjee, H. Brenner, G. Leurent, C. Peikert & A. Rosen

SHA-3 candidate — **SIMD is a Message Digest**, *Hash function*.
G. Leurent, C. Bouillaguet & P.-A. Fouque

## Selected Publications

Eurocrypt 2018 — **The Missing Difference Problem, and its Applications to Counter Mode Encryption**.
G. Leurent, F. Sibleyras

ACM CSS 2016 — **On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN**, *CVE-2016-2183, CVE-2016-6329*.
K. Bhargavan & G. Leurent

Crypto 2016 — **Breaking Symmetric Cryptosystems Using Quantum Period Finding**.
M. Kaplan, G. Leurent, A. Leverrier & M. Naya-Plasencia

Asiacrypt 2013 — **New Generic Attacks against Hash-based MACs**.
G. Leurent, T. Peyrin & L. Wang

FSE 2008 — **MD4 is Not One-Way**.
G. Leurent