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

Positions

2013– **Researcher**, *Inria*, Paris-Rocquencourt, France.
Starting Research Position

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

2003–2007 **École Normale Supérieure student**, *ENS*, Paris.
Civil servant in training, very competitive entrance exam

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)*

2007 **Agrégation de mathématiques**, *Ranked 70th*.
Civil service competitive examination for high school teacher positions.

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

Research Visits

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

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

Services to the Community

Program Committee **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)

Research Topics

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

Supervision

2017 **Supervision of a MPRI intern (Master 2)**.
Ferdinand Sibleras. Topic: *Cryptanalysis of Modes of Operations*

2015–2018 **Co-supervision of a Ph.D. student**.
Sébastien Duval. Topic: *Constructions for lightweight cryptography*.

2013 **Served in a PhD committee**.
Patrick Derbez. Title: *Meet-in-the-Middle Attacks against AES*

Selected Conference publications

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

Eurocrypt 2015 **The Sum can be Weaker than Each Part**.
G. Leurent & L. Wang

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

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

Journal Publications

Algorithmica **Improved Generic Attacks Against Hash-based MACs and HAIFA**, *Algorithmica*, 2016.
I. Dinur & G. Leurent

IJACT **Practical key-recovery attack against APOP, an MD5 based challenge-response authentication**, *International Journal of Applied Cryptography*, 2008.
G. Leurent

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

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.

Software Developments

ARXTools: `https://who.rocq.inria.fr/Gaetan.Leurent/arxtools.html`
Analysis of differential characteristics for ARX designs.
Construction of characteristics for Skein.
Open source. Graphical interface.

Implementations of SIMD, Blake, and SCREAM
Optimized with vector instructions for x86, ARM, and PowerPC architectures.
Open Source, available as part of eBASH. Fastest Blake on ARM NEON.

Implementation of most attacks described in my research publications
Partial implementation for theoretical attacks.
Use of clusters and GPU for large computations.

Invited Conference 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

Seminars

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 Generalized attacks on Hash-based MACs

CCA — **CCA seminar (Coding, Cryptology, Algorithms)**, *Paris*, June 2013.
Differential Attacks against ARX Designs

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

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