Gaëtan Leurent

Cryptographer

Centre de recherche Inria de Paris — EPI Cosmiq
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*.

Services to the Community

Co Editor-in-Chief **IACR Transactions on Symmetric Cryptology** (2020, 2021)

Program Committee **Eurocrypt** (2013, 2021, 2022); **Crypto** (2017); **Asiacrypt** (2018); **FSE/ToSC** (2015, 2016, 2017, 2018, 2019, 2022); **CHES/TCHES** (2019); **SAC** (2012, 2013, 2016, 2017, 2018); **Financial Crypto** (2017); **SCN** (2014, 2018); **Indocrypt** (2015, 2016, 2021); **Africacrypt** (2013); **CANS** (2011, 2013); **ACISP** (2016)

Organizing Committee **JC2 2021**, 130 attendees (co-organizer)
Euro S&P 2017, 300 attendees (posters chair)
WCC 2015, 150 attendees (co-organizer)

Other **IACR Transactions** LaTeX template

Students supervision

Augustin Bariant **Master** (2019), **Ph.D.** (2021-2024)

Clara Pernot **Master** (2020), **Ph.D.** (2020-2023)

Ferdinand Sibleyras **Master** (2017), **Ph.D.** (2017–2020)

Sébastien Duval **Master** (2014), **Ph.D.** (2015–2018). Co-supervision with Anne Canteaut.

Research Schools

July 2022 — **Cyber in Nancy**, *Nancy*, France.
(Symmetric) Cryptanalysis in Practice

April 2022 — **IACR-CROSSING School on Combinatorial Techniques in Cryptography**, *Valetta*, Malta.
Generic Attacks against MAC Algorithms and Hash Functions

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

Popularization

Outreach — **Le traçage anonyme, dangereux oxymore**, `https://www.risques-tracage.fr/`, April 2020.
X. Bonnetain, A. Canteaut, V. Cortier, P. Gaudry, L. Hirschi, S. Kremer, S. Lacour, M. Lequesne, G. Leurent, L. Perrin, A. Schrottenloher, E. Thomé, S. Vaudenay & C. Vuillot

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

CVD-2020-0041 — **Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2**, C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht & L. Stennes.

CVE-2019-14855 — **Shambles attack**, G. Leurent & T.Peyrin.

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.

Collaborative projects

2021–2024 — **French PI of ANR-PRCI SELECT** with Thomas Peyrin, *NTU*, Singapore, ≈500k€.

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

Awards

Eurocrypt 2021 — **Best paper award**.
New Representations of the AES Key Schedule
G. Leurent and C. Pernot

Asiacrypt 2020 — **Best paper award**.
New Results on Gimli: Full-Permutation Distinguishers and Improved Collisions
A. Flórez-Gutiérrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher, & F. Sibleyras

NDSS 2016 — **Distinguished paper award**.
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

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

Design of Cryptographic Schemes

NIST lightweight — **Saturnin**, *Block cipher-based Authenticated Encryption*.
A. Canteaut, S. Duval, G. Leurent, M. Naya-Plasencia, L. Perrin, T. Pornin & A. Schrottenloher

NIST lightweight — **Spook**, *Sponge-based Authenticated Encryption*.
D. Bellizia, F. Berti, O. Bronchain, G. Cassiers, S. Duval, C. Guo, G. Leander, G. Leurent, I. Levi, C. Momin, O. Pereira, T. Peters, F-X.. Standaert & F. Wiemer

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 2021 — **New Representations of the AES Key Schedule**.
G. Leurent and C. Pernot
`https://eprint.iacr.org/2020/1253`

USENIX 2020 — **SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust**.
G. Leurent and T. Peyrin
`https://www.usenix.org/system/files/sec20-leurent.pdf`

Eurocrypt 2018 — **The Missing Difference Problem, and its Applications to Counter Mode Encryption**.
G. Leurent, F. Sibleyras
`https://link.springer.com/chapter/10.1007/978-3-319-78375-8_24`

ACM CSS 2016 — **On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN**.
K. Bhargavan & G. Leurent
`https://dl.acm.org/doi/pdf/10.1145/2976749.2978423`

Crypto 2016 — **Breaking Symmetric Cryptosystems Using Quantum Period Finding**.
M. Kaplan, G. Leurent, A. Leverrier & M. Naya-Plasencia
`https://link.springer.com/chapter/10.1007/978-3-662-53008-5_8`