

# Gaëtan Leurent

---

## Education

- 2006–2010 **Ph.D. in Computer Science**, *École Normale Supérieure (ENS)*, Paris.  
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*.  
2003–2004 **Bachelor's Degree in Computer Science**, *ENS*, Paris.  
2001–2003 **Mathematics Prep. Course**, *Lycée privé Sainte Geneviève*, Versailles.  
MPSI and MP\*. Intensive higher education prep.  
Admitted in the ENS with rank 15 (very selective entrance examination).

---

## Positions

- 2010 **Postdoctoral researcher**, *University of Luxembourg*, Luxembourg.  
AFR grant from the FNR  
2007–2010 **Ph.D. student**, *ENS*, Paris, (DGA grant).  
2003–2007 **ENS student**, *ENS*, Paris.

---

## Ph.D. Thesis

- Title* **Design and Analysis of Hash Functions**  
*Supervision* David Pointcheval (*Supervisor*) and Pierre-Alain Fouque (*Scientific Advisor*)  
*Reviewers* Anne Canteaut et Bart Preneel  
*Jury* Antoine Joux (*President*), Alex Biryukov, Orr Dunkelman Arnaud Durand  
*Description* Hash functions are essential primitives in modern cryptography, used in many protocols and standards. My work has been organized around the SHA-3 competition, launched by NIST to select a new hash function standard. In the first part, I studied the new attacks of Wang *et al.* against MD4 and MD5. I describe some improvements of these attacks, and new applications to higher-level constructions. In the second part, I describe a new hash function, SIMD, which has been submitted to NIST for the SHA-3 competition. The design of SIMD follows ideas from the MD4 family, but I used my knowledge of this family to make it resistant to most attacks. Finally, in the third part, I describe new attacks against SHA-3 candidates. I give new attacks techniques which are general enough to apply to several hash functions or block ciphers. Thus, this thesis covers the two main realms of symmetric cryptography: design and analysis.

---

## Research Topics

- Symmetric cryptography: hash functions, bloc ciphers, stream ciphers
- Cryptanalysis, design, implementation

---

## Research Publications

- Eurocrypt 2012 *Narrow Bicliques: Cryptanalysis of Full IDEA*, with D. Khovratovich and C. Rechberger
- CT-RSA 2012 *Boomerang Attacks on Hash Function using Auxiliary Differentials*, with A. Roy
- SAC 2011 *New Insights on Impossible Differential Cryptanalysis*, with C. Bouillaguet, O. Dunkelman and P.-A. Fouque
- FSE 2011 *Practical Near-Collisions on the Compression Function of BMW*, with S. Thomsen
- Africacrypt 2010 *Cryptanalysis of the 10-Round Hash and Full Compression Function of SHAvite-3<sub>512</sub>*, with P. Gauravaram, F. Mendel, M. Naya, T. Peyrin, C. Rechberger and M. Schl affer
- SAC 2010 *Security Analysis of SIMD*, with C. Bouillaguet and P.-A. Fouque
- SAC 2010 *Attacks on Hash Functions based on Generalized Feistel - Application to Reduced-Round Lesamnta and SHAvite-3*, with C. Bouillaguet, O. Dunkelman and P.-A. Fouque
- CT-RSA 2010 *Practical Key Recovery Attack against Secret-prefix EDON-R*
- FSE 2010 *Another Look at the Complementation Property*, with C. Bouillaguet, O. Dunkelman and P.-A. Fouque
- FSE 2010 *Cryptanalysis of ESSENCE*, with M. Naya-Plasencia, A. R ock, J.-P. Aumasson, W. Meier, T. Peyrin
- SHA-3 candidate *SIMD is a Message Digest*, with C. Bouillaguet and P.-A. Fouque
- CHES 2009 *Practical Electromagnetic Template Attack on HMAC*, with P.-A. Fouque, D. Real, and F. Valette
- Crypto 2009 *How Risky is the Random-Oracle Model?*, with P. Nguyen
- CT-RSA 2008 *Cryptanalysis of a Hash Function Based on Quasi-cyclic Codes*, with P.-A. Fouque
- FSE 2008 *MD4 is Not One-Way*
- Crypto 2007 *Full Key-Recovery Attacks on HMAC/NMAC-MD4 and NMAC-MD5*, with P.-A. Fouque and P. Nguyen
- FSE 2007 *Message Freedom in MD4 and MD5 Collisions: Application to APOP*
- Asiacrypt 2005 *An Analysis of the XSL Algorithm*, with C. Cid

---

## Research Internships

- F b-Jul 2006 **Master 2 Internship**, ENS.  
Supervision: Pierre-Alain Fouque and Phong Nguyen  
*Study and automation of Wang's attack against MD4*
- Mar-Jul 2005 **Master 1 Internship**, Royal Holloway University of London.  
Supervision: Carlos Cid  
*Algebraic attacks and analysis of the XSL algorithm.*
- Jun-Jul 2004 **Bachelor Internship**, ENS Lyon.  
Supervision: Arnaud Tisserand  
*FPGA implementation of multipliers over  $\mathbb{F}_{2^n}$  and comparison of different designs*

---

## Computer Skills

- Programming C, OCaml, Perl, and some assembly, C++, and Java  
Implementation of the SIMD hash function with vector instructions on x86, PowerPC and ARM.
- System Good knowledge of Linux and Unix-like Operating Systems.
- Misc. LaTeX, HTML, Shell.