

Gaëtan Leurent

Ph.D. Student in cryptography

ENS - DI
45, rue d'Ulm
75005 Paris – France

☎ +33.1.44.32.20.47

✉ Gaetan.Leurent@ens.fr

French, age 25

<http://www.di.ens.fr/~leurent>



Education

- Since 2006 **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*.
Courses: ▷ Cryptology ▷ Algorithms for combinatory optimization ▷ Algorithms analysis ▷ Algorithmic aspects of combinatory ▷ FPGA implementation ▷ Motion planning ▷ Computer algebra algorithms ▷ Programming languages ▷ Linear logic ▷ Correcting codes and computer algebra: application to cryptology ▷ Quantum calculus.
- 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).

Experience

- 2008 **Teaching assistant**, *École Polytechnique*, Paris.
Practical work in *Programming* course.
- 2008 **Teaching assistant**, *ENS*, Paris.
Practical work in *Programming Languages and Compilers* course.
- 2007–2008 **Teaching assistant**, *ENSTA*, Paris.
Practical work in *Programming* and *Algorithmic* course.
- March–July 2005 **Intern**, *Royal Holloway University of London*, supervisor: C. Cid.
Algebraic attacks and analysis of the XSL algorithm.
- June–July 2004 **Intern**, *ENS Lyon*, supervisor: A. Tisserand.
FPGA implementation of multipliers over \mathbb{F}_{2^n} and comparison of different designs.

Ph.D. Thesis

- project title *Design and Analysis of Hash Functions*
- I intend to complete the Ph.D. in December 2009
- supervisors David Pointcheval and Pierre-Alain Fouque
- description The first part will be dedicated to cryptanalytic results. I will describe various results against members of the MD4 family, which include the most widely used hash function today. I also show some attacks on various other designs, including some SHA-3 candidates. This part includes academic breaks, and attacks against some higher level constructions. In the second part, I will explain the design of SIMD, our candidate in the SHA-3 competition. This design is inspired by the MD4 family, but we used our knowledge of previous attacks to build a secure hash function. As of today, there are no known weaknesses in SIMD.

Research Publications

- SHA-3 candidate *SIMD is a Message Digest*, with C. Boullaguet and P.-A. Fouque
Eprint *Practical Key Recovery Attack against Secret-prefix EDON- \mathcal{R}*
Online *Cryptanalysis of ESSENCE*, with M. Naya-Plasencia, A. Röck, J.-P. Aumasson, W. Meier, T. Peyrin
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 Interests

- SHA-3 Competition
- Symmetric key cryptography
- Cryptanalysis
- Design of symmetric key primitives

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.

Languages

- French **Native**
English **Fluent**
German **Basic**

Other Activities

- social Treasurer of the ENS students' association for one year.
interests Movies, travels, free software, ...