Damien Robert

Researcher in cryptography

Inria Bordeaux Sud-Ouest

Paris, France
☎ *+33 6 66 56 25 49*
✉ *damien.robert@inria.fr*
www.normalesup.org/~ robert/
French, Born in 1984

Research

Mars 2012–Actuel — **Researcher**, *Inria Bordeaux Sud-Ouest, Bordeaux*, Projet team LFANT.
List of publications: *www.normalesup.org/~ robert/pro/publications/*
See also the appendix.

Work

August 2011–February 2012 — **Researcher Engineer**, *Microsoft Research, Redmond*, Team manager: Kristin Lauter.
Developing the Microsoft cryptographic library.

October 2010–August 2011 — **Postdoc**, *Inria Bordeaux Sud-Ouest, Bordeaux*, Team manager: Andreas Enge.
Genus 2 curves and complex multiplication.

July 2010–September 2010 — **Microsoft Research Summer Internship**, *Redmond, USA*, Mentor: Kristin Lauter.
Speeding up the CRT method in genus 2 for generating class polynomials

Education

January 2007–June 2010 — **PhD Thesis**, *Loria, Nancy*, Advisor: Guillaume Hanrot.
Theta functions and applications in cryptography. Defended July 23 2010.

September–December 2006 — **Master of Science in Computer Science**, *Paris*, Master Parisien de Recherche Informatique, (Inscription Pédagogique).
Courses in cryptography and algebraic number theory

2004–2006 — **Master of Science in Mathematics**, *Paris VI, Paris VII, Paris XI, École Polytechnique*, Algebra and Geometry, With Honors (Courses: 19.88/20, Master Thesis: 18/20, Total: 18.94/20).
(Pedagogic inscription in 2004–2005.) Master Thesis on "Classification of complex reflexion groups", Advisor: Michel Broué (Institut Henri Poincaré).

2004–2005 — **Agrégation in Mathematics**, Nationwide competitive examination for recruiting teachers for undergraduate students, Rank 9.

2003–2004 — **Bachelor of Science in Mathematics (L3–M1)**, With Honors (L3: 19/20, M1 Courses: 18.67/20, M1 Thesis: 14/20, M1 Total: 17/20).
Minor in Computer Science. Bachelor Thesis on « Clifford modules and K-theory », with Mehdi Tibouchi, advisor François Pierrot.

2003 — **École Normale Supérieure**, *Paris*, Computer Science, Admitted after the French "Grandes Écoles" competitive examination, Rank 1.

Teaching

2007–2010 **Teaching Fellow (Moniteur) in Computer Science**, *University Henri Poincaré (Nancy).*

- Tutorials of the cryptography course (M1, 30h).
- Course on Web technologies: HTML, CSS, PHP and MySQL (L1, 60h).
- Tutorials of the OCaml programming course (L1, 120h).

March–May 2004 **Quadratic fields and class group**, *École Normale Supérieure.*
Workgroup organized with Mehdi Tibouchi. *See gt/index.html.*

2003–2005 **Teaching Assistant in Mathematics (Khôlles)**, *Lycée Louis Le Grand,Paris.*
In charge of weekly oral examinations (about 60 hours a year) of undergraduate students.

Experiences

2003–2006 **Computer Tutor**, *École Normale Supérieure.*
Help students to use the school computers, organizations of workgroup on LaTeX, Unix… *See www.tuteurs.ens.fr.*

2003–2006 **Student administrator**, *École Normale Supérieure.*
Help the system administrators to maintain the school computers (on Solaris and FreeBSD), configuration of the user sessions, software installation.

Langages

French **Native Speaker**

English **Fluent** *I have lived one year in Knoxville, Tennessee*

German **Basic**

Technical Skills

Programing	C, Java, Ocaml, Perl, PHP, Ruby, Shell.	Notions of	Haskell (Monades), Scheme (`call/cc`).
OS	Linux, Unix, Windows	Personnal Computers	Debian testing and unstable, Ubuntu, Windows XP and Seven.
Scientific	Magma, Matlab, Sage.	Typography	LaTeX, XeTeX.
Web	(X)HTML, CSS, Javascript.	Database	MySQL, PostgreSQL.

Hobbies

Sport Tennis, Table tennis, Badminton, Rock Climbing, Natation, Swimming, Footing.

Juggling Balls and Clubs, Devil Stick.

Safety French First Aid Certificate

Other Driving license.