

Cyril Bouvier

Ph.D. in Computer Science

☎ +33 6 13 96 91 43

✉ mail@cyrilbouvier.fr

🌐 www.cyrilbouvier.fr

Date of birth: 12th January, 1988 (Age: 30)

French nationality

Positions

Research engineer in Computer Science

June 2016–Feb. 2018

Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM),
Montpellier, France

Post-doctoral Researcher at Université de Bordeaux

Sept. 2015–May 2016

Institut de Mathématiques de Bordeaux, Bordeaux, France

Funded by the ANR project SIMPATIC on pairing-based cryptography

Advisors: Guilhem Castagnos and Damien Robert

Education

Ph.D. in Computer Science

Sept. 2012–Aug. 2015

Université de Lorraine, Nancy, France

Title: "Algorithms for integer factorization and discrete logarithms computation"

Thesis director: Paul Zimmermann

"Rapporteurs": Guillaume Hanrot et Reynald Lercier

Other jury members : Jean-Marc Couveignes, Nadia Heninger and Pierre-Étienne Moreau

Research internship

Sept. 2011–July 2012

INRIA, Nancy, France

Subject: "Implementation of the ECM algorithm on graphics cards"

Advisor: Paul Zimmermann

Master of Science in Pure Mathematics (with high honours)

Sept. 2011

Université Paris VI, Paris, France

Master thesis: "Factorization with elliptic curves and graphics cards"

Advisor: Paul Zimmermann

Took classes from Parisian Master of Research in Computer Science

Sept. 2009–June 2010

École Normale Supérieure, Paris, France

Courses completed on cryptography, computer algebra, polynomial systems

Education at École Normale Supérieure de Paris

Sept. 2008–Aug. 2012

École Normale Supérieure, Paris, France

Mathematics and Computer Science programs

Admitted with Scholarship

July 2008

École Normale Supérieure, Paris, France

National competitive exam in Mathematics, Physics and Computer Science

Higher School Preparatory Classes

Sept. 2006–July 2008

Lycée Saint-Louis, Paris, France

Undergraduate courses to prepare nationwide competitive exams in sciences

Teaching

Teaching Fellow during my Ph.D.

Sept. 2012–Aug. 2015

TELECOM Nancy, Nancy, France

192 hours of teaching in Computer Science:

- *Language C (practicals and tutorial class, 30 hours in 2012–2013)*
- *Mathematics for computer science (course and tutorial class, 30 hours in 2012–2013 and in 2013–2014)*
- *Fundamentals of computer systems (tutorial and practical class, 12 hours in 2012–2013 and 45 hours 2013–2014 and in 2014–2015)*

Oral examiner

Sept. 2009–June 2010

Lycée Saint-Louis, Paris, France

30 hours of oral examination of undergraduate Mathematics majors

Skills

Programming skills

- Programming languages: C, Python, Bash, CUDA
- Computer algebra system: Sage, Magma
- Revision control software: Git, SVN

Languages

- French: native language
- English: fluent, written and spoken
- Italian: basic

Software development

GMP-ECM

<http://ecm.gforge.inria.fr/>

Implementation in C of Lenstra's Elliptic Curve Method (ECM) for factoring integers.

Author of the GPU code available in the latest releases.

CADO-NFS

<http://cado-nfs.gforge.inria.fr/>

Complete implementation in C/C++ of the NFS and NFS-DL algorithms.

One of the main authors, I mostly contributed to the polynomial selection step and the filtering step.

Publications

Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret.

PhD thesis. 2015. French.

URL: <https://hal.inria.fr/tel-01167281>

Better polynomials for GNFS.

S. Bai, C. Bouvier, A. Kruppa, and P. Zimmermann.

In: (2015).

DOI: [10.1090/mcom3048](https://doi.org/10.1090/mcom3048)

URL: <https://hal.inria.fr/hal-01089507>

Division-Free Binary-to-Decimal Conversion.

C. Bouvier and P. Zimmermann.

In: 63.8 (2014), pp. 1895–1901. ISSN: 0018-9340.

DOI: 10.1109/TC.2014.2315621

URL: <https://hal.inria.fr/hal-00864293>

Discrete logarithm in $GF(2^{809})$ with FFS.

R. Barbulescu, C. Bouvier, J. Detrey, P. Gaudry, H. Jeljeli, E. Thomé, M. Videau, and P. Zimmermann.

In: *Public-Key Cryptography – PKC 2014*. Ed. by H. Krawczyk. Vol. 8383. Lecture Notes in Computer Science. Springer-Verlag, 2014, pp. 221–238. ISBN: 978-3-642-54630-3.

DOI: 10.1007/978-3-642-54631-0_13

URL: <http://hal.inria.fr/hal-00818124>

The filtering step of discrete logarithm and integer factorization algorithms.

C. Bouvier.

Preprint, 22 pages. 2013.

URL: <http://hal.inria.fr/hal-00734654>

Finding ECM-Friendly Curves through a Study of Galois Properties.

R. Barbulescu, J. W. Bos, C. Bouvier, T. Kleinjung, and P. L. Montgomery.

In: *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*. Ed. by E. W. Howe and K. S. Kedlaya. Vol. 1. Open Book Series. Mathematical Sciences Publishers, 2013, pp. 63–86.

DOI: 10.2140/obs.2013.1.63

URL: <https://hal.inria.fr/hal-00671948>

Factorisation à l’aide de courbes elliptiques et de cartes graphiques.

C. Bouvier.

Mémoire de stage de Master. 2011

Talks

Seminars

- Crypto seminar of Rennes, IRMAR, Rennes (01/29/2016)
- Seminar of the ECO/ESCAPE teams, LIRMM, Montpellier (12/16/2015)
- Seminar of the LFANT team, IMB, Bordeaux (09/08/2015)
- Seminar of the POLSYS team, LIP6, Paris (07/02/2015)
- Seminar of the ARIC team, LIP, Lyon (01/17/2013)
- Seminar of the CAMEL team, LORIA, Nancy (11/30/2011)
- Seminar at LACAL, EPFL, Lausanne (11/15/2011)
- Seminar of the CAMEL team, LORIA, Nancy (06/30/2011)

Invited speaker

- at “CATREL Workshop: Advances in Discrete Logarithms” at LIX, Paris (10/01-02/2015)
- at 8th Scientific Days of Toulon University as part of a serie of talks intituled “High Performance Computing: from cryptanalysis to bulk of scientific data” (04/15-16/14)