Cyril Bouvier

Docteur en Informatique

+33 6 13 96 91 43
mail@cyrilbouvier.fr
www.cyrilbouvier.fr
Né le 12 janvier 1988 (30 ans)
Nationalité française

Expérience professionnelle

Ingénieur de Recherche en Informatique juin 2016–fév. 2018
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier (LIRMM), Montpellier, France
Service Appui à la Recherche pour le pôle Algo–Calcul du département Informatique

Postdoctorant à l'Université de Bordeaux sept. 2015–mai 2016
Institut de Mathématiques de Bordeaux, Bordeaux, France
Dans le cadre du projet ANR SIMPATIC sur la cryptographie à base de couplages
Responsables : Guilhem Castagnos et Damien Robert

Formation

Doctorat en Informatique sept. 2012–août 2015
Université de Lorraine, Nancy, France
Titre : "Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret"
Directeur de thèse : Paul Zimmermann
Rapporteurs : Guillaume Hanrot et Reynald Lercier
Jury : Jean-Marc Couveignes, Nadia Heninger et Pierre-Étienne Moreau

Stage de recherche sept. 2011–juil. 2012
INRIA, Nancy, France
Sujet : "Implémentation de l'algorithme ECM sur cartes graphiques"
Sous la direction de Paul Zimmermann

Master de Mathématiques fondamentales (Mention Bien) sept. 2011
Université Paris VI, Paris, France
Sujet du mémoire : "Factorisation à l'aide de courbes elliptiques et de cartes graphiques"
Sous la direction de Paul Zimmermann

Cours du Master Parisien de Recherche en Informatique sept. 2009–juin 2010
École Normale Supérieure, Paris, France
Cours de cryptographie, calcul formel, systèmes polynomiaux

Scolarité à l'École Normale Supérieure de Paris sept. 2008–août 2012
École Normale Supérieure, Paris, France
Parcours Mathématiques–Informatique

Admis au concours d'entrée de l'École Normale Supérieure de Paris juil. 2008
École Normale Supérieure, Paris, France
Concours Mathématiques–Physique–Informatique

Classes Préparatoires sept. 2006–juil. 2008
Lycée Saint-Louis, Paris, France
MPSI puis MP

Baccalauréat Général Scientifique juil. 2006
Lycée Racine, Paris
Mention Très Bien

Enseignements

Doctorant contractuel chargé d'enseignement sept. 2012–août. 2015
TELECOM Nancy, Nancy, France
192 heures d'enseignement en Informatique :
— *Langage C (TP/TD, 30 heures en 2012–2013)*
— *Mathématiques pour l'Informatique (cours–TD, 30 heures en 2012–2013 et en 2013–2014)*
— *Principes fondamentaux des systèmes informatiques (TP/TD, 12 heures en 2012–2013 et 45 heures en 2013–2014 et en 2014–2015)*

«Colleur» sept. 2009–juin 2010
Lycée Saint-Louis, Paris, France
30 heures d'interrogation orale en Mathématiques en MPSI

Compétences

Compétences informatiques

— Programmation : C, Python, Bash, CUDA
— Logiciels scientifiques : Sage, Magma
— Gestionnaires de versions : Git, SVN

Langues

— Anglais : bon niveau, oral et écrit
— Italien : niveau scolaire

Contributions logicielles

GMP-ECM `http://ecm.gforge.inria.fr/`
Implémentation en C de la méthode de factorisation d'entiers à l'aide de courbes elliptiques.
Auteur du code pour cartes graphiques disponibles dans les dernières versions.

CADO-NFS `http://cado-nfs.gforge.inria.fr/`
Implémentation complète en C/C++ des algorithme NFS et NFS-DL.
Un des principaux développeurs, majoritairement pour les étapes de filtrage et de sélection polynomiale.

Publications

Algorithmes pour la factorisation d'entiers et le calcul de logarithme discret.
Thèse de doct. 2015.
URL : `https://hal.inria.fr/tel-01167281`

Better polynomials for GNFS.
S. Bai, C. Bouvier, A. Kruppa et P. Zimmermann.
In : (2015).
DOI : `10.1090/mcom3048`
URL : `https://hal.inria.fr/hal-01089507`

Division-Free Binary-to-Decimal Conversion.
C. Bouvier et P. Zimmermann.
In : 63.8 (2014), p. 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 et P. Zimmermann.
In : *Public-Key Cryptography – PKC 2014*. Sous la dir. de H. Krawczyk. T. 8383. Lecture Notes in Computer Science. Springer-Verlag, 2014, p. 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 et P. L. Montgomery.
In : *ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium*. Sous la dir. d'E. W. Howe et K. S. Kedlaya. T. 1. Open Book Series. Mathematical Sciences Publishers, 2013, p. 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

Séminaires et conférences

Séminaires

— Séminaire de cryptographie de Rennes, IRMAR, Rennes (29/01/2016)
— Sémainaire des équipes ECO/ESCAPE, LIRMM, Montpellier (16/12/2015)
— Sémainaire de l'équipe LFANT, IMB, Bordeaux (08/09/2015)
— Sémainaire de l'équipe POLSYS, LIP6, Paris (02/07/2015)
— Sémainaire de l'équipe ARIC, LIP, Lyon (17/01/2013)
— Sémainaire de l'équipe CARAMEL, LORIA, Nancy (30/11/2011)
— Séminaire au LACAL, EPFL, Lausanne (15/11/2011)
— Sémainaire de l'équipe CARAMEL, LORIA, Nancy (30/06/2011)

Orateur invité

— au «CATREL Workshop : Advances in Discrete Logarithms» au LIX, Paris (01-02/10/2015)
— aux 8^{e} Journées Scientifique de l'Université de Toulon dans le cadre du colloque intitulé «Calcul Haute Performance : de la cryptanalyse aux masses de données scientifiques» (15-16/04/14)