

## ACADEMIC DEGREES

- Jul. 2011    **Doctor of Philosophy** in Computer Science  
*Thesis.* “Endomorphism Rings in Cryptography”  
Eindhoven University of Technology, The Netherlands  
Institut National Polytechnique de Lorraine, Nancy, France
- Oct. 2007    **Master of Science** in Mathematics  
*Thesis.* “On the generation of pairing-friendly elliptic curves”  
University of Paris XI, France
- Jul. 2006    **French Agrégation** in Mathematics
- Jul. 2004    **Admitted to the École Normale Supérieure** through competitive examinations

## RESEARCH EXPERIENCE

- since        **Research Fellow**  
Sept. 2011    *Supervisor:* Igor SHPARLINSKI, Department of Computing  
Macquarie University, Sydney, Australia
- June–        **Research Intern**  
Sept. 2011    *Supervisor:* Kristin LAUTER, Cryptography Group  
Microsoft Corporation, Redmond, United States
- Feb. 2008–    **Ph.D. Candidate**  
Jul. 2011     *Advisors.* Pierrick GAUDRY, LORIA Lab, Nancy, France  
                  Tanja LANGE, Eindhoven University of Technology, The Netherlands
- Apr.–        **Research Student**  
Sept. 2007    *Advisor:* Takakazu SATOH, Number Theory Group  
Tokyo Institute of Technology, Japan

## TEACHING EXPERIENCE

- Sept. 2008–    **Teaching Fellow** (*moniteur*) of Computer Science  
Aug. 2011     Duties include teaching graduate courses:
- Tutorials for the Java programming course; 117 hours in total.
  - Tutorials for the entrance seminar; 52 hours in total.
  - Course on algorithmic graph theory; 14 hours in total.
  - Course on algorithms for integer factorization; 14 hours in total.
  - Tutorials for the “IT Techniques and Solutions” course; 10 hours in total.
- École Nationale Supérieure des Mines de Nancy, France
- Sept. 2005–    **Teaching Assistant** (*colleur*) of Mathematics  
Apr. 2007     In charge of weekly oral examinations of undergraduate students; 124 hours in total.  
Lycée Louis-le-Grand (MPSI) and Lycée Chaptal (MP\*), Paris, France

## MISCELLANEOUS SKILLS

**Languages:** Fluent in English and French; basic conversation in German and Japanese.

**Programming:** Proficient in C, PARI/GP, Magma,  $\text{\LaTeX}$ , and POSIX shell.

**Recreational activities:**

- Game of Go (ranked 7 kyu),
- Sailing (skipper of 45-foot sailboats),
- Diving (PADI Advanced Open Water Diver).

**Contributions to open-source software:**

- Developer for the Arch Linux distribution,
- CS Tutor at the École Normale Supérieure,
- Author of the StirFS encrypted filesystem.

## RESEARCH ARTICLES

Gaetan BISSON. “Computing endomorphism rings of elliptic curves under the GRH.”  
In: *Journal of Mathematical Cryptology*. 5.2 (Oct. 2011), pages 101–113.  
DOI: 10.1515/JMC.2011.008.

Gaetan BISSON and Andrew V. SUTHERLAND.  
“A low-memory algorithm for finding short product representations in finite groups.”  
In: *Designs, Codes and Cryptography* 63.1 (2012), pages 1–13.  
DOI: 10.1007/s10623-011-9527-8.

Gaetan BISSON and Andrew V. SUTHERLAND.  
“Computing the endomorphism ring of an ordinary elliptic curve over a finite field.”  
In: *Journal of Number Theory* 131.5 (May 2011): *Elliptic Curve Cryptography*. Edited by  
Neal KOBLITZ and Victor S. MILLER, pages 815–831.  
DOI: 10.1016/j.jnt.2009.11.003.

Gaetan BISSON and Takakazu SATOH.  
“More discriminants with the Brezing-Weng method.”  
In: *Progress in Cryptology — INDOCRYPT 2008*.  
Edited by Dipanwita R. CHOWDHURY, Vincent RIJMEN, and Abhijit DAS. Volume 5365.  
Lecture Notes in Computer Science. Springer, Dec. 2008, pages 389–399.  
DOI: 10.1007/978-3-540-89754-5\_30.

## SERVICE ACTIVITIES

*Program Committee Member.* Manifestation des Jeunes Chercheurs en Sciences et  
Technologies de l’Information et de la Communication.  
Bordeaux, France, Oct. 13–15, 2010.

*Scientific Council Member.* École Normale Supérieure. Paris, France, Nov. 2006–Oct. 2007.

*Student Body Representative.* École Normale Supérieure.  
Paris, France, Nov. 2004–Oct. 2006.

## SOFTWARE

Gaetan BISSON, Romain COSSET, and Damien ROBERT.  
*AVIsogenies, a library for computing isogenies between abelian varieties.*  
Software registered at the Agence pour la Protection des Programmes under reference  
IDDN.FR.001.440011.000.R.P.2010.000.10000. Dec. 2010.  
URL: <http://avisogenies.gforge.inria.fr/>.

## ACADEMIC WORK

Gaetan BISSON. “Endomorphism Rings in Cryptography.” PhD Thesis. Eindhoven University of Technology & Institut National Polytechnique de Lorraine, July 2011. ISBN: 90-386-2519-7.

Gaetan BISSON. “On the generation of pairing-friendly elliptic curves.” Master’s Thesis. University of Paris-Sud 11, Aug. 2007.

Gaetan BISSON and Marc SAGE.  
“Problème de Deligne-Simpson additif, carquois et algèbres de Kac-Moody.” Bachelor’s Thesis. University of Paris-Sud 11, Apr. 2005.

## SELECTED TALKS

### Invited

Gaetan BISSON. “Computing Endomorphism Rings of Abelian Varieties.” Invited talk at the Workshop on Elliptic Curve Cryptography — ECC 2011. INRIA Nancy, France, Sept. 19, 2011.

### Contributed

Gaetan BISSON. “Un algorithme à la Pollard pour le problème du sac à dos.” Talk at the Journées Codage et Cryptographie. CNRS, La Vieille Perrotine, France, Apr. 5, 2011.

Gaetan BISSON. “More Discriminants with the Brezing–Weng Method.” Talk at the International Conference on Cryptology in India. IIT Kharagpur, India, Dec. 15, 2008.

Gaetan BISSON. “Multiplication complexe et discriminants.” Talk at the Journées Nationales de Calcul Formel. CIRM, Luminy, France, Oct. 20, 2008.

Gaetan BISSON. “Construction de courbes elliptiques pairing-friendly.” Talk at the École Jeunes Chercheurs en Informatique Mathématique. CIRM, Luminy, France, Mar. 31, 2008.

## Seminars

- Gaetan BISSON. “Abelian varieties, isogenies, and endomorphism rings.”  
Talk at the LACAL Group Seminar.  
École Polytechnique Fédérale de Lausanne, Switzerland, May 10, 2012.
- Gaetan BISSON. “Variétés abéliennes, isogénies et anneaux d’endomorphismes.”  
Talk at the “Butte aux Cailles” Seminar. Telecom ParisTech, France, May 4, 2012.
- Gaetan BISSON. “Un algorithme à la Pollard pour le problème du sac à dos.”  
Talk at the CRYPTO Group Seminar. University of Versailles, France, May 2, 2012.
- Gaetan BISSON. “Un algorithme à la Pollard pour le problème du sac à dos.”  
Talk at the LFANT Group Seminar. University of Bordeaux, France, Apr. 12, 2012.
- Gaetan BISSON. “Variétés abéliennes, isogénies et anneaux d’endomorphismes.”  
Talk at the Number Theory Seminar. University of Caen, France, Apr. 6, 2012.
- Gaetan BISSON. “Abelian varieties, isogenies and endomorphism rings.”  
Talk at the Number Theory Seminar.  
University of Warwick, United Kingdom, Apr. 2, 2012.
- Gaetan BISSON. “Courbes elliptiques, isogénies et anneaux d’endomorphismes.”  
Talk at the ARITH Group Seminar. University of Montpellier, France, Mar. 28, 2012.
- Gaetan BISSON. “Computing Endomorphism Rings of Abelian Varieties.”  
Talk at the Computational Algebra Seminar. Sydney University, Australia, Nov. 10, 2011.
- Gaetan BISSON. “Endomorphism Rings in Cryptography.”  
Talk at the ACAC Group Seminar. Macquarie University, Australia, Oct. 21, 2011.
- Gaetan BISSON. “Cryptographic Applications of Isogenies.”  
Talk at the Cryptography Group Lunch Seminar.  
Microsoft Research Redmond, United States, July 20, 2011.
- Gaetan BISSON. “Graphes d’isogénies et applications cryptographiques.”  
Talk at the Cryptology Seminar. University of Caen, France, May 26, 2011.
- Gaetan BISSON. “Un algorithme à la Pollard pour le problème du sac à dos.”  
Talk at the Cryptography Seminar. University of Rennes, France, Feb. 4, 2011.
- Gaetan BISSON. “Courbes elliptiques : sécurité et isogénies.”  
Talk at the CRYPTO Group Seminar. University of Versailles, France, Apr. 8, 2010.
- Gaetan BISSON.  
“Calcul des anneaux d’endomorphismes des variétés abéliennes sur les corps finis.”  
Talk at the Number Theory Seminar. University of Bordeaux, France, Nov. 20, 2009.
- Gaetan BISSON.  
“Calcul des anneaux d’endomorphismes des courbes elliptiques sur les corps finis.”  
Talk at the ATI Group Seminar. University of Marseille, France, May 28, 2009.
- Gaetan BISSON.  
“Computing endomorphism rings of ordinary elliptic curves over finite fields.”  
Talk at the EiPSI Group Seminar.  
Technische Universiteit Eindhoven, The Netherlands, Mar. 18, 2009.
- Gaetan BISSON. “Anneaux d’endomorphismes de courbes elliptiques en cryptographie.”  
Talk at the Cryptography Seminar. University of Rennes, France, Jan. 23, 2009.
- Gaetan BISSON. “Complex multiplication and discriminants.”  
Talk at the Number Theory Seminar. Tokyo Institute of Technology, Japan, Oct. 27, 2008.
- Gaetan BISSON. “Complex multiplication and discriminants.”  
Talk at the LCIS Group Seminar. University of Tsukuba, Japan, Oct. 28, 2008.