



# Charles Bouillaguet

*né le 21 janvier 1984, nationalité française*

## Etudes Supérieures

2011–2012 **Post-doctorant**, *Université de Versailles/Saint-Quentin en Yvelines*.

2007–2011 **Doctorat d'informatique**, *Ecole Normale Supérieure (ENS), Paris*.

Titre Etude d'hypothèses algorithmiques et attaques de primitives cryptographiques

Jury	Pierre-Alain Fouque	(responsable)	ENS, France
	Joan Daemen	(rapporteur)	ST Microelectronics, Belgique
	Henri Gilbert	(rapporteur)	ANSSI, France
	Jacques Stern	(président)	ENS, France
	Hubert Comon-Lundh		ENS de Cachan, France
	Arnaud Durand		Université Paris 7, France
	Ludovic Perret		Université Paris 6, France
	Vincent Rijmen		Katholieke Universiteit Leuven, Belgique

2007 **Master Parisien de Recherche en informatique**, *Mention très bien, classé 14ème*.

Mémoire Sécurité et preuves de sécurité des fonctions de hachage

Responsable Pierre-Alain Fouque

Cours suivis ▷ Logique linéaire et paradigmes logiques ▷ Concurrence ▷ Démonstration automatique  
▷ Fondements des systèmes de preuves ▷ Assistants de preuves ▷ Vérification de systèmes dynamiques et paramétrés ▷ Algorithmique avancée ▷ Cryptologie ▷ Codes correcteurs d'erreurs, systèmes polynomiaux et applications à la cryptographie ▷ théorie des jeux ▷ Optimisation ▷ Algorithmique des graphes ▷ Informatique quantique et applications

2005 **Licence d'informatique**, *mention très bien*.

2004–2007 **Etudiant à l'Ecole Normale Supérieure de Cachan**.

2002–2004 **Classes préparatoires**, *Lycée Henri IV, Paris*.  
MPSI puis MP. Admis à l'Ecole Normale Supérieure de Cachan.

2002 **Baccalauréat scientifique**, *mention très bien*.

## Charges d'enseignement

2009–2011 **Chargé de TD**, *Ecole Normale supérieure, Paris*.  
Algorithmique en L3 (une séance sur deux), 13h

2009–2011 **Chargé de TD**, *Lycée Louis-le-Grand, Paris*.  
Programmation en OCaml en deuxième année de classes prépa (MP\*), 80 h/an

2007–2009 **chargé de TD**, *ENSTA, Paris*.  
Programmation en C, et introduction à l'algorithmique, 30h/an

2007–2008 **chargé de TD**, *Lycée Raspail, Paris*.  
Programmation en Maple, en 1ère année de classes prépa (PCSI), 60h

2007–2008 **chargé de TD**, *Lycée Lakanal, Sceaux*.  
Programmation en Maple, en 1ère année de classes prépa (MSI), 60h

*Charles Bouillaguet, UVSQ (PRiSM Lab)*

45, avenue des États-Unis – 78035 Versailles Cedex – France

☎ +33.6.18.12.13.93 • ✉ [charles.bouillaguet@gmail.com](mailto:charles.bouillaguet@gmail.com)

• <http://www.di.ens.fr/~bouillaguet>

---

## Publications

### Vulgarisation scientifique

- 2011 *Sommes-nous prisonniers des CODES SECRETS ?*, avec P.-A. Fouque, collection “les petites pommes du savoir”, éditions du pommier
- 2010 Postface du roman *Le code de Cambridge*, de Tony Gheeraert, collection “roman et plus”, éditions du pommier

### Articles de recherche

- Asiacrypt 2011 *Practical Key-recovery For All Possible Parameters of SFLASH*, avec P.-A. Fouque et G. Maccario-Rat
- CRYPTO 2011 *Automatic Search of Attacks on round-reduced AES and Applications*, avec P. Derbez, P.-A. Fouque et L. Perret
- SAC 2011 *New Insights on Impossible Differential Cryptanalysis*, avec O. Dunkelman, P.-A. Fouque et G. Leurent
- PKC 2011 *Practical Cryptanalysis of the Identification Scheme Based on the Isomorphism of Polynomial With One Secret Problem*, avec J.-C. Faugère, P.-A. Fouque et L. Perret
- J. Math. Crypto *A Family of Weak Keys in HFE and the Corresponding Practical Key-Recovery*, avec P.-A. Fouque, A. Joux et J. Treger
- CHES 2010 *Fast Exhaustive Search for Polynomial Systems Over  $\mathbb{F}_2$* , avec H.-C. Chen, C.-M. Cheng, T. Chou, R. Niederhagen, A. Shamir, and B.-Y. Yang
- SAC 2010 *Security Analysis of SIMD*, avec P.-A. Fouque et G. Leurent
- SAC 2010 *Attacks on Hash Functions based on Generalized Feistel - Application to Reduced-Round Lesamnta and SHAvite-3*, avec O. Dunkelman, G. Leurent et P.-A. Fouque
- FSE 2010 *Another Look at the Complementation Property*, avec O. Dunkelman et G. Leurent, P.-A. Fouque
- SHA-3 candidate *SIMD is a Message Digest*, avec G. Leurent et P.-A. Fouque
- SAC 2009 *Herding, Second Preimage and Trojan Message Attacks Beyond MD*, avec E. Andreeva, J. Kelsey et O. Dunkelman
- SAC 2008 *Analysis of the Collision Resistance of RadioGatún using Algebraic Techniques*, avec P.-A. Fouque
- Eurocrypt 2008 *Second Preimage Attacks On Iterated Hash Functions*, avec E. Andreeva, P.-A. Fouque, J. Hoch, J. Kelsey, A. Shamir et S. Zimmer
- VMCAI 2007 *Using First-Order Theorem Provers in the Jahob Data Structure Verification System Verification*, avec V. Kuncak, T. Wies, K. Zee et M. Rinard

---

## Exposés dans des Workshops ou des séminaires extérieurs

- Octobre 2008 **Séminaire ENSTA/LIP6, Paris.**
- Juin 2010 **Séminaire crypto de l'UVSQ, Versailles.**
- Juin 2010 **Exposé aux workshop TOOLS et SCC, Egham, UK.**
- Décembre 2010 **Séminaire du GREYC, Caen.**
- Novembre 2011 **Séminaire crypto de l'IRMAR, Rennes.**
- Décembre 2011 **Séminaire du LSV, Cachan.**
- Janvier 2012 **Séminaire de l'équipe CAMEL au LORIA, Nancy.**

---

## Sejours à l'étranger

- 2006 **Avril → septembre, Stage de M1 sous la direction de Viktor Kuncak.**  
Massachusetts Institute of Technology, Cambridge, MA, USA
- 2011 **Fevrier, Séjour d'une semaine dans l'équipe de Vincent Rijmen.**  
Katholieke Universiteit Leuven, Belgique

---

## Responsabilités Scientifiques

○ J'ai référé des articles pour de nombreuses conférences de cryptographie, telles que CRYPTO 2009 et 2011, Eurocrypt 2009, Asiacrypt 2009, 2010 et 2011, FSE 2011, PKC 2010, ICALP 2008 et SAC 2009. J'ai également référé des articles pour les revues *Journal of Cryptology*, *Information Processing Letters*, et *Design, Codes and Cryptology*.

---

## Divers

- Langues parlées Français, Anglais (écrit et oral), un peu d'Allemand
- Programmation C, C++, Ocaml, PHP, Java, Python, Prolog, SQL, un peu d'assembleur