1 B rue du Pont Royal
92220 Bagneux, France
+33 6 17 37 61 17
fabrice.ben.hamouda@ens.fr
www.normalesup.org/~fbenhamo
Né le 28/10/1991

Fabrice Ben Hamouda--Guichoux

Formation

2012–2016 **Thèse et stage prédoctoral**, *ENS, Équipe Crypto CASCADE*, Paris, « Diverse modules and zero-knowledge », sous la direction de Michel Abdalla et David Pointcheval.
Défendue le 1er juillet 2016. Mention très honorable. Jury : Michel Abdalla, Dennis Hofheinz, Antoine Joux (président), Eike Kiltz (rapporteur), David Pointcheval, Leonid Reyzin, Victor Shoup (rapporteur).
Bourse de la Fondation CFM pour la Recherche (2013–2016).
Lauréat du prix de thèse Gilles Kahn 2016 de la SIF

2009–2013 **Département d'informatique**, *École normale supérieure (ENS)*, Paris.

2011–2012 **Master 2 d'informatique**, *ENS – MPRI*, Paris, mention très bien, classé premier.

2010–2011 **Master 1 d'informatique**, *ENS – MPRI*, Paris, mention très bien.

Expériences

2016– **Post-doctorat**, *IBM Watson Research Center, Cryptography Research Group*, NY, USA.

Stages, visites et projets

Sep.–Déc. 2015 **Visiteur**, *IBM Watson Research Center — Cryptography Research Group*, Yorktown Heights, New-York, US, 3 mois.
Non-interactive secure multiparty computation and multilinear maps

Avril–Mai 2012 **Visiteur**, *Technicolor*
Encadrants : Marc Joye et Benoît Libert, Rennes, 1 mois.
Aggrégation de données et protection de la vie privée

Mars–Juillet 2012 **Stagiaire**, *ENS — Équipe Crypto CASCADE*
Encadrants : Michel Abdalla et David Pointcheval, Paris, 4,5 mois.
Sécurité exacte des schémas de signature forward-secure

Mars–Août 2011 **Stagiaire**, *Université de Bristol — Cryptography and Information Security Group*
Encadrants : Elisabeth Oswald et Dan Page, Bristol, Royaume-Uni, 5 mois.
Efficacité et sécurité contre les attaques par canaux auxiliaires de diverses implémentations de RSA
Assembleur x86_64, ARM7, Nios II ; attaques DPA

Juin–Août 2010 **Stagiaire**, *INRIA — Encadrant : Michel Banâtre*, Rennes, 3 mois.
Sûreté de fonctionnement des systèmes de couplage — informatique ubiquitaire (RFID, Java)

2010 **Jeu en ligne sur plateforme Azure**, *ENS*, coordinateur du projet.
Projet du cours « Génie logiciel et Cloud computing », cité sur le blog d'Azure et présenté à Eric Rudder, Senior Vice President, Technical Strategy of Microsoft World (C#, Asp.Net)

Enseignement

2013–2014 **Monitorat**, *Université Paris 7*.
TP d'introduction à la programmation (IF1, L1) et TD de concepts informatiques (CI2, L1)

2014–2015 **Monitorat**, *Université Paris 7*.
TP d'introduction à la programmation (IF1, L1) et TD d'éléments algorithmiques (EA3, L2) ; participation à l'écriture des sujets (nouvelle maquette)

Publications

Articles de conférence

CCA-Secure Inner-Product Functional Encryption from Projective Hash Functions. In PKC'2017.
Fabrice Benhamouda, Florian Bourse, and Helger Lipmaa.

Removing Erasures with Explainable Hash Proof Systems. In PKC'2017.
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Optimization of Bootstrapping in Circuits. In SODA'2017.
Fabrice Benhamouda, Tancrède Lepoint, Claire Mathieu, and Hang Zhou.

Randomness Complexity of Private Circuits for Multiplication. In Eurocrypt'2016.
Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud.

Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryptography with Weak Pseudorandomness. In PKC'2016.
Fabrice Benhamouda, Céline Chevalier, Adrian Thillard, and Damien Vergnaud.

Multilinear and Aggregate Pseudorandom Functions: New Constructions and Improved Security. In Asiacrypt'2015.
Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue.

Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting. In Crypto'2015.
Fabrice Benhamouda, Geoffroy Couteau, David Pointcheval, and Hoeteck Wee.

An Algebraic Framework for Pseudorandom Functions and Applications to Related-Key Security. In Crypto'2015.
Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue.

Security of the J-PAKE Password-Authenticated Key Exchange Protocol. In SP'2015.
Michel Abdalla, Fabrice Benhamouda, and Philip MacKenzie.

Disjunctions for Hash Proof Systems: New Constructions and Applications. In Eurocrypt'2015.
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks. In PKC'2015.
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Efficient Zero-Knowledge Proofs for Commitments from Learning With Errors over Rings. In ESORICS'2015.
Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak.

Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures. In Asiacrypt'2014.
Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven.

Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier. In Crypto'2014.
Michel Abdalla, Fabrice Benhamouda, Alain Passelègue, and Kenneth G. Paterson.

SPHF-Friendly Non-Interactive Commitments. In Asiacrypt'2013.
Michel Abdalla, Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, and David Pointcheval.

New Techniques for SPHFs and Efficient One-Round PAKE Protocols. In Crypto'2013.
Fabrice Benhamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud.

Tighter Reductions for Forward-Secure Signature Schemes. In PKC'2013.
Michel Abdalla, Fabrice Ben Hamouda, and David Pointcheval.

Efficient UC-Secure Authenticated Key-Exchange for Algebraic Languages. In PKC'2013.
Fabrice Ben Hamouda, Olivier Blazy, Céline Chevalier, David Pointcheval, and Damien Vergnaud.

Articles de journaux

Efficient Cryptosystems From 2^k-th Power Residue Symbols.
Journal of Cryptology, 2016.
Fabrice Benhamouda, Javier Herranz, Marc Joye, and Benoît Libert.

A New Framework for Privacy-Preserving Aggregation of Time-Series Data.
ACM TISSEC, 18(3):10:1–10:21, March 2016.
Fabrice Benhamouda, Marc Joye, and Benoît Libert.

Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks.
IET Information Security, 10(6):288–303, 2016.
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Demandes de brevets

Method and device for cryptographic key generation.
Marc Joye, Fabrice Benhamouda, and Benoît Libert.
European patent application WO2015EP65807 20150710, 2014.

Method for determining a statistic value on data based on encrypted data.
Fabrice Benhamouda, Marc Joye, and Benoît Libert.
European patent application EP20130306642 20131129, 2013.

Autres responsabilités

Comités de programme

EUROCRYPT 2017 et PKC 2017

Rapporteur externe

ASIACRYPT 2014, 2015, 2016 ; ACM CCS 2015 ; CRYPTO 2015, 2016 ; CT-RSA 2017 ; EUROCRYPT 2013, 2014, 2015, 2016 ; PKC 2014, 2015, 2016 ; TCC 2016b ; Journal of Cryptology ; Design, Codes, and Cryptography ; IEEE Transactions on Information Forensics and Security

Administration et organisation

2015–2016 **Secrétariat du concours MP/I des ENS**, *Mission doctorale 32h eq td.*
Organisation des oraux et accueil des examinateurs et des candidats.

2016– Co-organisateur du séminaire New York CryptoDay (`https://nycryptoday.wordpress.com`).

2015–2016 Co-organisateur du groupe de lecture Crypto Working Group de l'équipe Crypto de l'ENS.

2013–2016 Organisateur du séminaire CU (Crypto Underground) de l'équipe Crypto de l'ENS.

Sites web

CryptoBib: `https://cryptobib.di.ens.fr` maintenue avec Michel Abdalla

Site web de l'Équipe Crypto de l'ENS: `https://crypto.di.ens.fr`, création du site web

Compétences informatiques

Programmation	Python, C#, C, C++, OCAML *(avancé)* ; Perl, Shell *(moyen)*
Microcontrôleurs	Microchip PIC (C, Asm - *avancé*) ; Nios II (C, Asm) ; Blackfin (linux embarqué)
Hardware	VHDL et Verilog (CPLD / FPGA, Xilinx CoolRunner, Spartan 3A et Altera Cyclone III)
Web	HTML, CSS, PHP, Python / web2py, JavaScript *(moyen)*
Autre	Windows Azure (Cloud computing), RFID tags *(moyen)*
Logiciels	MacOS, Linux (Ubuntu et Debian), Windows, LaTeX (Beamer), SVN, Git, LibreOffice

Compétences linguistiques

Anglais courant

Allemand notions

Centres d'intérêts

Lecture (essentiellement des romans), Vélo, Natation (loisir)