Fabrice Ben Hamouda--Guichoux

✉ *fabrice.benhamouda@normalesup.org*
www.normalesup.org/~fbenhamo

Education

2012–2016 **PhD thesis**, *ENS, Crypto Team CASCADE*, Paris, "Diverse modules and zero-knowledge," under the supervision of Michel Abdalla and David Pointcheval..
Defended on July 1st, 2016. Jury: Michel Abdalla, Dennis Hofheinz, Antoine Joux (president), Eike Kiltz (reviewer), David Pointcheval, Leonid Reyzin, Victor Shoup (reviewer).

2009–2013 **Computer science department**, *École normale supérieure (ENS) — a prestigious institution of higher education providing specialized training to students who will become professors and researchers*, Paris.

2010–2012 ***Master* (equivalent to a Master's degree) in computer science**,
ENS – MPRI, Paris, with highest honors, ranked first.

2009–2010 ***Licence* (equivalent to a Bachelor's degree) in computer science**,
ENS – University Paris 7, Paris, with highest honors.

Professional Experiences

2018– **Research Staff Member**, *IBM T.J. Watson Research Center, Cryptography Research Group*, NY, USA.

Feb.–May 2018 **Postdoc**, *Cryptography Lab, Columbia University*, NY, USA.

2016–2018 **Postdoc**, *IBM T.J. Watson Research Center, Cryptography Research Group*, NY, USA.

Internships and Visits

Jun. 2016 **Visit**, *Cryptology Group, CWI*, Amsterdam, The Netherlands, 1 week.

Sep.–Dec. 2015 **Short-term scholar**, *IBM T.J. Watson Research Center — Cryptography Research Group*, Yorktown Heights, New-York, USA, 3 months.
Non-interactive secure multiparty computation and multilinear maps

Apr.–May. 2012 **Internship**, *Technicolor*
Supervisors: Marc Joye et Benoît Libert, Rennes, France, 1 month.
Privacy-preserving data aggregation

Mar.–July 2012 **Internship**, *ENS — Crypto Team CASCADE*
Supervisors: Michel Abdalla and David Pointcheval, Paris, France, 4.5 months.
Exact security of forward-secure signature schemes

Mar.–Aug. 2011 **Internship**, *Bristol University — Cryptography and Information Security Group*
Supervisors: Elisabeth Oswald and Dan Page, Bristol, United Kingdom, 5 months.
Exploration of efficiency and side-channel security of different implementations of RSA (x86_64, ARM7, Nios II assembly; DPA attacks)

June–Aug. 2010 **Internship**, *INRIA*
Supervisor: Michel Banâtre, Rennes, France, 3 months.
Dependability of aggregating systems — ubiquitous computing (RFID, Java)

2010 **Online multiplayer game on Windows Azure platform**, *ENS*, project coordinator.
Project of the course "Software engineering and Cloud computing", quoted on the Azure Team blog and presented to Eric Rudder, Senior Vice President, Technical Strategy of Microsoft World (C#, Asp.Net)

Teaching

2013–2015 **Teaching assistant**, *University Paris 7, France.*
Introduction to programming and algorithms (undergraduate level)

Honors and Awards

2018 Best paper award: *k-Round MPC from k-Round OT via Garbled Interactive Circuits.* In Eurocrypt 2018 (to appear). Fabrice Benhamouda and Huijia Lin.

2017 ERCIM Cor Baayen Young Researcher Award, Honorary mention

2017 Winner of the iDASH 2017 Track 1 competition (De-duplication for Global Alliance for Genomics and Health). Joint work with Chitchanok Chuengsatiansup, Gilad Asharov, Benny Pinkas, and Tal Rabin.

2016 Gilles Kahn PhD prize

2016 Invited to China Theory Week 2016

2015 Paper invited to IET Information Security:
Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks. In PKC 2015. Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

2013–2016 PhD Scholarship from the CFM Foundation

2011 Best paper award: *Dependability of Aggregated Objects, a pervasive integrity checking architecture.* In UBICOMM 2011. Fabien Allard, Michel Banâtre, Fabrice Ben Hamouda-Guichoux, Paul Couderc, and Jean-François Verdonck

Publications

Conference Papers

Two-Round Adaptively Secure Multiparty Computation from Standard Assumptions. In TCC 2018 (to appear).
Fabrice Benhamouda, Huijia Lin, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam.

On the Local Leakage Resilience of Linear Secret Sharing Schemes. In Crypto 2018.
Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin.

k-Round MPC from k-Round OT via Garbled Interactive Circuits. In Eurocrypt 2018.
Fabrice Benhamouda and Huijia Lin.

Hash Proof Systems over Lattices Revisited. In PKC 2018.
Fabrice Benhamouda, Olivier Blazy, Léo Ducas, and Willy Quach.

Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation. In IEEE Workshop on Blockchain Technologies and Applications (BTA), 2018 IEEE International Conference on Cloud Engineering, IC2E 2018.
Fabrice Benhamouda, Shai Halevi, and Tzipora Halevi.

Robust Non-interactive Multiparty Computation Against Constant-Size Collusion. In Crypto 2017.
Fabrice Benhamouda, Hugo Krawczyk, and Tal Rabin.

Private Multiplication over Finite Fields. In Crypto 2017.
Sonia Belaïd, Fabrice Benhamouda, Alain Passelègue, Emmanuel Prouff, Adrian Thillard, and Damien Vergnaud.

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.

Non-interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms. In ESORICS 2017.
Fabrice Benhamouda, Houda Ferradi, Rémi Géraud, and David Naccache.

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.

From Rational Number Reconstruction to Set Reconciliation and File Synchronization. In TGC 2012.
Antoine Amarilli, Fabrice Ben Hamouda, Florian Bourse, Robin Morisset, David Naccache, and Pablo Rauzy.

Dependability of Aggregated Objects, a pervasive integrity checking architecture. In UBICOMM 2011.
Fabien Allard, Michel Banâtre, Fabrice Ben Hamouda-Guichoux, Paul Couderc, and Jean-François Verdonck.

Journal Papers

On the Tightness of Forward-Secure Signature Reductions.
Journal of Cryptology, 2018 (to appear).
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Related-Key Security for Pseudorandom Functions Beyond the Linear Barrier.
Journal of Cryptology, 2018.
Michel Abdalla, Fabrice Benhamouda, Alain Passelègue, and Kenneth G. Paterson.

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.

Patent Applications

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.

Other Papers

Verifier-Based Password-Authenticated Key Exchange: New Models and Constructions.
Fabrice Benhamouda and David Pointcheval.
Cryptology ePrint Archive, Report 2013/833, 2013.

Non-Academic Publications

Apr. 2017 *Article in 1024 – Bulletin de la Société Informatique de France about my thesis.* (in French)
`http://www.societe-informatique-de-france.fr/wp-content/uploads/2017/04/1024-no10-Benhamouda.pdf`

Feb. 2017 *Blog Post on the Blog Binaire about my thesis.* (in French)
`http://binaire.blog.lemonde.fr/2017/02/03/demontrer-sans-donner-la-preuve`

Professional Activities

Program Committee Member

ACM CCS 2018

Crypto 2018

Eurocrypt 2017

PKC 2017

External Reviewer

ACNS 2018; Asiacrypt 2013, 2014, 2015, 2016, 2017; ACM CCS 2015; Crypto 2015, 2016, 2017; CT-RSA 2017; Eurocrypt 2013, 2014, 2015, 2016, 2018; PKC 2014, 2015, 2016, 2018; SODA 2018; TCC 2016b, 2017, 2018; Journal of Cryptology; Designs, Codes, and Cryptography; IEEE Transactions on Information Forensics and Security; IEEE Transactions on Dependable and Secure Computing

Administration and Organization

2017–2018 Assistant to the General Chair of Crypto 2018

2016– Co-organizer of the New York CryptoDay seminar (`https://nycryptoday.wordpress.com`)

2017 Website admin of `https://eurocrypt2017.di.ens.fr`

2015–2016 Co-organizer of the Crypto Working Group of the ENS Crypto Team

2013–2016 Organizer of the CU seminar (Crypto Underground) of the ENS Crypto Team

2015–2016 Secretariat for entrance examination of ENS, Maths and Computer Science.
Organization of the oral examinations and reception of the candidates

CryptoBib

BibTeX database of papers related to Cryptography `https://cryptobib.di.ens.fr`, maintained with Michel Abdalla

Computer Skills

Programming Python, C#, Java, Go, C, C++, OCAML, Node.js *(advanced)* ; Perl, Shell *(average)*

Microcontroller Microchip PIC (C, Asm – *advanced*) ; Nios II (C, Asm) ; Blackfin (embedded linux, C)

Hardware VHDL (CPLD / FPGA Xilinx – CoolRunner and Spartan 2 / 3A / 3A DSP)

Web HTML, CSS, PHP, Python / web2py, JavaScript *(average)*

Other Windows Azure (Cloud computing), RFID tags *(average)*

Software MacOS, Linux (Ubuntu and Debian), Windows, LaTeX (Beamer), SVN, Git, LibreOffice

Presentations and Invited Talks

k-Round MPC from k-Round OT via Garbled Interactive Circuits
New York Crypto Day, Cornell Tech, NY, USA. Mar. 2018.
Charles River Crypto Day, Northeastern University, Boston, USA. Dec. 2017.

De-duplication for Global Alliance for Genomics and Health
iDASH Privacy & Security Workshop 2017, Orlando, FL, USA. Oct. 2017.

On the Robustness of Non-Interactive Multi-Party Computation /
Robust Non-Interactive Multiparty Computation Against Constant-Size Collusion.
Conference Crypto 2017, Santa Barbara, CA, USA. Aug. 2017.
Charles River Crypto Day, Boston University, Boston, USA. May. 2017.

Optimization of Bootstrapping in Circuits.
Rutgers/DIMACS Theory of Computing Seminar, Piscataway, NJ, USA. Apr. 2017.

Removing Erasures with Explainable Hash Proof Systems.
Conference PKC 2017, Amsterdam, The Netherlands. Mar. 2017.

Diverse Modules and Zero-Knowledge.
Gilles Kahn PhD Prize, Reims, France. Feb. 2017.
Public-Key Cryptography, Dagstuhl seminar, Germany. Sep. 2016.
China Theory Week, Hong Kong. Aug. 2016.

Easing Coppersmith Methods Using Analytic Combinatorics: Applications to Public-Key Cryptography with Weak Pseudorandomness.
Conference PKC 2016, Taipei, Taiwan. Mar. 2016.
Monthly Lattice Meeting, ENS de Lyon, Lyon, France. Mar. 2016

New Techniques for SPHFs and Efficient One-Round PAKE Protocols.
MIT, Cambridge, USA. Nov. 2015
Cryptology Group, CWI, The Netherlands. Jun. 2016.

Implicit Zero-Knowledge Arguments and Applications to the Malicious Setting.
New York Crypto Day, Columbia University, NY, USA. Oct. 2015.

New Results on Password-Authenticated Key-Exchange.
Google Security Group, Mountain View, CA, USA. May 2015.

Security of the J-PAKE Password-Authenticated Key Exchange Protocol.
IEEE Symposium on Security and Privacy, San Jose, CA, USA. May 2015.

Disjunctions for Hash Proof Systems: New Constructions and Applications.
IBM T.J. Watson Research Center, NY, USA. Sep. 2015.
Conference Eurocrypt 2015, Sofia, Bulgaria. Apr. 2015.
Cryptography Seminar of Rennes, France. Apr. 2015.

Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks.
Conference PKC 2015, NIST, MD, USA. Mar. 2015.

Better Zero-Knowledge Proofs for Lattice Encryption.
ENS Lyon – ENS Paris Monthly Meetings, ENS Lyon, Lyon, France, Feb. 2015.

Smooth Projective Hash Functions and Applications.
Technicolor, Palo Alto, CA, USA. Apr. 2014.

SPHF-Friendly Non-Interactive Commitments.
Conference Asiacrypt 2013, Bangalore, India. Dec. 2013.

Comment dévoiler des informations à un agent secret? (French)
Séminaire résidentiel du département d'informatique de l'ENS. Jan. 2014.
Département d'informatique de l'ENS. Oct. 2013.

New Techniques for SPHFs and Efficient One-Round PAKE Protocols.
Conference Crypto 2013, Santa Barbara, CA, USA. Aug. 2013.

Tighter Reductions for Forward-Secure Signature Schemes.
Conference PKC 2013, Nara, Japan. Feb. 2013.
Journées C2, Dinard, France. Sep. 2012.