
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 professor and researchers, Paris.
- 2010–2012 **Master (equivalent to a Master’s degree) in computer science**, *ENS – MPRI*, Paris, with highest honor, ranked first.
- 2009–2010 **Licence (equivalent to a Bachelor’s degree) in computer science**, *ENS – University Paris 7*, Paris, with highest honor.

Experiences

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

Internships, visits, and projects

- Jun. 2016 **Visit**, *Cryptology Group, CWI*, Amsterdam, The Netherlands, 1 week.
- Sep.–Dec. 2015 **Short-term scholar**, *IBM 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

- 2016 Gilles Kahn PhD prize
- Aug. 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 Fellowship from the CFM Foundation

Publications

Conference articles

On the Robustness of Non-Interactive Multi-Party Computation. In Crypto'2017 (to appear).
Fabrice Benhamouda, Hugo Krawczyk, and Tal Rabin.

Private Multiplication over Finite Fields. In Crypto'2017 (to appear).
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, Tancrede 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.

Journal articles

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.

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

EUROCRYPT 2017

PKC 2017

External reviewer

ASIACRYPT 2014, 2015, 2016; ACM CCS 2015; CRYPTO 2015, 2016, 2017; 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 and organization

- 2016–2017 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 (<i>advanced</i>) ; Perl, Shell (<i>average</i>)
Microcontroller	Microchip PIC (C, Asm – <i>advanced</i>) ; 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 (<i>average</i>)
Other	Windows Azure (Cloud computing), RFID tags (<i>average</i>)
Software	MacOS, Linux (Ubuntu and Debian), Windows, L ^A T _E X (Beamer), SVN, Git, LibreOffice

Presentations and Invited Talks

On the Robustness of Non-Interactive Multi-Party Computation.

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.

New Techniques for SPHF's 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 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.
- 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.