Fabrice
Ben Hamouda--Guichoux

✉ fabrice.benhamouda@gmail.com
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

2023– **Senior Applied Scientist**, *Amazon Web Services*, NY, USA

2019–2023 **Researcher**, *Algorand Foundation*, NY, USA

2018–2019 **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

Sep.–Dec. 2015 **Short-term scholar**, *IBM T.J. Watson Research Center, Cryptography Research Group*, NY, USA
Non-interactive secure multiparty computation and multilinear maps

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

Mar.–July 2012 **Internship**, *ENS — Crypto Team CASCADE*
Supervisors: Michel Abdalla and David Pointcheval, Paris, France
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
Exploration of efficiency and side-channel security of different implementations of RSA (x86_64, ARM7, Nios II assembly; DPA attacks)

Teaching

2020–2023 **Guest lectures and presentations about Algorand**
GoTechnica Hackathon 2019, UC Davis 2020, UCSB Blockchain Acceleration Foundation 2021, IEEE Blockchain Americas Virtual Event 2021, UC Berkeley 2021 & 2022, University of Pennsylvania 2022 & 2023, Columbia DevFest Hackathon 2023

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

Honors and Awards

2021 Best paper award: *On the (in)security of ROS.*
In Eurocrypt 2021. Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova

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

2018 IET Information Security Premium Award: *Public-Key Encryption Indistinguishable Under Plaintext-Checkable Attacks.*
In IET Information Security. Michel Abdalla, Fabrice Benhamouda et David Pointcheval

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

Threshold Cryptography as a Service (in the Multiserver and YOSO Models). In ACM CCS 2022.
Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk, Alex Miao, and Tal Rabin.

On the (In)security of ROS. In Eurocrypt 2021.
Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova.

Multiparty Reusable Non-interactive Secure Computation from LWE. In Eurocrypt 2021.
Fabrice Benhamouda, Aayush Jain, Ilan Komargodski, and Huijia Lin.

Mr NISC: Multiparty Reusable Non-Interactive Secure Computation. In TCC 2020.
Fabrice Benhamouda and Huijia Lin.

Can a Public Blockchain Keep a Secret? In TCC 2020.
Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Shai Halevi, Hugo Krawczyk, Chengyu Lin, Tal Rabin, and Leonid Reyzin.

From Single-Input to Multi-client Inner-Product Functional Encryption. In Asiacrypt 2019.
Michel Abdalla, Fabrice Benhamouda, and Romain Gay.

Algebraic XOR-RKA-Secure Pseudorandom Functions from Post-Zeroizing Multilinear Maps.
In Asiacrypt 2019.
Michel Abdalla, Fabrice Benhamouda, and Alain Passelègue.

Decentralizing Inner-Product Functional Encryption. In PKC 2019.
Michel Abdalla, Fabrice Benhamouda, Markulf Kohlweiss, and Hendrik Waldner.

Two-Round Adaptively Secure Multiparty Computation from Standard Assumptions. In TCC 2018.
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 (In)Security of ROS.
Journal of Cryptology, 35(4):25, 2022.
Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova.

On the Local Leakage Resilience of Linear Secret Sharing Schemes.
Journal of Cryptology, 34(2):10, 2021.
Fabrice Benhamouda, Akshay Degwekar, Yuval Ishai, and Tal Rabin.

Gage MPC: Bypassing Residual Function Leakage for Non-Interactive MPC.
PoPETS, 2021(4):528–548, 2021.
Ghada Almashaqbeh, Fabrice Benhamouda, Seungwook Han, Daniel Jaroslawicz, Tal Malkin, Alex Nicita, Tal Rabin, Abhishek Shah, and Eran Tromer.

Falcon: Honest-Majority Maliciously Secure Framework for Private Deep Learning.
PoPETS, 2021(1):188–208, 2021.
Sameer Wagh, Shruti Tople, Fabrice Benhamouda, Eyal Kushilevitz, Prateek Mittal, and Tal Rabin.

On the Tightness of Forward-Secure Signature Reductions.
Journal of Cryptology, 32(1):84–150, 2019.
Michel Abdalla, Fabrice Benhamouda, and David Pointcheval.

Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation.
IBM Journal of Research and Development, 63(2/3):3:1–3:8, March 2019.
Fabrice Benhamouda, Shai Halevi, and Tzipora Halevi.

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.

Other Papers

SPRINT: High-Throughput Robust Distributed Schnorr Signatures.
Fabrice Benhamouda, Shai Halevi, Hugo Krawczyk, Yiping Ma, and Tal Rabin.
Cryptology ePrint Archive, Paper 2023/427, 2023.

Anonymous Counting Tokens.
Fabrice Benhamouda, Mariana Raykova, and Karn Seth.
Cryptology ePrint Archive, Paper 2023/320, 2023.

Weighted Secret Sharing from Wiretap Channels.
Fabrice Benhamouda, Shai Halevi, and Lev Stambler.
Cryptology ePrint Archive, Paper 2022/1578, 2022.

Publicly verifiable anonymous tokens with private metadata bit.
Fabrice Benhamouda, Tancrède Lepoint, Michele Orrù, and Mariana Raykova.
Cryptology ePrint Archive, Report 2022/004, 2022.

Initial Public Offering (IPO) on Permissioned Blockchain using Secure Multiparty Computation.
Fabrice Benhamouda, Angelo DeCaro, Shai Halevi an Tzipora Halevi, Charanjit jutla, Yacov Manevich, and Qi Zhang, 2019.
Accepted at the Workshop on Privacy ENhancing Cryptography In Ledgers (PENCIL) 2019.

How to Profile Privacy-Conscious Users in Recommender Systems.
Fabrice Benhamouda and Marc Joye.
arXiv:1812.00125, 2018.
Accepted at the Privacy Preserving Machine Learning NeurIPS 2018 Workshop (PPML).

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`

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.

Professional Activities

Program Committee Member

Crypto 2023, TCC 2022, Asiacrypt 2021, Crypto 2021, PKC 2021, Eurocrypt 2020, Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC) 2019, SAC 2019, Workshop on Privacy ENhancing Cryptography In Ledgers (PENCIL) 2019, ACM CCS 2018, Crypto 2018, Eurocrypt 2017, PKC 2017

External Reviewer

ACNS 2018; Asiacrypt 2013, 2014, 2015, 2016, 2017, 2020; ACM CCS 2015, 2018; Crypto 2015, 2016, 2017, 2019, 2020, 2022; CT-RSA 2017, 2021; Eurocrypt 2013, 2014, 2015, 2016, 2018, 2019, 2021, 2022, 2023; Euro S&P 2021; ICALP 2020; ISIT 2022; PKC 2014, 2015, 2016, 2018, 2019, 2023; SODA 2018; STOC 2023; TCC 2016b, 2017, 2018; Journal of Cryptology; SIAM Journal on Computing; Designs, Codes, and Cryptography; IEEE Transactions on Information Forensics and Security; IEEE Transactions on Dependable and Secure Computing; IBM Journal of Research and Development; Security and Communication Networks

Administration and Organization

2017–2018	Co-organizer of the conference Crypto 2018
2016–	Co-organizer of the New York CryptoDay seminar (`https://nycryptoday.wordpress.com`)
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	Go, Python, C#, Java, C, C++, OCAML, Node.js *(advanced)* ; Rust, Bash *(intermediate)*
Microcontroller	Microchip PIC (C, Asm – *advanced*) ; Nios II (C, Asm) ; Blackfin (embedded linux, C)
Web	HTML, CSS, Python/web2py, JS/ReactJS *(intermediate)*
Other	Google Cloud Platform, VHDL/Verilog for FPGA *(basic)*
Software	MacOS, Linux (Ubuntu and Debian), Windows, LaTeX (Beamer), Git, Office / LibreOffice

Presentations and Invited Talks

Mr NISC from LWE: Multiparty Reusable Non-Interactive Secure Computation
Lattices: Algorithms, Complexity, and Cryptography Reunion. Jun. 2021

Mr NISC: Multiparty Reusable Non-Interactive Secure Computation
Conference TCC 2020, Virtual. Nov. 2020

On the Local Leakage Resilience of Linear Secret Sharing Schemes
Cornell Crypto Seminar, Cornell Tech, NY, USA. Mar. 2019

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