Samuel Bouaziz--Ermann

samuel.bouaziz@ens-rennes.fr
perso.eleves.ens-rennes.fr/people/samuel.bouaziz/ • 0009-0003-6394-9387

Professional Experience

2026–now Postdoctoral researcher, Applied Cryptography Unit, OIST, Okinawa
Supervisor: Carlos Cid

2021–2025 PhD in Computer Science, Sorbonne Université, LIP6, CNRS, Paris
Title: Cryptographic Primitives in Quantum Idealized Models
Supervisors: Damien Vergnaud and Alex Bredariol Grilo

Feb. 2024 Invited Researcher, Simons Institute, UC Berkeley, California

2021 Master internship, Almasty and QI team, LIP6, Sorbonne Université, Paris
Title: On quantum key exchange with classical communication from one-way functions
Supervisors: Alex Grilo and Damien Vergnaud

2020 Master internship, EMSEC team, Inria, Rennes
Title: Finding short vectors in lattices
Supervisors:Adeline Roux-Langlois and Olivier Bernard

2019 Bachelor internship, EMSEC team, Inria, Rennes
Title: Implementation of a blind signature in C
Supervisors: Adeline Roux-Langlois, Guillaume Kaim and Gautier Eberhart

Education

2020–2021 Master 2, Parisian Master of Research in Computer Science (MPRI), Paris

2020–2021 Magistère, Ecole Normale Supérieure de Rennes, Rennes

2018–2021 License and Master 1 in computer science, Ecole Normale Supérieure de Rennes, Rennes

2016–2018 Preparatory classes, Lycée Saint-Louis, Paris

Publications and Preprints

- Cryptographic Primitives in Quantum Idealized Models (2025), PhD Manuscript
  Samuel Bouaziz--Ermann
- On Limits on the Provable Consequences of Quantum Pseudorandomness (2025), Preprint
  Samuel Bouaziz--Ermann, Minki Hhan, Quoc-Huy Vu, Garazi Muguraza
- Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way (2024), Preprint
  Samuel Bouaziz--Ermann, Garazi Muguraza
- Towards the Impossibility of Quantum Public Key Encryption with Classical Keys from One-Way Functions (2024), Communications in Cryptology
  Samuel Bouaziz--Ermann, Alex Bredariol Grilo, Damien Vergnaud, Quoc-Huy Vu
- Quantum security of subset cover problems (2023), ITC 2023
  Samuel Bouaziz--Ermann, Alex Bredariol Grilo, Damien Vergnaud

Talks

Conference

Quantum Security of Subset Cover Problems, June 2023, ITC 2023

Workshops

L'impact des ordinateurs quantiques sur les cinq mondes d'Impagliazzo, April 2025, WRACH 2025

Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way, July 2024, Almasty team Workshop

Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way, May 2024, IQC-PCQT Workshop

Seminars

Quantum Security of Subset Cover Problems, June 2023, Algocomp seminar

Quantum Security of Subset Cover Problems, December 2022, Almasty team Seminar

Quantum Pseudorandomness Cannot Be Shrunk In a Black-Box Way, May 2024, Séminaire de l'équipe Quasar, Ottawa, Canada

Others

Cryptographic Primitives in Quantum Idealized Models, October 2025, PhD Defense

The Wonderful Worlds of Quantum Pseudorandomness, April 2025, Journées C2 2025

On the impossibility of Quantum Public Key Encryption, Octobre 2023, Journées C2 2023

On quantum key exchange with classical communication from one-ways functions, April 2022, Journées C2 2022

Teaching

Graduate Teaching

2023-2024 Modern Cryptography, Lab, Master 2

Complexe, Tutorial and Lab, Master 1

Discrete Mathematics, Lab, Master 1

Advanced C, Lab, License 2

2022-2023 Introduction to relational databases, MySQL, Tutorial and Lab, License 2

Advanced quantum algorithms, Tutorial, Master 2

Functionnal programming, Ocaml, Lab, License 2

2021-2022 Functionnal programming, Ocaml, Lab, License 2

Programming elements, Python, Lab, License 1

Other Interventions

2021-2025 Science Outreach Volunteer, Presented computer science concepts to elementary and middle school students at a science festival

2019 Pedagogy Course, Presented computer science concepts to middle school students

Service

Participated as a subreviewer for international conferences (EC 2026, ITCS 2025, AC 2025, QIP 2024, Crypto 2023, CCC 2023)

Languages

French Native language

English Advanced

Programming languages

C, C++, HTML/CSS, Latex, Lisp, Ocaml, Python, Sage, Java, Javascript