Olivier Blazy

PROFESSOR IN CYBERSECURITY | CRYPTOGRAPHER

École Polytechnique — LIX, GRACE team — Institut Polytechnique de Paris, Palaiseau, France | olivier.blazy@polytechnique.edu | blazy.eu

Academic Positions

2026 – **Scientific Director, CIEDS** École Polytechnique · Institut Polytechnique de Paris

2021 – **Professor, École Polytechnique** LIX · GRACE team · Palaiseau

2014 – 2021 **Associate Professor (MCF), Université de Limoges** XLIM · Cryptis — HDR 2019

2012 – 2014 **Postdoctoral Researcher, Ruhr-Universität Bochum** Foundations of Cryptography

Education

2012 **Ph.D. in Computer Science, ENS Paris** advisor: David Pointcheval

2019 **Habilitation (HDR), Université de Limoges**

Research Interests

Provable security and smooth projective hash functions; post-quantum and code-based cryptography (incl. HQC, a NIST standard); anonymous credentials and group signatures; digital identity and online age verification; privacy-preserving protocols and secure messaging.

Selected Publications

80+ peer-reviewed publications. Full list: blazy.eu/#papers.

- **How fast do you heal? A taxonomy for post-compromise security in secure-channel establishment**. *USENIX Security*, 2023.
- **Durandal: A Rank Metric Based Signature Scheme**. *EUROCRYPT*, 2019.
- **(Hierarchical) Identity-Based Encryption from Affine Message Authentication**. *CRYPTO*, 2014.
- **Public-Key Generation with Verifiable Randomness**. *ASIACRYPT*, 2020.
- **Structure-Preserving Smooth Projective Hashing**. *ASIACRYPT*, 2016.
- **SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol**. *IEEE EuroS&P*, 2019.
- **Hash Proof Systems over Lattices Revisited**. *PKC*, 2018.
- **Efficient Encryption from Random Quasi-Cyclic Codes**. *IEEE Trans. Information Theory*, 2018.

Ph.D. Supervision

8 doctoral students — 5 defended (2018–2023), 3 in progress — on identity-based, privacy-preserving and post-quantum cryptography.

Academic Service

- Program committee member for 55+ international conferences and workshops (incl. major IACR venues); 60+ invited talks across 16 countries.
- Editorial Board, *Computer Law and Security Review* (Elsevier), since 2020.
- Director of a national code-and-cryptography working group (2021–2025); board member of national research groups on information security and on cybersecurity and humanities.
- Vice-President, Department of Computer Science (DIX), École Polytechnique (2024–2026). Expert reviewer: ANR, Horizon Europe; technical expert, CNIL.

Teaching

Introduction to Computer Programming (Python), Bachelor of Science, École Polytechnique. Academic advisor for the X-Bachelor, MScT Cybersecurity and X-EPITA programmes. 2009–2021: cryptography, security and algorithmics courses at Limoges and Paris.