123 avenue Albert Thomas
Université de Limoges
87000 Limoges (France)
✉ olivier@blazy.eu
http://www.blazy.eu
Born 20/03/1986 (Décines, France)

Olivier Blazy

Employment

2014–* **Maître de Conférence (∼ Tenured Associate Professor)**, *University of Limoges*, Master level teaching in various areas of Security and Cryptography (Public Key, Private Key, Network Security and Administration, . . .).

2012–2014 **Postdoctoral Position**, *Ruhr-University Bochum*, with Eike Kiltz in the Foundation of Cryptography workgroup, Horst Görtz Institute for IT-Security.
Zero-Knowledge Proofs, Semi-Functional spaces, Tight Signatures

Education

2019 **Habilitation (HDR) in Computer Science**, *University of Limoges*, Hash Proofs Systems and Applications to Implicit Cryptography.

2008–2012 **PhD in Computer Science**, *University Paris 7*, supervised by David Pointcheval (ENS, CNRS), Interactive and Non-Interactive proofs of knowledge.

2005–2009 **Predoctoral Studies in Computer Science**, *ENS*, Paris.

2006-2009 **Research Master in Computer Science**, *MPRI, ENS*.

2007 **Master Internship (6 months)**, *VeriSign*, Mountain View (United States).
- Advisor David M'Raihi.
- Topics: OpenID, Recommendation Engine, PKI, . . .

2005-2006 **Bachelor in Computer Science**, *Paris VII, ENS*.

2006 **Bachelor Internship (2 months)**, *Catholic University of Louvain-la-Neuve*, Belgium.
- *Automatic Analysis of cryptographic protocols based on modular exponentiation*
  Advisor Olivier Pereira.
- Topics: GDH Protocols, PKA, . . .

2003–2005 **Preparatories classes MPSI, MP* (Aux Lazaristes)**, Lyon, France.

July 2005 **Admission to the École Normale Supérieure**, *National Rank 9th*.

Organizations of Scientific Meetings

2017 **IoT Cybersecurity Day**, *Angoulême (France)*, co-organized with the tech-pole from Nouvelle-Aquitaine, Conferences about security, and cryptographic research in IoT.

Since 2016 **Cryptis Days**, *Limoges (France)*, Alumni conferences about security, and cryptography.

Since 2014 **Cryptis Seminar**, *Limoges (France)*, Every two weeks, Invited Seminars from French and Europeans researchers.

Since 2014 **CCA Seminar**, *Paris (France)*, Every three months, National seminars from the Code and Crypto work group.

Dissemination / Teaching

Media Interview, More than 20 interviews in National / International Press (Times, Financial Times, WSJ,...) about security, and it's impact on the population.

Undergraduate Teaching, Algorithmics, Automatons, Finite-State Machines, Introduction to Cryptography, Network Security, Secure Development.

Research Level Teaching, Various Courses in Public Key Cryptography, Secret Key Cryptography, Cryptographical Mecanisms.

Invited Talks, More than 20 visits and Invited seminars often coupled with a short stay (1-2 weeks) in various places like Oxford, ENS, KIT, UCL, ...

Management / Organization

Since Sept 2020 **GT-C2/GDR-Secu**, in charge of the french national workgroup on codes and cryptography (roughly 250 members), and part of the national research group committee on Security..

Since 2020 **Redocs**, Co-Organizer of the Redocs week, where PhD students meet company to work on shared project and discover research in the industry.

Since 2016 **Cryptis**, In charge of the organization / promotion of Limoges Cybersecurity Master program. I applied and got the SecNumEdu label from french ANSSI (French National Cybersecurity Agency), This gave me the opportunity to exchange with several industries / agencies to better tailor our courses, and prepare student to fit the real world.

Ongoing **PhD. Supervision**, L. Brouilhet, N. Fournaise, B. Cottier (co-supervised with D.Pointcheval, ENS), A. Barthoulot. The 2 last ones were "Cifre" Ph.D in collaboration with a company, P. Germouty (defended in 2018).

Ongoing **Postdoc Supervision**, Sayantan Mukherjee.

Grants and funding

Project title	Source	Amount	Dates	Role
CBCrypt ⋆	ANR	580'000 €	10.2017/09.2021	Member
ALAMBIC	ANR	534'760 €	10.2016/03.2021	Member
IDFIX	ANR	225'000 €	10.2016/03.2021	PI
UNITED	Regional	5'000 €	2015	Member
SUITED	Regional	5'000 €	2016	PI
Secu-Fleet	French NNE	24'000 €	2014/2016	Co-PI
IoTSEC	French NNE	24'000 €	2015/2017	Member

⋆ Through the CBCrypt project, we proposed 6 contenders for the NIST Post Quantum standardization process. After the final round, I have 2 contenders (BIKE and HQC) selected as alternate candidates where NIST has said that they'd like to standardize one of them.

Publications / Scientific Life

- I am part of the ANR Astrid committee in charge of evaluating grant application related to cyber security.
- I have over 40 publications (nearly 1,000 citations) in various academic conferences / journals of the field (Crypto, Eurocrypt, Asiacrypt, Euro S&P,...).
  A full list is available on: blazy.eu/bibli2.php.
- Program Chair of WISTP'18 in Bruxelles (Belgium).
- Program Committee of various international conferences (Asiacrypt 2019, 2020, CT-RSA 2020, ...), reviewers for many more
- Invited Panelist at IEEE Smart Cities 2020

Skills

- Cryptography: Provable Security, Protocol Design, Identity-based Cryptography, Zero-Knowledge Proof, Implicit Proof, Post-Quantum protocols.
- Development: Rust, Python, C++, Java, Ruby, OCamL, Charm.
  Recent prototypes: https://github.com/oblazy/
- Languages: French, English (985 Toeic), German (B1), Basic notions of Italian and Russian.