Julien Béguinot

PhD Student

14 Rue Fermat
75014 Paris
06 74 05 19 53
julien.beguinot@telecom-paris.fr

Formation

2022-... **Télécom Paris**, *Institut Polytechnique de Paris*, PhD Student
Evaluation of Information Leakage in Side Channels & Key Distillation/Distribution under the supervision of Pr. Olivier Rioul and Pr. Sylvain Guilley.

2019-2022 **Télécom Paris**, *Institut Polytechnique de Paris*, Engineering and Master Degrees
- M2 MICAS: Machine Learning, Communications and Security
- Cryptography, Quantum Cryptography and Formal Calculus at the M2 MPRI (Parisian Master of Research in Computer Science)
- ACCQ: Applied Algebra : Cryptography, Quantum information, Coding theory
- MACS: Stochastic Processes and Scientific Computations

2018-2019 **MP* Lycée Saint Louis**

2017-2018 **MPSI Lycée Lakanal**

Awards

- **Comelec Dept. Research Excellence Award (2024)** (1250E grant)
- **UPSaclay & IPParis Best PhD Student Poster Audience Award (2023)** (500E)

Research Publications

- *Formal security proofs via Doeblin coefficients: Optimal side-channel factorization from noisy leakage to random probing*, CRYPTO 2024
- *What can information guess ? Guessing advantage vs. Rényi entropy for small leakages*, ISIT 2024
- *Reliability of Ring Oscillator PUFs with Reduced Helper Data*, IWSEC 2023.
- *Maximal Leakage of Masked Implementations Using Mrs. Gerber's Lemma for Min-Entropy*, ISIT 2023
- *Improved alpha-information bounds for higher-order masked cryptographic implementations*, ITW 2023
- *Removing the field size loss from Duc et al.'s conjectured security bound for masked encodings*, COSADE 2023
- *Side-Channel Expectation-Maximization Attacks*, CHES 2022
- *Side-channel information leakage of code-based masked implementations*, CWIT 2022
- *Be my guess: Guessing entropy vs. success rate for evaluating side-channel attacks of secure chips*, DSD 2022

Projects and Internships

- Intern within the **research and developpment team of Secure-IC**. I worked on the reliability of ring oscillator PUFs. (2022)
- Intern (2 months) in the Tanière-Facile start-up . (2021)
- Project on **intrusion detection system** and counter-attacks on a network. With machine learning over IP packets we detected intrusion in a network. We considered counter-attacks using GANs and explored the corresponding counter-measures using "distillations". (2020)

Teaching

- In 2023, I am teaching assistant at Télécom Paris.
  - Probability: measure theory, conditional expectation, martingale (MACS 201)
  - Algebra: group theory, finite fields (ACCQ 201)
  - Information Theory (ACCQ 202)
  - Coding Theory (ACCQ 204)
  - Statistical Learning (SI 221/ MICAS 911)
  - Cryptography (MICAS 931)
  - Physical Layer Security (MICAS 932)
- In 2022, I have been teaching assistant at Ecole Polytechnique.
  - Efficient Implementation of Learning Algorithms in C++ (INF 442)
  - Algorithmics (CSE 103)

Languages

- English C1 (IELTS 7.5)
- German B1
- Japanese A2

Associative projects

- **Sublimaths** I organize a math club for secondary schoolkid. See https://sublimath.rezel.net/ for more details.
- **JWOC** I have been junior comittee of the junior conference JWOC 2023.
- **Télécom Paris BDS** I co-organized the first edition of the "ekiden du platal" race.
- **Treasurer of Télécom Robotics and Télecode** (2020)