Lachguel Rayan Bachir

rayan.lachguel@student-cs.fr | +33 7 69 94 20 13 | French

Education

MEng/MSc

CentraleSupélec - Paris-Saclay University
Expected Sep 2025 | France
Grande École with a highly selective national exam for entry

Relevant Coursework
Computer Networks and Security
Algorithms and Complexity
Quantum & Statistical Physics
Advanced Computer Networks
Computer Architecture
Algebra and Cryptography

Classes préparatoires

Collège Stanislas and Sorbonne University
Grad. Jun 2022 | France
Intense two year program equivalent to a BSc in math and physics

Links

Github:// sobornostea
LinkedIn:// lachguel
Website:// lachguel.com

Skills

Programming

C • Rust
VHDL • arm & RISC-V assembly
Haskell • Nix • Python • Sage
Git • LaTeX • Linux

Electronics

ChipWhisperer toolchain • FPGA • Emulators

Mathematics

Algebraic number theory for cryptography • Undergrad math (general and linear algebra, real analysis, measure theory...)

Languages

French (Native) • English (Fluent) • German (Intermediary) • Moroccan Arabic (Informal)

Interests

Philosophy • Gardening • Running, swimming, cycling

Experience

Inria - CAPSULE | Research

Nov 2023 – Mar 2024 | Rennes, France

- Improved the security and portability of Falcon and similar primitives
- Study of MPC-in-the-head schemes
- Intervened in internal seminars and was a TA for cryptography courses at the university

TU Berlin - SecT | Research

Feb 2023 – Jul 2023 | Berlin, Germany

- Completed fault injections attack on the MAYO reference implementation
- Identified leaking points for side-channel power analysis
- Reviewed papers internally before submission

Matters | Site reliability engineering intern

Sep 2021 – Feb 2022 | Paris, France

- Managed serverless deployments used by +200 clients including major companies (Vinci, Carrefour, La Poste...)
- Took part in developing a security policy

ViaRézo (student ISP) | Core Team

Sep 2020 – Feb 2021 | Gif-sur-Yvette, France

- Delivered high-speed internet to 2000+ people with a 20 member team
- Managed OpenStack and Ceph deployments with 2000+ instances
- Audited and hardened our internal OAuth2 implementation and password storage scheme

Some projects

Post-quantum cryptographic primitives in Rust | Academic project

Nov 2022 - Present
Contributed and reviewed code for cryptographic primitives

IoT for the LoRa platform | Semester-long university project

Sep 2022 - Feb 2023 | CentraleSupélec, France
Deployed a network of sensors with a focus on security (technologies : LoRa, C...) with a team of five students

Volunteer work

POPL 2024 Student Volunteer

LGBT+ club : Organized a screening day in collaboration with a local hospital
Invited queer artists for an art installation and conference cycle

Tutoring in disadvantaged high-schools

Visiting isolated patients in hospitals

Publications

- *Implementation attacks against MAYO* (in submission)
  T. Aulbach, R. Lachguel, S. Marzougui, J-P. Seifert, V. Ulitzsch