Laz Panard

Ph.D candidate (Nov. 2024) in Lattice-based Cryptography

Centre Inria de l'Université de Rennes, Capsule Team,
Campus de Beaulieu, 263 Avenue Général Leclerc,
35042 Rennes Cedex, France.
☎ *06 79 79 14 47*
✉ *laz.panard@inria.fr*

Internships

May - Oct. 2023 **Intern**, *CAPSULE Team (INRIA)*, Rennes (France), **supervised by Daniel de Almeida Braga, Pierre-Alain Fouque and Aurore Guillevic**
Lattice-based digital signature "FALCON-like" primitives to remove floating-point arithmetic
First implementation of the Zalcon protocol (Fouque et. al, PQC NIST, 2021)
Literature review of state-of-the-art lattice-based cryptography, especially digital signatures, sampling in lattices and Hash-and-Sign signatures

April - July 2023 **IT Intern**, *CyberPeace Institute*, Geneva (Switzerland)
Digital platform "Mattermost" interactions automation
Golang development, post-incident investigation (malicious intrusion), API handling and development

February 2022 **Cybersecurity Analyst Trainee in CSIRT**, *Nickel*, Nantes (France)
Internal phishing campaign : design, technical implementations and operations
Brief review of the mailing security protocols (SPF, DKIM, DMARC)

Education

2021 - 2024 **Engineer's Degree**, *IMT Atlantique*, Nantes & Rennes (France)
Specialisations in Cybersecurity & Digital Platforms

- ○ Introduction to Research: Constraints programming basic solver development and presentation of found results, supervised by Charles Prud'Homme
- ○ Introduction to Cryptology: Symmetric protocols and primitives, hash functions, mathematics for asymmetric cryptography *(discrete logarithm, integer factorisation, elliptic curves)*, asymmetric protocols and primitives *(Diffie-Hellman, RSA, El-Gamal)*, digital signatures *(RSA, El-Gamal, ECDSA)*, PKI infrastructure, **oral presentation of the NIST post-quantum cryptography competition candidate BIKE**
- ○ Network Security: SSL, 802.1X, IPSec, Kaminsky attack for DNS cache poisoning
- ○ Blockchain & Consensus: Review of *Byzantine Generalized Lattice Agreement*, an article about distributed systems consensus
- ○ Half-year Project: Redaction of a recommendation guide oriented towards theoretical security models, imputability and IAM good practice for the Brest (France) hospital

2023 - 2024 **M2 Computer Science**, *EUR "CyberSchool", Université de Rennes*, Rennes (France)
Double Degree Agreement. UE "SIMP" - Side channel analysis & API Security for Hardware

- ○ Side-channel analysis: *Chip whisperer* practical work
- ○ Hardware API Security: Analysis and penetration of a Raspberry tool for symmetric key storage and handling

2019 - 2021 **Preparatory Classes for Grandes Ecoles ("CPGE")**, *Kléber High School*, Strasbourg (France)

MPSI then MP*, computer science option

- TIPE: A Python implementation of the Hungarian algorithm, proof and measure of performance
- Mathematics & Physics Major
- Computer science fundamentals and discovery of OCaml

Technical Skills

Languages	Python, SageMath, Java, LaTeX, C, Golang, SQL, OCaml, Bash, R, HTML/CSS/JS
OS & Systems	Linux/UNIX, Openstack & Kubernetes, network configuration, web server setup
Cyber. Law	NIS directives, GDPR, contract law, fundamentals of regulations

Soft Skills

Languages	French (Native), English (C1, IELTS 8.0/9.0), Spanish (B1)
Oral Fluency	Prior experience in improv theatre (4 years), associative work as chairman of general meetings, various oral presentations (mandatory and optional) through secondary and superior education
Teamwork	Associative experience (4 years): 2024 Rennes TFJM^2 edition, secretary and logistic manager for a student congress (200 people); a dozen group projects carried out throughout my education
Autonomy	Internships projects carried out in partial to full autonomy, personal and academic projects (including research projects, archiving work, events organisation, etc.)

References

Team Leader	**Pierre-Alain Fouque**, Professor at Rennes University, Head of CAPSULE Team, mail
Lab Supervisor	**Aurore Guillevic**, INRIA Researcher, Member of CAPSULE Team, mail
Former Professor	**Guillaume Doyen**, Professor at IMT Atlantique, Head of SOTERN Team, mail