YANN AGUETTAZ

Computer Scienctist & Engineer

@ yann@aguettaz.me   📞 (+33)6 51 00 01 70   🌐 yann.aguettaz.me   yann-a   in Yann Aguettaz

EDUCATION

Master's in Computer Science & Cyber Security
Ecole Polytechnique Fédérale de Lausanne (EPFL)

📅 2021 – 2023   📍 Lausanne, Switzerland

Topics : Cryptography, Software Security, Information Security, Security Protocols, Privacy-Enhancing Technologies, Formal verification, TCP/IP Networking, Hardware Compilation, Distributed Algorithms, Database Systems, Natural Language Processing

Projects : Formal Verification: Tableau prover. Master's Thesis: Post-quantum cryptanalysis.

Master's & Bachelor's in Computer Science
École Normale Supérieure (ENS) de Lyon

📅 2019 – 2023   📍 Lyon, France

Topics : Cryptography, Information Theory, Quantum Information and Computation, Performance Evaluation, Compilers and Program Analysis, Theoretical Computer Science, Programming languages theory, Logic, Computer Architecture and Systems, Advanced Algorithms, Computational Geometry, Parallel and Distributed Algorithms, Distributed Systems, Optimization and Approximation, Machine Learning, Computational Complexity, Databases and Data Mining, Algebra, Probabilities

Programming projects :
Mini-projects in C / C++ / Ocaml / Python / Haskell / Erlang, Competitive programming (ACM-like), OCaml interpreter in Ocaml and π-calculus interpreter in Go Group project with 10 other students : Rework and enhance a platform used at ENS to teach programming to first year students.

EXTRACURICULAR

Volunteer at ENSeigner (2019 – 2022)

    Tutoring for underprivileged high-school students in mathematics.

System Administrator at AliENS (2020 – 2024)

    Student association for the promotion and development of free software. Proposes technical support and online services to students.

Secretary at BuL (2020 – 2021)

    Organization of events on and off campus for 100+ students. Administrative handling of the association.

CONTESTS

2021&22	ICPC's SWERC	$31^{th}/97$
2021	TRACS (Intelligence contest by DGSE)	$5^{th}/94$
2020	Brigitte Friang (CTF by DGSE)	6th
2020&21	Prologin (French algorithmics contest)	Finalist
2020&21	Participation to Google's CodeJam & Hashcode and other various programming contests and CTFs	

INTERESTS & SKILLS

Computer Science

Cryptography, Cybersecurity, Privacy, Formal Verification, Quantum computation, Information Theory, Compilation

Other interests

Diffusion of knowledge, Politics, Linguistics

Language

French (Native)
English : C2 *(Cambridge Advanced at grade A)*
German : B1 level *(Deutsches Sprachdiplom)*

Technical Skills

Python, Ocaml, C, C++, Scala, Rust, Go
Web : HTML/CSS, PHP, SQL, Javascript, Flask
Tools : Git, LaTeX, Bash, Linux
Sys Admin : Nginx, Docker, Ansible

EXPERIENCE

Research Internship
École Normale Supérieure

📅 2023 (6 months)   📍 Paris, France

Cryptanalysis of multivariate post-quantum signature schemes.

Research Internship
Huawei

📅 2022 (6 months)   📍 Paris, France

Anonymous communication protocols on the internet at the network layer.

Research Internship
UCLouvain

📅 May – July 2021   📍 Louvain-la-Neuve, Belgium

Side-Channel Analysis of an AES protected implementation and countermeasures assessment

Research Internship
VeriQloud

📅 June – July 2020   📍 Paris, France

Quantum protocols for secured multiparty computation. Definition of quantum protocols for SMPC and comparison with classical ones.