Guilhem Niot

Github:// GuilhemN LinkedIn:// Guilhem Niot
+33 6 40 40 34 29 | guilhem@gniot.fr

SKILLS

PROGRAMMING
C++/C • Python • Golang • Rust • Java • JavaScript • PHP

HARD SKILLS
Cryptography • Cyber Security • Decentralized Systems • Pen-testing • Reverse Engineering • Software Security • Software Development

ADDITIONAL SKILLS
Teamwork • Empathy • Open-mindedness • Open-source

PROJECTS

- Dolphin: a decentralized and secure bill-sharing app. CRDTs for managing distributed data, and TreeKEM for **Group Key Management** and key rotations. *Tech:* Golang.
- Saccha: dog model for training veterinary students on heart murmurs. Team of 4 students. *Tech:* Electron JS, Raspberry Pi.
- Pingo: a π-calculus interpreter in Go.
- ... and more on my Portfolio.

CONTESTS

- Google Hash Code: top 15% in 2020 & 2021 & 2022
- TRACS: A hacking contest by the DGSE (France secret services). **5th/90** in 2021, **2nd/90** in 2019.
- BattleDev: Programming contest. **18th/10000+**.

VOLUNTARY ACTIVITIES

- 2020 - 2022: Vice-president of AliENS, the IT association of ENS de Lyon (600 members). Sysadmin, programming, events organization.

OTHER

LANGUAGES
English — Proficient (C1 Advanced)
French — Native

HOBBIES
Climbing, Cooking, Hiking

EDUCATION

EPFL, LAUSANNE | Switzerland
Master in Computer Science, Minor in Cyber Security
09/2021 - Graduation 09/2023 GPA: 5.76/6

ENS DE LYON | France
BS and MS in Computer Science
09/2019 - Graduation 09/2023 GPA: 17.75/20

EXPERIENCE

PQSHIELD
Oct. 2023 - Present | Paris | PhD student
Constructions and protocols based on lattices.

Feb. 2023 - Aug. 2023 | Tokyo, and Paris | Cryptography Research Intern
Submission to NIST of Squirrels [1], a practical digital signature scheme based on unstructured lattices. Achieves signature size **between the two NIST finalists** based on lattices, Falcon and Dilithium. Attended Eurocrypt and RWC 2023.

ADOBE RESEARCH | Software Security Intern
Aug. 2022 - Jan. 2023 | Basel, Switzerland
Work with the security team of Adobe Experience Manager.
- Refactor and speed up **OAuth authentication** in AEM. Make it multi tenant.
- Pen-testing: report and fix of **critical vulnerabilities**. Threat modeling.

Tech: Fastly, Kubernetes, Envoy, Java, Golang, VCL

LASEC LABORATORY, EPFL | Cryptography Research project
Feb. 2022 - Jul. 2022 | Lausanne, Switzerland
Optimization of Post-Quantum cryptography in TLS 1.3 handshake. Asynchronous computations using a KEM adapted from SIKE to reduce handshake latency. *Tech:* Rust, C, Python, Mininet.

SACS LABORATORY, EPFL | Student Intern
April. 2021 - Jul. 2021 | Lausanne, Switzerland
Research and improvement of an approximation technique for KNN applications based on Jaccard similarity [2]. Up to **79% speed improvement** over previous state-of-the-art for same accuracy. *Tech:* Java, C, Python.

LABRI, CNRS | Confidential Computing Intern
Jun. 2020 - Jul. 2020 | Bordeaux, France
Experience with **Intel SGX** to build a proxy anonymizing requests to a recommendation app. **Scalability**, and **unlinkability** properties. *Tech:* C, C++.

OPEN-SOURCE | Open Source Contributor and Maintainer
2015 – Present
Lead Maintainer of NelmioApiDocBundle - a **2k stars** library.
Member of several open-source organizations, regular open-source contributor.

PUBLICATIONS

[1] Espitau, T., Niot, G., Chao, S., and Tibouchi, M. Squirrels: An efficient and secure post-quantum signature scheme based on plain lattices. Tech. rep., National Institute of Standards and Technology, 2023.

[2] Guerraoui, R., Kermarrec, A.-M., Niot, G., Ruas, O., and Taïani, F. GoldFinger: Fast & Approximate Jaccard for Efficient KNN Graph Constructions. *Transactions on Knowledge and Data Engineering* (2022).