

GUILHEM NIOT

guilhem@gniot.fr | gniot.fr | Github:// [GuilhemN](#) | LinkedIn:// [guilhem-niot](#)

EDUCATION

PQShield & Université de Rennes | PhD in Cryptography | Paris, France 2023 - present

EPFL | Master in Computer Science, Minor in Cyber Security | Lausanne, Switzerland 2021 - 2023
GPA 5.76/6

ENS Lyon | BSc and MSc in Computer Science | Lyon, France 2019 - 2023
GPA 17.75/20

EXPERIENCE

PQShield | Cryptography Researcher | Paris, France Nov 2023 - present

- Conducting cutting-edge research on post-quantum cryptography with team of 10 senior researchers internationally, focusing on design and analysis of lattice-based primitives and protocols.
- 1 publication [1] at CRYPTO 2024 and 4 ongoing research projects (one single-authored work).
- Collaborating with researchers internationally.

PQShield | Research Intern | Tokyo, Japan Feb - Aug 2023

- Investigated side-channel countermeasures, and design of a scheme published at EUROCRYPT [2].
- Wrote a signature scheme NIST submission [3] with conservative security, and small size ~1kB.

Adobe Research | Software Security Intern | Basel, Switzerland Aug - Dec 2022

- Conducted penetration testing that uncovered over 10 security vulnerabilities, including 3 critical and 5 major issues.
- Initiated major refactor in OAuth authentication of AEM. Work in environment of >200 engineers.

LASEC Lab, EPFL | Research project | Lausanne, Switzerland Feb - Jul 2022

- Optimized Post-Quantum cryptography in TLS 1.3 handshake. Over **50% reduction** of cryptography cost of modified CSIDH.
- Integrated asynchronous computations using a KEM adapted from SIKE to reduce handshake latency.

SaCS Lab, EPFL | Student intern | Lausanne, Switzerland Apr - Jul 2021

- Researched an approximation technique for KNN applications based on Jaccard similarity [4].
- Up to 79% speed improvement over previous state-of-the-art for same accuracy.

LaBRI, CNRS | Student intern | Bordeaux, France Jun - Jul 2020

- Experimented with Intel SGX to build a proxy anonymizing requests to a recommendation app. Two proposed designs. Scalability, and unlinkability properties.

LANGUAGES

English: **fluent** (C1 CAE Advanced)

French: **native**

SKILLS

Programming: **C++/C** • **Python** • **Golang** • **Rust** • **Java** • **JavaScript** • **PHP**

Tools: **Kubernetes**, **Docker**

PUBLICATIONS

[1] **Flood and Submerge: Distributed Key Generation and Robust Threshold Signature from Lattices** With T. Espitau, T. Prest. *CRYPTO*, 2024.

[2] **Plover: Masking-Friendly Hash-and-Sign Lattice Signatures**. With M. Esgin, T. Espitau, T. Prest, A. Sakzad, R. Steinfeld. *EUROCRYPT*, 2024.

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

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

Writing in progress: threshold primitives, secure messaging, key exchange.

OTHER PROJECTS

- Open-source: various contributions, founder of [NelmioApiDocBundle](#), 2k stars project.
 - CTFs: TRACS, Brigitte Friang challenge; programming contests: SWERC, Google Hash Code, etc.
 - Vice-president of AliENS, the IT association of ENS de Lyon (600 members) from 2020 until 2022.
 - Random personal projects:
 - [Saccha](#): dog training model for veterinary students
 - [Mixed Feelings](#): game developed in 24h during the Orbital Game Jam 2022 at EPFL.
 - Dolphin: a toy decentralized bill-sharing app. CRDTs for managing distributed data, and TreeKEM for Group Key Management and key rotations.
 - [Pingo](#): a π -calculus interpreter in Go.
 - [Modelling of impact of Covid tracing apps](#). Presented in a commission of French assembly.
-

TALKS

- *Flood and Submerge: Distributed Key Generation and Robust Threshold Signature from Lattices*, ENSL/CWI/KCL/IRISA joint crypto seminar (30/09/2024)
- *Flood and Submerge: Distributed Key Generation and Robust Threshold Signature from Lattices*, CRYPTO 2024 (08/2024)
- *Plover: Masking-Friendly Hash-and-Sign Lattice Signature*, EUROCRYPT 2024 (05/2024)
- *Plover: Masking-Friendly Hash-and-Sign Lattice Signature*, CAPSLOCK Seminar Rennes (04/2024)
- *Squirrels: a post-quantum signature scheme based on plain lattices*, Journées C2 (10/2023)