JACOB PRUD'HOMME

jacobprudhomme
jacob.prudhomme@epfl.ch
Zürich, Switzerland
jacob-prudhomme
jacobprudhom.me

SELECTED WORK EXPERIENCE

Junior Software Engineer — Mission Control Space Services
Feb 2022 – Sept 2024 — Ottawa, Canada

- Laid groundwork for embedded software project on European Space Agency OPS-SAT "orbital laboratory" satellite, leveraging an Intel Cyclone V SoC
- Managed framework for collecting data for satellite position determination, to be used in machine learning models
- Integrated flagship mission control software with various robotics backends to meet time-critical mission/project requirements for a variety of stake-holders

Software Developer (Cybersecurity) — Crypto4A
Sept 2020 – Dec 2020 — Ottawa, Canada

- Led design and implementation of Vue.js visualization frontend and Kotlin app for an M-of-N access control system
- Helped attain FIPS 140-2 security compliance by contributing to ACVP cryptographic testing framework
- Maintained and improved core services written in C running on flagship quantum-safe "datacentre-in-a-box"

Secure Software Developer — ESCRYPT
May 2019 – Aug 2019 — Waterloo, Canada

- Researched SCMS, a novel PKI-like system for securing V2X (vehicle-to-everything) communications
- Ensured network security by configuring virtual network and reverse proxy, restricting endpoint access to only routers on-board vehicles
- Maintained and improved on-vehicle cryptography SDK in C++

SELECTED ACADEMIC EXPERIENCE

Semester Research Project Student
Project title: Implementation of pSIDH

LASEC – Cryptography and Security Lab

Supervisor: Laurane Marco

Spring Semester 2023 — EPFL, Switzerland

- Developed reference implementation in SAGE of pSIDH, an isogeny-based post-quantum key exchange protocol, based on the Deuring correspondence between isogenies of supersingular elliptic curves and ideals of a special type of subring in a quaternion algebra
- Based on PhD thesis and follow-up preprint *A New Isogeny Representation and Applications to Cryptography* [Antonin Leroux]

Paper Study and Seminar Presentation
CSIDH: An Efficient Post-Quantum Commutative Group Action [Wouter Castryck et al.]

Course – Student Seminar: Security Protocols and Applications

Mentor: Tako Boris Fouotsa

Spring Semester 2023 — EPFL, Switzerland

- Along with mentor guidance, delivered a comprehensive seminar on CSIDH, an isogeny-based post-quantum key exchange algorithm, distilling complex theoretical concepts into intuitive explanations for an audience with only general knowledge of cryptography

OTHER EXPERIENCE

Undergrad Research Assistant – C∀
PLG – programming languages lab

Spring Sem. 2021 — University of Waterloo

Software Engineering Intern
SigOpt (acquired by Intel)

Q1 2020 — San Francisco, USA

Full-Stack Developer
360insights

Q1 + Q4 2018 — Whitby, Canada

Web Applications Developer
Blindside Networks

Q3 2017 — Ottawa, Canada

EDUCATION

MSc in Cyber Security
EPFL + ETH Zürich [Joint Degree]

Sept 2022 – present

Bachelor of Computer Science
Minor in Combinatorics & Optimization

University of Waterloo

Sept 2016 – Aug 2021

RELEVANT COURSES

- **EPFL** – Cryptography & Security (COM-401)
- **EPFL** – Advanced Cryptography (COM-501)
- **EPFL** – Number Theory in Cryptography (MATH-489)

SKILLS

Proficient: C | Javascript / Typescript | Python | SAGE | HTML | CSS+variants

Comfortable: C++ | Java | Scala | PHP

Tools and Frameworks: Bash | Git | Docker | React | Vue.js | Svelte

LANGUAGES

English Native
French Native
Italian Beginner