

# 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 stakeholders

**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

**Implementation of pSIDH**

*Semester Research Project*

**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]

**CSIDH: An Efficient Post-Quantum Commutative Group Action** [Wouter Castryck et al.]

*Paper Study and Seminar Presentation*

**LASEC – Cryptography and Security Lab**

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

## EDUCATION

**MSc in Cyber Security**

**Joint Degree – EPFL and ETH Zürich**

📅 Sept 2022 – present

**Bachelor of Computer Science**

**Minor in Combinatorics & Optimization**

**University of Waterloo**

📅 Sept 2016 – Aug 2021

## MORE EXPERIENCE

**Undergrad Research Assistant – CV**

**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

## SKILLS

**Proficient:** C Javascript / Typescript

Python SAGE HTML CSS+variants

**Comfortable:** Rust C++ Java Scala

**Tools and Frameworks:** Bash Git

Docker React Vue.js Svelte

## RELEVANT COURSES

- **EPFL** – Cryptography & Security
- **EPFL** – Advanced Cryptography
- **EPFL** – Number Theory in Cryptography
- **EPFL** – Quantum Information Processing
- **EPFL** – Quantum Computation
- **ETHZ** – Network Security

## LANGUAGES

🇬🇧 **English** Native  
🇫🇷 **French** Native  
🇮🇹 **Italian** Beginner