

JÉRÉMI DO DINH

jdodinh.io | [jdodinh](https://github.com/jdodinh) | [jdodinh](https://www.linkedin.com/in/jdodinh) | jeremi.dodinh@gmail.com

I'm a cryptographic engineer specializing in Rust-based tooling for zero-knowledge proof systems. I earned my MSc at EPFL, where I worked with Alessandro Chiesa and Giacomo Fenzi on proof systems and zero-knowledge arguments. I currently work at Ligerio, where I build cryptographic infrastructure for privacy-preserving protocols.

My focus is on deepening my expertise in Rust-based cryptographic engineering, with the goal of taking on increasingly complex systems and technical leadership over the coming years.

EXPERIENCE

Cryptographic Engineer at Ligerio

June 2025 - *present*

- Started as an intern in June 2025, converted to full-time contract in September 2025.
- Built a packed secret sharing library accelerating BN254 polynomial evaluation via CRT decomposition into NTT-friendly primes, custom Montgomery arithmetic with optional AVX2 SIMD vectorization, and multi-level parallelism, achieving up to 24% speedup on 128-core cloud instances.
- Building Rust-based cryptographic tooling for Ligetron, with C++ interop via CXX.
- Led the development of the documentation site alongside the research team, including interactive concrete security analysis tooling.
- Building a Rust verifier targeting Risc0's ZKVM, with EC2-based benchmarking infrastructure.
- Active in the development of new features for Ligetron and the SDK.

Post Graduation Projects

October 2024 - June 2025

- Reimplementing and optimizing the STIR protocol with a benchmarking suite.
- Contributing to Plonky3 implementation of WHIR.
- Building a BitTorrent client (CodeCrafters).
- Implementation of the sum-check protocol from scratch.

Freelancing

December 2024 - *present*

- Automating accounting/reporting tasks using Python and Excel for small businesses.

Java Software Engineering Intern at SonarSource

September 2023 - February 2024

- Contributed to the development and maintenance of new and existing features for Python analysis, operating within a Scrum framework.
- Gained experience in test-driven development methodologies, ensuring high-quality software deliverables.

Software Developer at RailVision Analytics

September 2020 - June 2021

- Close work with core server architecture and APIs used in the data processing pipeline.
- Key role in the migration to AWS.

Teaching & Tutoring

September 2019 - June 2023

- Regular appointments as a teaching assistant at McGill and EPFL.
- Certified kitesurfing instructor (*IKO*), with experience teaching in Sicily.


Summer internship at CN Rail

May 2019 - August 2019

- Contributed to the winning team of the I&T Business Case competition, targeted at developing a technology-based business solution for CN. Received C\$1200 scholarship as part of the winnings.

EDUCATION

EPFL - MSc in Computer Science

- Thesis: “*Simulation Security in the Random Oracle Model*” – [PDF](#) 
- Supervised by Alessandro Chiesa and Giacomo Fenzi.

September 2021 - August 2024

(GPA: 5.25/6.0)

McGill University - BSc in Mathematics & Computer Science

- Minor in Musical Science & Technology.
- Exchange semester at UBC Vancouver (January-April 2020).

September 2017 - April 2021


(GPA: 3.87/4.0)

RESEARCH & PUBLICATIONS

Tight inapproximability of well-supported Nash equilibria in public goods games 2023



- with Alexandros Hollender – [ipl.2024.106486](#)  [arXiv:2402.14198](#) 

- Obtained hardness results for computing approximate equilibrium points in public goods games, significantly improving the previous upper bound. Completed at [THL5](#), [EPFL](#).

Integer Programming with Complete Constraint Matrices [Report](#)  2022

- Investigated properties of integer vectors ($b \in \mathbb{N}^m$) and their relation to the existence of a solution x on the binary hypercube such that $Ax = b$, where the constraint matrix $A \in \{0, 1\}^{m \times 2^m}$ is *complete*.
- Master’s Semester Project Supervised by Alexandra Lassota, [DISOPT](#), [EPFL](#).

ACADEMIC PROJECTS

BobbyChain: Smart Contracts using PoW and pBFT [Report](#)  - [Presentation](#)  2022

- Implemented an array of functionalities of “*Peerster*”, a gossip-based peer-to-peer application.
- Built smart contracts on top of a generic consensus interface, along with two consensus algorithms, which can be used interchangeably: Proof-of-Work and practical Byzantine Fault Tolerance.
- Completed as part of the *Decentralized Systems Engineering* course at EPFL.

Broadcast Algorithms [Course](#)  2021

- Implemented in Java the necessary building blocks for a functioning distributed system including *Perfect Links*, *FIFO Broadcast* and *Localized Causal Broadcast*.
- Completed as part of the *Distributed Algorithms* course at EPFL.

ML For Science: Mouse Action Segmentation [Repository](#)  - [Course](#)  2021

- Trained models able to identify behavior of mice, based on videos annotated by experts.
- Focused on the feature engineering aspect of the project.
- Completed as part of the *Machine Learning* course at EPFL.

FingerSynth [Repository](#)  - [Demo](#)  2021

- Developed a C++ based synthesizer (using [STK](#)) that can be played with the use of the trackpad.

SKILLS AND INTERESTS

Technologies Rust, C/C++, Java, Python, Go, Git, L^AT_EX, Bash.

Languages *Fluent*: English, French and Polish. *Learning*: German and Italian.

Interests Theory of Computation, Software Development, Zero-Knowledge, Probabilistic Proof Systems, Music, Kitesurfing, Skiing.