

# ADRIAN HAMELINK

† 14.09.1996   @ adrian@hamelink.com   ☎ +41 (0) 79 961 24 10   📍 Rue Couchirard 13, 1004 Lausanne, Switzerland  
🌐 adrianhamelink.com   🐦 @adr1anh   🔗 adrianhamelink   📄 adr1anh

## PROFESSIONAL EXPERIENCE

### s Research Intern (50%) **Taurus SA**

📅 September 2020 – current   📍 Lausanne, Switzerland

- self-motivated research in various cryptographic topics.
- quickly learn and reason about new mathematical concepts.
- assisting in audits of popular cryptographic libraries.

### Software Development Intern **MindMaze**

📅 July 2018   📍 Lausanne, Switzerland

Over the course of one month, I developed a C library for real-time analysis of heart-rate signals. Operating under a tight time constraint taught me how to better focus my efforts, while simultaneously adapting to a new workspace.

## PROJECTS

### Open-Source implementation of FROST-Ed25519

**Taurus SA (2021)**

A Go implementation of the FROST protocol by Komlo & al. for threshold Ed25519 signature generation.

### A Survey of Threshold ECDSA Signing

**Joint work with J-P. Aumasson (Taurus) and O. Shlomovits (ZenGo)**

A brief overview of various ECDSA threshold signature schemes published between 2018 and 2020.

### Impossibility of superlogarithmic isogeny evaluation

**Master's semester project (Spring 2020)**

Using algebraic complexity theory in an attempt to prove that fast isogeny evaluation implies  $P = NP$ .

### Implementation and Profiling of the Wesolowski VDF

**Bachelor's project (Spring 2019)**

Developed and assessed the performance of the Verifiable Delay Function construction by B. Wesolowski, in C using GMP.

### Various school projects

- Design and implementation of P2P protocol **GoLang** 2020
- Creation of Deep Learning framework **Python** 2020
- Implementation of broadcast algorithms **C** 2019
- Physical simulation with 3D visualization **C++** 2016
- Creation and publication of iOS game **Objective-C** 2015

## EDUCATION

### Master's in Communication Systems

**Ecole Polytechnique Fédérale de Lausanne**

📅 2019 – current   📍 Lausanne, Switzerland

### Bachelor's in Mathematics

**Ecole Polytechnique Fédérale de Lausanne**

📅 2015 – 2019   📍 Lausanne, Switzerland

### Maturité Gymnasiale

**Collège Calvin**

📅 2011 – 2015   📍 Geneva, Switzerland

## SKILLS

- Implementing cryptographic primitives.
- Auditing cryptographic projects.
- 

### Programming Languages

C/C++   Go   Python   LaTeX

### Research and interests

Threshold cryptography   zkSNARKs  
MPC   Blockchain   Isogenies

## LANGUAGES

English   ● ● ● ● ●  
French   ● ● ● ● ●  
German   ● ● ● ● ●  
Dutch   ● ● ● ● ●

## HOBBIES

- Sports: Roller Blading, Swimming
- Cooking
- Travelling