Yolan **Romailler**

APPLIED CRYPTOGRAPHY & SECURITY ENGINEER

Lausanne, Vaud, Switzerland

☎ upon request | ✉ yolan@romailler.ch | ⌂ romailler.ch | Lery | @AnomalRoil

Experience

drand, Protocol Labs
Remote

DISTRIBUTED SYSTEMS ENGINEER
Feb. 2022 – present

- **Tech lead** and applied cryptographer on the distributed randomness team (drand).
- Enabling the League of Entropy, a permissioned network based on threshold BLS signatures and Pedersen Distributed Key Generation.
- Pairing-based cryptography & **timelock encryption** research and implementations.
- **Security Expert** for the wider ecosystem (Filecoin Foundation, Lotus, NetOps).
- Interviewer for SWE and Security roles, for culture and technical interviews.

Digital Lab, SICPA
Prilly, Switzerland

PRINCIPAL CRYPTOGRAPHER
May 2021 – Jan. 2022

- **Self-Sovereign Identity**: DIDs, DIDComm, authenticated key exchanges and encrypted transport.
- Subject Matter Expert on everything cryptography within SICPA R&D teams.
- **CBDC** design: building blocks, protocols & architecture.
- Secure coding & cryptography awareness.

Novi Financial, Facebook
Remote

CONTINGENT WORKER (CONTRACT, EXTENDED)
Sep. 2020 – Apr. 2021

- **Libra Core** security team: providing threat modeling, code review and design services to 200+ developers.
- Implementation of verifying APIs and client relying on EdDSA signatures in Rust.
- **Dedicated Security Partner** for the Ecosystem layer (custody, SDKs, smart contracts).
- Hash-based integer range proofs & micro-payments systems.

Fundamental Research, Kudelski Security
Cheseaux-sur-Lausanne, Switzerland

SENIOR SECURITY RESEARCHER
Sep. 2016 – Apr. 2021

- **Vulnerability research**, fault attacks, side-channels.
- **Cryptography** R&D (signature schemes, elliptic curves, functional encryption, ...)
- Presenting our research in conferences and publishing our results appropriately.
- Worked on VoIP, Messaging, Blockchain technologies, e-voting, hardware-software co-design and more.
- Secure coding consultancy (implementations of core cryptographic primitives and protocols, **code audits** and design reviews).
- Started as a trainee, promoted to Researcher on 2017-03-01, promoted to **Senior** on 2018-11-01.

Skills

Programming	Go, C++, Rust, LaTeX, Git & Continuous Integration
Code reading	C, Python, Scala, Java & JS
Languages	French: native ; German and English: fluent ; Japanese: beginner

Conferences

Non-exhaustive list. See my website.

Real World Crypto
Tokyo, Japan

TLOCK: PRACTICAL TIMELOCK ENCRYPTION BASED ON THRESHOLD BLS
Mar. 2023

- Talk explaining how we built the first practical timed release encryption system using Identity-Based Encryption and threshold BLS.
- Published our full paper on ePrint.

DEF CON 30
Las Vegas, USA

A DEAD MAN'S FULL-YET-RESPONSIBLE-DISCLOSURE SYSTEM
Aug. 2022

- Explaining how one can leverage timelock encryption to perform responsible disclosure.
- Released our code and web-demo as open-source software.

GopherCon EU
Online

TAKING THE (QUANTUM) LEAP WITH GO
May 2021

- Explaining how post-quantum cryptography will soon be required and what are the most likely algorithms we'll be using.
- Released our open-source code implementing these algorithms in pure Go.

DEF CON 26 — *Las Vegas, USA*

REAPING AND BREAKING KEYS AT SCALE: WHEN CRYPTO MEETS BIG DATA — *Aug. 2018*

- Talk available online explaining how RSA public keys are still vulnerable to batch GCD, and how to do it at scale.

Fault Diagnosis and Tolerance in Cryptography, FDTC — *Taipei, Taiwan*

PRACTICAL FAULT ATTACK AGAINST THE ED25519 AND EDDSA SIGNATURE SCHEMES — *Sep. 2017*

- Accepted paper & talk introducing the **first fault attack against EdDSA**, along with a novel infective countermeasure.
- FDTC is a peer-reviewed workshop collocated with CHES.

Black Hat USA 2017 — *Las Vegas, USA*

AUTOMATED TESTING OF CRYPTO SOFTWARE USING DIFFERENTIAL FUZZING — *Jul. 2017*

- Talk & whitepaper introducing a new open source software (CDF) implementing the novel “differential fuzzing”, in Go.
- Explained the bugs discovered on the high-profile, widely used crypto software components tested.

Patents

2020	**Systems and methods for registering or authenticating a user with a relying party**,	*EP4012970A1*
2019	**Incremental assessment of integer datasets**,	*EP3821563B1*
2018	**Fault attacks counter-measures for EdDSA**,	*US20190089543A1*

Education

HES-SO (Haute École Spécialisée de Suisse Occidentale) — *Lausanne, Switzerland*

MSC. IN ENGINEERING ICT (INFORMATION AND COMMUNICATION TECHNOLOGIES) — *Feb. 2017*

- Specialization in Enterprise Networks and IT Security
- Semester project on the **Yao Garbled Circuits**
- Master Thesis on “**Automated Cryptographic Testing**”

EPFL (École Polytechnique Fédérale de Lausanne) — *Lausanne, Switzerland*

BSC. IN MATHEMATICS — *Jun. 2015*

- Semester project developing an **Automated Symbolic Coefficients Resolver** in Python
- Bachelor Project on the **latest DLP algorithm** by A. Joux
- Mean grade in last year: 5.0/6.0

Kantonsschule Frauenfeld — *Frauenfeld, Switzerland*

MATURITÉ BILINGUE (BILINGUAL FRENCH-GERMAN) — *Jul. 2010*

CTF Contests

INSOMNI’HACK, Y-NOT-CTF, PLAID CTF, GOOGLE CTF — *—*

DUKS TEAM MEMBER — *2016–2019*

- Gained experience in hacking and teamwork.
- Won Google CTF **500$ award** for one of my write-ups of Google CTF 2018.
- Scored **2nd** in 2016, **1st** in 2017 and 3rd in 2018 at Y-NOT-CTF in Yverdon.
- Scored 8th (**1st swiss team**) in 2017 and 17th in 2018 at INSOMNI’HACK in Geneva. (Top 10%)
- Scored 39th at Plaid CTF 2017, done in remote. (Top 10%)
- Scored 38th at Google CTF 2017, done in remote. (Top 10%)

HELVETIC CODING CONTEST — *Lausanne, Switzerland*

XENOCORE TEAM MEMBER — *2011 – 2013*

- Gained expertise in algorithm design and coding (done in C++.
- Participated in three editions and won a prize on our second participation.

Hobbies & Extracurricular Activities

PolyJapan (Student Association of the EPFL supporting Japanese culture) — *Lausanne, Switzerland*

COMMITTEE MEMBER — *Sep. 2013 – Mar. 2020*

- Organized 7 editions of JAPAN IMPACT, the biggest Swiss convention about Japanese culture, with over 8000 visitors.
- Managed for 1 year the treasury as part of the presidency team of the PolyJapan commission, with a total turnover between 120k and 240k$.
- Managed for 4 year JAPAN IMPACT’s custom ticketing system.
- Managed for 2 years the marketing and promotion of JAPAN IMPACT.
- Gained knowledge in several business fields such as management, strategy, finance and marketing.
- Gained expertise in **team management**, as one of 25 committee members coordinating over 150 staff members.

Sports	Climbing, Bouldering, Kite-surfing, Skiing (authorized J+S instructor)
Other	Board games, Chess, Go (the strategy game), Books, Sysadmin of my homelab

Published work

Non-exhaustive list

tlock: Practical timelock encryption based on threshold BLS

Real World Crypto *2023-02-13*

- Accepted talk at Real World Crypto 2023, available on ePrint with open-source implementation in **Go**.
- In which we present a practical instantiation of timelock encryption relying on **Identity-Based Encryption** and threshold BLS.

HashWires: Hyperefficient Credential-Based Range Proofs

Privacy Enhancing Technologies Symposium (PETS) *2021-03-07*

- Accepted paper at PETS 2021, available on ePrint with open-source implementation in **Rust**.
- In which we introduced "credential-based" (almost zero-knowledge) quantum-resistant range proofs based on hashing.

The definitive guide to "Modulo Bias and how to avoid it"

Kudelski Security Research Blog *2020-07-28*

- Posted on Kudelski Security's Research Blog.
- In this piece, I explain what a Modulo Bias is, and how it can lead to a full private key recovery in Schnorr-like signature schemes.
- I also present 3 different ways to avoid Modulo Bias in your codebase.

Boxcryptor Security Audit

Secomba GmbH *2020-06-24*

- Public code audit of the "Boxcryptor" closed-source software in **C#**.
- Found 3 potential security issues & 6 observations related to general code safety.

ZCash Sapling Update Security Audit

ZCash *2019-01-30*

- Public security audit of the "Sapling Update" of ZCash in **Rust**.
- Found 2 potential security issues related to the "pairing" component.
- Found 3 potential security issues related to the "Bellman" component.

Bulletproofs Security Audit

Monero *2018-07-23*

- Public code audit of the **Bulletproof** implementation made by Monero in **C++**.
- Found 3 potential security issues & 8 observations related to general code safety.

Breaking RSA OAEP with Manger's attack

Kudelski Security Research Blog *2018-04-05*

- Posted on Kudelski Security's Research Blog.
- In this piece, I explain how Manger's attack work and how to implement it in **Go**.

"Testons votre crypto"

Multi-System & Internet Security Cookbook, MISC *Apr. 2018*

- Article for the french IT-Sec magazine MISC.
- Introduced the ways one can test their crypto implementations using automated tools such as CDF or Wycheproof.

Wire Security Review of Android Client

Wire GmbH *2018-03-07*

- Public code audit of the Wire Android client application in **Scala**.
- Wire wanted a security assessment of their client, which is also a security-critical component of their messaging application.

Ethereum Classic Client (Mantis) & Icarus Wallet Security Audits

IOHK *2018-01-26 & 2018-10-17*

- Public code audit of the "Mantis" Ethereum Classic wallet in **Scala**.
- Found 7 potential security issues of medium severity & 5 observations related to general code safety.
- Public code audit of the "Icarus" Cardano wallet in **Rust**.
- Found 3 potential security issues of low severity & 11 observations related to general code safety.

Answer to "Constructing Garbled Circuits"

Crypto StackExchange *2017-06-08*

- Answered on the Cryptography StackExchange website.
- In this answer, I describe how Yao's garbled circuits work and how they can be constructed.
- Figures contributed to the TikZ for Cryptographers website.

How (not) to break your (EC)DSA

Kudelski Security Research Blog *2017-04-10*

- Posted on Kudelski Security's Research Blog.
- In this piece, I mostly discuss the DSA and ECDSA algorithms and their respective domains and parameters.