MATHILDE RAYNAL

PhD Candidate, Security and Privacy

mathilde.raynal@epfl.ch
github.com/PizzaWhisperer
/scholar/mathilde.raynal
/in/mathilde-raynal

EDUCATION

PhD - *SPRING Lab, EPFL* **2021 - Present**
Supervised by Prof. Carmela Troncoso within the SPRING Lab. Research interests include privacy, machine learning, applied cryptography, and thinking about how adversaries can subvert systems, with the unified objective of understanding the impact of AI-based technologies on society.

Joint MSc in Cybersecurity (GPA: 5.41/6) - *EPFL & ETHZ* **2018 - 2021**
Master Thesis: Side-Channel resilient implementation of NIST post-quantum cryptography candidates. Integration of PQC in OTR and WireGuard protocols. **Awarded the Kudelski jury prize for significant contributions to the field of cryptography**.

BSc in Communication Systems - *EPFL* **2015 - 2018**

EXPERIENCE

R&D Intern - *Kudelski Security* **10/2020 – 08/2021**
Topics: post-quantum cryptography as part of master thesis, and AI-Governance with the draft of an AI-centric dashboard.

ML Research Intern - *Cyber-Defense Campus* **07/2020 – 09/2020**
Evaluation of keyless and lightweight image obfuscation techniques towards privacy-preserving ML.

Student Assistant - *DeDiS Lab, EPFL* **2018 - 2020**
Participation in various tasks of the drand (Distributed RANDomness) project such as design of new features and implementation of a JS library that enables communication with a drand network. Coverage: `blog.cloudflare.com/league-of-entropy`

PUBLICATIONS

S&P 2023	**On the (In) security of Peer-to-Peer Decentralized Machine Learning** Dario Pasquini, Mathilde Raynal, Carmela Troncoso
PoPETS 2023	**Private Collection Matching Protocols** Kasra EdalatNejad, Mathilde Raynal, Wouter Lueks, Carmela Troncoso
EuroS&P 2022	**HyperLogLog: Exponentially Bad in Adversarial Settings** Kenny Patterson, Mathilde Raynal
NIST 3rd PQC Standardization Conference 2022	**PQ-WireGuard: We Did It Again** Mathilde Raynal, Aymeric Genet, Yolan Romailler

PRE-PRINTS

Under Submission	**On the conflict of Robustness and Learning in Collaborative Learning** Mathilde Raynal, Carmela Troncoso
arXiv 2023	**Can Decentralized Learning be more Robust than Federated Learning?** Mathilde Raynal, Dario Pasquini, Carmela Troncoso
arXiv 2020	**Image obfuscation for Privacy-Preserving Machine Learning** Mathilde Raynal, Mathias Humbert, Radhakrishna Achanta

TALKS (EXCLUDES CONFERENCE PRESENTATIONS)

Research@Linc (Commission Nationale Informatique et Libertés) **2023**
Collaborative Machine Learning: is it ready yet?

Summer School on Real-World Crypto and Privacy **2022**
Probabilistic Structures in Adversarial Scenarios: the case of HyperLogLog

GopherCon, GopherCon Europe, Conf42, BlackAlps **2021**
Taking the (Quantum) Leap with Go

GoTime Podcast **2021**
Using Go in unusual ways

SERVICE

Teaching Assistant **2022, 2023**
Computer Security, Advanced Topics in Privacy-Enhancing Technologies

Publicity Chair **2022, 2023, 2024**
PETS

External Reviewer
EuroS&P 2022, PoPETS 2023, USENIX 2023, TCOM 2023

Community involvement
VP of *Women+ in IC* **2023, 2024**
Introduction to programming to 5- to 12-year-olds using Scratch and Python with TechSpark Academy **2018**