CHRISTIAN MOUCHET

christian.mouchet@bluewin.ch – https://cmct.ch

EDUCATION

École polytechnique fédérale de Lausanne (EPFL) Lausanne, Switzerland

– *Ph.D. in Computer Science* 2023

Advisor: Carmela Troncoso, Co-Advisor: Jean-Pierre Hubaux
Dissertation: *Multiparty Homomorphic Encryption: from Theory to Practice*

– *M.Sc. in Computer Science* 2017

Minor: Information Security
Master thesis: *Homomorphic Lattice-based Cryptography for Secure Distributed Computation*

– *B.Sc. in Computer Science* 2014

Collège Calvin Geneva, Switzerland

– *Swiss federal high school diploma* 2010

WORK EXPERIENCE

Kudelski Security, Kudelski Group Chesaux, Switzerland

– *Security Engineer Extern* Feb 2016 - Jul 2017

In the Managed Security Services department during the early stages of it's new *Threat Monitoring Service*, I developed a model and associated software solution to help them abstract the complexity and diversity of their customer's infrastructure and requirements.

– *Security Engineer Intern* Jul. 2016 - Feb 2017

In the Cyber Fusion Center, I evaluated the service-critical data-source monitoring solutions and demonstrated that they were, at the time, insufficient.

Swiss Armed Forces Switzerland

– *Mechanized Infantry Group Leader, Sergeant* 2011

ACTIVITIES

Lattigo: A Multiparty Homomorphic Encryption Library in Go 2018-Present

I am co-authoring and maintaining the Lattigo open-source library, an advanced cryptographic library implementing the main fully homomorphic encryption schemes and their multiparty variants. The library is now well established in the community and is now a collaboration between EPFL and Tune Insight SA.

Research Projects Supervision (EPFL)

- G. Torrisi, *Helium: Implementation of an end-to-end encrypted MPC framework* *2023*
- A. Cucos, *Implementation of a multiparty homomorphic encryption circuit evaluator* *2022*
- M. Michel, *Implementation of a network layer for multiparty homomorphic encryption* *2021*
- Adrien Laydu, *Implementation of a threshold homomorphic encryption scheme* *2021*
- H. Sassi, W. Ben Naceur, *Implementation of a multikey homomorphic encryption scheme* *2021*
- A. Ibrahim, V. Parodi, *Cloud-based MPC using homomorphic encryption* *2020*
- C. Altmeyerhenzien, *Implementation of multiparty homomorphic encryption schemes* *2020*
- E. Daou, *Profiling and optimization of an homomorphic encryption library* *2020*
- Elia Anzuoni, *Implementation of an MPC framework using homomorphic encryption* *2020*
- E. Bertrand, *Practicality analysis of a threshold cryptosystem based on RLWE* *2020*

- B. Guðmundsson, *Lattice-based signature and key-exchange protocols for the Onet library* *2019*
- J. Lanzrein, *Network layer for lattice-based secure multiparty computation protocols* *2019*

TEACHING EXPERIENCE

École polytechnique fédérale de Lausanne (EPFL) Lausanne, Switzerland

– *COM-402: Information security and privacy, Teaching assistant* Fall 2019, 2020, 2021

– *COM-405: Mobile networks, Teaching assistant* Spring 2019, 2020, 2021, 2022

– *CS-523: Advanced topics on privacy enhancing technologies, Teaching assistant* Fall 2018

– *MATH-111: Linear Algebra, Teaching assistant* Fall 2017

Swiss Academy of Engineering Sciences (SATW) Switzerland

– *TecDays module: "AI: Contrôle une colonie de fourmis artificielle", Lecturer* 2019, 2020

Swiss Armed Forces Switzerland

– *Milice Instructor* 2010-2020

ACADEMIC PUBLICATIONS

PELTA – Shielding Multiparty-FHE against Malicious Adversaries
S Chatel, **C Mouchet**, AU Sahin", A Pyrgelis, C Troncoso, JP Hubaux
Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS 2023, to appear)

An Efficient Threshold Access-Structure for RLWE-Based Multiparty Homomorphic Encryption
C Mouchet, E Bertrand, JP Hubaux
IACR Journal of Cryptology 2023 (JOC 2023)

Multiparty Homomorphic Encryption from Ring-Learning-with-Errors
C Mouchet, J Troncoso-Pastoriza, JP Bossuat, JP Hubaux
Proceedings on Privacy Enhancing Technologies 2021 (PETS 2021)

Efficient bootstrapping for Approximate Homomorphic Encryption with Non-sparse Keys
JP Bossuat, **C Mouchet**, J Troncoso-Pastoriza, JP Hubaux
International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2021)

Lattigo: A Multiparty Homomorphic Encryption Library in Go
C Mouchet, JP Bossuat, J Troncoso-Pastoriza, J Hubaux
Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC 2020)

UnLynx: A Decentralized System for Privacy-Conscious Data Sharing
D Froelicher, P Egger, J Sá Sousa, JL Raisaro, Z Huang, **C Mouchet**, B Ford, JP Hubaux
Proceedings on Privacy Enhancing Technologies 2017 (PETS 2017)

SKILLS

Languages	English (fluent), French (mother tongue), German (high-school level)
Programming	Go, Python, Scala, C/C++, Java, JavaScript
Software Tools	Git, LaTeX, Docker, MATLAB, SageMath

AWARDS

– *Teaching Assistant Award, Faculty of Computer and Communication Science, EPFL* 2021

– *Deloitte Zurich Hackaton, Winning team of the forensic track* 2017

– *Audiance Choice Award for the "Event-stream detection project", Big Data Course, EPFL* 2015