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

Hasso-Plattner-Institute, University of Potsdam Potsdam & Berlin, Germany

– *Postdoctoral Researcher & Lecturer* Feb 2024 - Present

In the Cybersecurity - Identity Management group, I'm pursuing my research and assisting the group by supervising Msc. & PhD. students. I'm also teaching the course *Computing on Encrypted Data*, which I designed.

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* 2011-2020

ACTIVITIES

Open-source

- *Lattigo: A Multiparty Homomorphic Encryption Library in Go* *2018-Present*
  Lattigo is an advanced cryptographic library implementing several fully homomorphic encryption schemes and their multiparty variants. I'm one of the original authors of the library, which is now maintained by Tune Insight SA.
- *Helium: An MHE-Based MPC Framework* *2024-Present*
  Helium is a secure multiparty computation (MPC) framework based on multiparty homomorphic encryption (MHE). Helium builds on Lattigo and is the first open-source implementation of the MHE-based MPC protocol.

Academic Service

As a Program Committee member:
EuroS&P 2025, ACM CCS 2025, USENIX Security 2026
As a sub-reviewer:
PETS 2023, ASIACRYPT 2024

Research Projects Supervision

- *Security Analysis of Homomorphic Encryption in the Apple Ecosystem* — *Fall 2025*
  Master thesis @ HPI by Nils Hanff
- *Multi-Party Private Joins* — *Fall 2024*
  Master thesis @ HPI by Andrey Sidorenko
- *Helium: Implementation of an end-to-end encrypted MPC framework* — *Spring 2023*
  Semester project @ EPFL by Giovanni Torrisi
- *Design and implementation of a multiparty homomorphic encryption circuit evaluator* — *Fall 2022*
  Semester project @ EPFL by Adrian Cucos
- *Implementation of a network layer for multiparty homomorphic encryption* — *Fall 2021*
  Semester project @ EPFL by Manon Michel
- *Implementation of a threshold homomorphic encryption scheme* — *Spring 2021*
  Semester project @ EPFL by Adrien Laydu
- *Implementation of a multikey homomorphic encryption scheme* — *Spring 2021*
  Semester project @ EPFL by Hedi Sassi and Walid Ben Naceur
- *Cloud-based secure multiparty computation using homomorphic encryption* — *Fall 2020*
  Semester project @ EPFL by Anas Ibrahim and Vincent Parodi
- *Implementation of multiparty homomorphic encryption schemes* — *Fall 2020*
  Semester Project @ EPFL by Clémence Altmeyerhenzien
- *Profiling and optimization of an homomorphic encryption library* — *Spring 2020*
  Semester project @ EPFL by Elie Daou
- *Implementation of secure multiparty computation using homomorphic encryption* — *Spring 2020*
  Semester project @ EPFL by Elia Anzuoni
- *Practicality analysis of a threshold cryptosystem based on RLWE* — *Spring 2020*
  Master thesis @ EPFL by Elliott Bertrand
- *Lattice-based signature and key-exchange protocols for the Onet library* — *Fall 2019*
  Semester project @ EPFL by Björn Guðmundsson
- *Network layer for lattice-based secure multiparty computation protocols* — *Fall 2019*
  Semester project @ EPFL by Johan Lanzrein

TEACHING EXPERIENCE

Hasso-Plattner-Institute, University of Potsdam (HPI) — Potsdam, Germany

– *Computing on Encrypted Data, Lecturer* — Fall 2024, 2025

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

Accurate and Composable Noise Estimates for CKKS with Application to Exact HE Computation
JP Bossuat, A Costache, **C Mouchet**, L Nürnberger, and JR Troncoso-Pastoriza
IACR Communications in Cryptology, vol. 2, no. 2, Jul 07, 2025 (CiC 2025)

Helium: Scalable MPC among Lightweight Participants and under Churn
C Mouchet, S Chatel, A Pyrgelis, and C Troncoso
Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS 2024)

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)

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

– *Distinguished Artifact Award for the implementation of Helium, ACM CCS 2024*	2024
– *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