Christian Knabenhans

cknabs.github.io | christian.knabenhans@epfl.ch

I am pursuing a PhD student in applied cryptography at EPFL, working with Alessandro Chiesa and Carmela Troncoso. My research interests lie in the gap between the theory and practice of advanced cryptographic primitives, with a focus on efficiency, ease of deployment, high-assurance implementations, and meaningful security guarantees against real-world threats. In particular, I focus on zero-knowledge succinct non-interactive arguments of knowledge (zkSNARKs) and fully homomorphic encryption (FHE).

Education

09/2023—present **Doctoral student**, EPFL, Computation Security Lab (Alessandro Chiesa) &
Security and Privacy Engineering Lab (Carmela Troncoso)

- Lattice-based SNARKs, concrete security, high-assurance implementation of SNARKs.
- Designing privacy-preserving applications and protocols for at-risk populations.

09/2019—11/2022 **M.Sc. in Cyber Security**, Joint degree from ETH Zurich and EPFL — GPA: 5.73/6
Thesis: Practical Integrity Protection for Private Computations — Grade: 6/6
Major in Cyber Security, Minor in Software Engineering

01/2019—03/2019 **Exchange quarter**, University of Washington, Seattle — GPA: 3.90/4
Machine learning, natural language processing, reinforcement learning.

09/2015—08/2018 **B.Sc. in Computer Science**, ETH Zurich — GPA: 5.69/6
Thesis: Automatic Inference of Hyperproperties — Grade: 6/6
Major in Software Systems and Software Engineering, Minor in Computational Science

Professional Experience

06/2025—08/2025 **Research intern**, Brave Software, Inc., with Sofía Celi
Designing private approximate nearest neighbor search algorithms for web search engines from PIR.

11/2022—08/2023 **Research assistant**, ETH Zurich, Privacy-Preserving Systems Lab (Anwar Hithnawi)
Combining zkSNARKs and FHE for communication-efficient maliciously-secure two-party computation.

07/2021—12/2021 **Summer intern**, EPFL, Laboratory for Data Security (Jean-Pierre Hubaux)
Designing and implementing lightweight symmetric integrity primitives for fully homomorphic encryption.

02/2021—07/2021 **Research assistant**, EPFL, Security and Privacy Engineering Lab (Carmela Troncoso)
Quantifying information leakage in federated learning (particularly, property inference attacks).

08/2018—12/2018 **Security engineering intern**, Airlock, Ergon Informatik AG, Zurich
Fuzzing and improvement of the Airlock web application firewall, setup of a bug bounty.

Peer-reviewed Publications

** denotes equal contribution*

Under submission
contribution order
SoK: Single-Server Private Information Retrieval
Christian Knabenhans, Giacomo Fiorindo, Sofía Celi

Under submission
contribution order
End-to-End-Encrypted Collaborative Documents
Christian Knabenhans*, Zayd Maradni*, Carmela Troncoso

Under submission
alphabetical order
Universally Composable Maliciously-secure on-the-fly Multi-Party Computation
Ganyuan Cao, Sylvain Chatel, **Christian Knabenhans**,

Under submission
contribution order
A Privacy-Preserving Humanitarian Aid Distribution System with Statistics
Christian Knabenhans, Lucy Qin and Carmela Troncoso

Under submission
alphabetical order
On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments
Alessandro Chiesa, Ziyi Guan, **Christian Knabenhans** and Zihan Yu

[C4] Asiacrypt'24
alphabetical order
Lova: Lattice-Based Folding Scheme from Unstructured Lattices
Giacomo Fenzi, Duc Tu Pham, **Christian Knabenhans**, and Ngoc Khanh Nguyen
International Conference on the Theory and Application of Cryptology and Information Security, 2024

[C3] CCS’24 **VERITAS: Plaintext Encoders for Practical Verifiable Homomorphic Encryption**
contribution order Sylvain Chatel, **Christian Knabenhans**, Apostolos Pyrgelis, Carmela Troncoso and Jean-Pierre Hubaux
ACM Conference on Computer and Communications Security (CCS), 2024
Artifacts available, evaluated functional, results reproduced.

[C2] WAHC’24 **Verifiable Fully Homomorphic Encryption**
contribution order **Christian Knabenhans**, Alexander Viand, Antonio Merino-Gallardo and Anwar Hithnawi
12th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC), 2024

[C1] USENIX’24 **Holding Secrets Accountable: Auditing Privacy-Preserving Machine Learning**
contribution order Hidde Lycklama, Alexander Viand, Nicolas Küchler, **Christian Knabenhans** and Anwar Hithnawi
33rd USENIX Security Symposium, 2024
Artifacts available, functional, reproduced.

Talks

End-to-End Encrypted Collaborative Documents

Jun. 2025	Media Cybersecurity conference of the European Broadcasting Union	Geneva

A Privacy-Preserving Aid Distribution System with Assessment Capabilities;
Or, a Case Study on Threat Modelling and System Design

Jul. 2025	ENSL/CWI/KCL/IRISA Joint Cryptography Seminar	Online
May 2025	Max Planck Security and Privacy Seminar	MPI-SP
Mar. 2025	Real World Crypto 2025	Sofia

On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments

Mar. 2025	ZKProof 7	Sofia

Lova: a Lattice-based Folding Scheme from Unstructured Lattices

Aug. 2024	COSIC Seminar	KU Leuven

Towards Robust FHE for the Real World (with Alexander Viand)

Mar. 2024	Real World Crypto 2024	Toronto

Verifiable Fully Homomorphic Encryption

Jun. 2023	Zurich Information Security & Privacy Center (ZISC)	ETH Zurich
Mar. 2023	FHE.org conference 2023	Tokyo
Mar. 2023	Guest lecture in Daniele Micciancio’s “Advanced Crypto” graduate course	UC San Diego
Mar. 2023	Berkeley Security Seminar	UC Berkeley
Mar. 2023	Stanford Security Seminar	Stanford University
Nov. 2022	Security and Privacy Engineering Lab Seminar	EPFL

Civil Society and Industry Outreach

Terre des Hommes **Privacy Analysis of a Case Management Tool for a Children Safety NGO**
Mar.’25–Mar.’26 Saiid El Hajj Chehade, **Christian Knabenhans**, and Carmela Troncoso
alphabetical order *Privacy analysis of a deployment of the Primero™ tool for the Terre des Hommes NGO, which supports case workers in protecting children from abuse and exploitation. Interviews with TdH headquarters and field workers, threat and harm modelling, and recommendations.*

IBC **Limitations of C2PA in Privacy-Sensitive Applications**
Sep. 2025 Mohamed Badr Taddist, **Christian Knabenhans**, Lucille Verbaere and Carmela Troncoso
contribution order *Paper presented at the International Broadcasting Convention, a global conference for the media, entertainment, and broadcasting industries.*

IAB/W3C agews **Limitations and Pitfalls of Integrating PETs in Online Age Verification**
Oct. 2025 Sylvain Chatel, **Christian Knabenhans**, Wouter Lueks, Mathilde Raynal, Carmela Troncoso, and Ádám Vécsi
alphabetical order *Position paper presented at the Internet Architecture Board (IAB) and World Wide Web Consortium (W3C) Workshop on Age-Based Restrictions on Content Access.*

IAB/W3C agews **Private and Decentralized Age Verification Architecture**
Oct. 2025 Sofía Celi, Kyle den Hartog, Hamed Haddadi, **Christian Knabenhans**, and Elizabeth Margolin
alphabetical order *Position paper presented at the Internet Architecture Board (IAB) and World Wide Web Consortium (W3C) Workshop on Age-Based Restrictions on Content Access.*

Service

External reviewer Asiacrypt’26, S&P’25, Crypto’25, Eurocrypt’24, CCS’23

Organizer EPFL-ETH Summer School on Lattice-Based Cryptography, July 2025
Co-organized with Shannon Veitch and Jonathan Bootle, under the patronage of Alessandro Chiesa and Kenny Paterson. 30 participants, 20 000 CHF budget.

Member Prefiltering committee for the EPFL doctoral program in computer science 2025

Reviewer Review of Application Materials Program (RAMP) of the doctoral student's association at EPFL in computer science, which provides feedback on application materials (to EPFL or elsewhere) for prospective Ph.D. students without mentorship opportunities

Software

lattirust **A toolbox for lattice-based zkSNARKs**
Lattirust is a Rust library for lattice-based zkSNARKs, with a focus on efficiency, security, and ease of use, designed to be compatible with the arkworks ecosystem. It implements state-of-the-art lattice-based proof systems and proofs of encryption and decryption for lattice-based encryption schemes (in particular, for FHE).

zkOpenFHE **OpenFHE wrapper with proofs of correct computation**
zkOpenFHE is a drop-in replacement for the OpenFHE fully homomorphic encryption library. It automatically synthesizes zkSNARK circuits corresponding to an FHE computation, and proves correct FHE evaluation using a zkSNARK.

circomlib-fhe **circom zkSNARK circuits for fully homomorphic encryption**
A library of zkSNARK circuit templates for computations under fully homomorphic encryption in the circom language, a high-level domain-specific language for zero-knowledge proofs.

ringSNARK **SNARKs over rings, applied to fully homomorphic encryption**
Open-source implementation of Rinocchio, a lattice-based SNARK for statements over generic rings, with instantiations for rings used in FHE computations.

Teaching

Fall 2024,2025
COM-301 **Computer Security and Privacy** Carmela Troncoso, Edouard Bugnion, Thomas Bourgeat
B.Sc. course — information security, cryptography, security engineering. ≈ 300 students

Spring 2024, 2025
CS-523 **Advanced Topics in Privacy-Enhancing Tech** Carmela Troncoso, Alessandro Chiesa
M.Sc. course — threat modelling, anonymous communication, differential privacy, secure multi-party computation, homomorphic encryption, zero-knowledge proofs. ≈ 100 students

Supervision

Fall 2025	Stefan-Gabriel Popescu — What use cases for the Swiss eID?	M.Sc. thesis
Fall 2025	Lina Mounan — Harms from verifiable and anonymous credentials	M.Sc. semester project
Fall 2025	Derya Cögendez — Deploying humanitarian aid privately *Co-supervised with Boya Wang (EPFL).*	M.Sc. semester project
Spring 2025	Mohamed Badr Taddist — A security and privacy analysis of C2PA *Co-supervised with Lucille Verbaere (European Broadcasting Union).*	M.Sc. thesis
Spring 2025	Gustave Charles-Saigne — zkFHE	M.Sc. semester project
Spring 2025	Pedro Laginhas Gouveia — zkFHE	M.Sc. semester project
Spring 2025	Adrien Bouquet — Constant-time client-side FHE operations	M.Sc. semester project
Spring 2025	Kwok Wai Lui — Pairing-based proofs of lattice encryption	M.Sc. semester project
Fall 2024	Ganyuan Cao — UC-secure on-the-fly MPC from FHE and zkSNARKs *Co-supervised with Sylvain Chatel (CISPA).*	M.Sc. thesis
Fall 2024	Emile Hreich — GPU Acceleration of lattice-based proof systems	M.Sc. semester project
Fall 2024	Jiajung Jiang — Lattice-based proofs of lattice encryption	M.Sc. semester project
Fall 2024	Giacomo Fiorindo — SoK: single-server private information retrieval	M.Sc. semester project
Fall 2024	Xavier Marchon — A fast estimator for SIS-based proof systems	M.Sc. semester project

Spring 2024	Zihan Yu — On the Fiat–Shamir security of PIOP-based arguments *Co-supervised with Ziyi Guan (EPFL).*	M.Sc. semester project
Spring 2024	Zoë Reinke — Understanding parameters of UC-secure zkSNARKs	M.Sc. semester project
Spring 2023	Antonio Merino-Gallardo — zkSNARKs for 3rd generation FHE	M.Sc. semester project

Volunteer work

11/2024—present **Co-founder & Board member**, EPFL Cyber Group — Student Initiative

08/2021—07/2022 **President & Head of Marketing**, ETH Cyber Group — Student Initiative

Organizing bi-monthly cybersecurity talks and cyber policy trainings with experts from academia, industry, and the public and military sector, for an audience of roughly 450 students at ETH Zurich.

01/2020—07/2022 **Competitor & Coach**, Cyber 9/12 Strategy Challenge

Yearly coaching of 4–6 interdisciplinary teams of ETH students in cyber policy and cyber defense topics, in preparation for the Atlantic Council's Cyber 9/12 challenge in Geneva. My team won first place in 2020 (out of 20 teams worlwide), and the teams we coached have won top places in the past years.

08/2019—03/2022 **Board Member for Culture**, L'Association Francophone des Étudiants de Zurich

Organizing cultural events for the roughly 550 french-speaking students in Zurich, collaborating with the French diplomatic representations and other french-speaking organizations.