Christian Knabenhans

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

I am a PhD student at EPFL, working with Alessandro Chiesa and Carmela Troncoso. My research aims to close the gap between the theory and practice of advanced cryptographic primitives, with a focus on efficiency and meaningful security guarantees against real-world threats.

I work with at-risk populations such as humanitarian aid organizations (Terre des Hommes, International Committee of the Red Cross) and journalists (International Consortium of Investigative Journalists, European Broadcasting Union). In interactions with these populations, I surface security and privacy problems that have remained unaddressed, together with their requirements and real-world threat models. I then formalize these requirements and design privacy-preserving systems to address them using advanced cryptographic primitives. Finally, I implement and evaluate these systems, and feed deployment constraints back into designs. As part of this work, I improve underlying cryptographic primitives, in particular zero-knowledge and succinct arguments.

Education

present – Sep. 2023 **Doctoral student**, EPFL
Thesis: Taking Advanced Cryptography from Theory to Practice to Protect at-risk Users

Nov. 2022 – Sep. 2019 **M.Sc. in Cyber Security**, Joint degree from ETH Zurich and EPFL — GPA: 5.73/6
Thesis: Practical Integrity Protection for Private Computations (with Anwar Hithnawi) — Grade: 6/6

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

Aug. 2018 – Sep. 2015 **B.Sc. in Computer Science**, ETH Zurich — GPA: 5.69/6
Thesis: Automatic Inference of Hyperproperties (with Peter Müller) — Grade: 6/6

Professional Experience

Jun. 2026 – Aug. 2026 **Research intern**, Microsoft Research, Cryptography group, with Greg Zaverucha
Designing and and optimizing secure collaboration tools as part of the Encrypted Spaces projects.

Aug. 2025 – Jun. 2025 **Research intern**, Brave Software Inc., Brave Research team, with Sofía Celi
Designing private approximate nearest neighbor search algorithms from private information retrieval.

Aug. 2023 – Nov. 2022 **Research assistant**, ETH Zurich, Privacy-Preserving Systems Lab, with Anwar Hithnawi
Combining zkSNARKs and FHE for communication-efficient maliciously-secure two-party computation.

Dec. 2021 – Jul. 2021 **Research intern**, EPFL, Laboratory for Data Security, with Jean-Pierre Hubaux
Lightweight integrity primitives for fully homomorphic encryption. (Summer@EPFL fellowship program)

Jul. 2021 – Feb. 2021 **Research assistant**, EPFL, Security and Privacy Engineering Lab, with Carmela Troncoso
Quantifying information leakage and success of property inference attacks in federated learning.

Dec. 2018 – Aug. 2018 **Security engineering intern**, Airlock, Ergon Informatik AG, Zurich
Fuzzing and improvement of the Airlock web application firewall, setup of a bug bounty.

Publications

** denotes equal contribution among contribution-ordered authors*
Authors are listed in alphabetical order in the cryptography community, and in order of decreasing contribution in the security and privacy community. [C] denotes a conference, [J] a journal, and [W] a workshop with proceedings.

Under submission (contribution order) **SafeCast: End-to-End Security for Ultra-High-Bitrate Broadcast Media**
Arman Kolozyan, **Christian Knabenhans**, Zayd Maradni, Carmela Troncoso

Under submission (contribution order) **On the (Privacy) Harms of the EU Digital Identity Framework**
Christian Knabenhans*, Shannon Veitch*, Mathilde Raynal, Theresa Stadler, Sylvain Chatel, Wouter Lueks, Carmela Troncoso

[C8] Asiacrypt'26 (alphabetical order) **HE-based On-the-Fly MPC, Revisited: Universal Composability, Approximate and Imperfect Computation, Circuit Privacy**
Ganyuan Cao, Sylvain Chatel, **Christian Knabenhans**
International Conference on the Theory and Application of Cryptology and Information Security, 2026

[C7] TCC'26 **Succinct Arguments from Lattice-Based Non-Interactive Linear Commitments**
alphabetical order Jonathan Bootle, Ziyi Guan, and **Christian Knabenhans**
Theory of Cryptography Conference, 2026

[J1] Proc. IEEE **How to Build Succinct Arguments from Succinct Commitments**
alphabetical order Alessandro Chiesa, Ziyi Guan, **Christian Knabenhans**, Eylon Yogev
Proceedings of the IEEE special issue — Cryptographically-Secure Computing with Privacy and Integrity

[C6] Crypto'26 **On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments**
contribution order Alessandro Chiesa, Ziyi Guan, **Christian Knabenhans**, Zihan Yu
International Cryptology Conference (Crypto), 2026

[C5] USENIX Sec'26 **End-to-End Encrypted Collaborative Documents**
contribution order **Christian Knabenhans***, Zayd Maradni*, Carmela Troncoso
USENIX Security Symposium, 2026
Artifacts available.
🎗 Internet Defense Prize, Distinguished Paper Runner-Up

[C4] PETS'26 **A Privacy-Preserving Humanitarian Aid Distribution System with Statistics**
contribution order **Christian Knabenhans**, Lucy Qin, Justinas Sukaitis, Vincent Graf Narbel, Carmela Troncoso
Privacy Enhancing Technologies Symposium (PETS), 2026
Artifact available, functional, reproduced.

[C3] Asiacrypt'24 **Lova: Lattice-Based Folding Scheme from Unstructured Lattices**
alphabetical order Giacomo Fenzi, Duc Tu Pham, **Christian Knabenhans**, Ngoc Khanh Nguyen
International Conference on the Theory and Application of Cryptology and Information Security, 2024

[C2] CCS'24 **VERITAS: Plaintext Encoders for Practical Verifiable Homomorphic Encryption**
contribution order Sylvain Chatel, **Christian Knabenhans**, Apostolos Pyrgelis, Carmela Troncoso Jean-Pierre Hubaux
ACM Conference on Computer and Communications Security (CCS), 2024
Artifacts available, evaluated functional, results reproduced.

[W1] WAHC'24 **Verifiable Fully Homomorphic Encryption**
contribution order **Christian Knabenhans**, Alexander Viand, Antonio Merino-Gallardo Anwar Hithnawi
Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC) @ ACM CCS, 2024

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

Talks

On the (Privacy) Harms of the EU Digital Identity Framework

[T20]	Jul. 2026	Policy-Relevant Research Workshop @ PETS 2026 (with Shannon Veitch)	Workshop
[P2]	Jul. 2026	German Bundestag, working group for digital affairs of the Linksfraktion	Panelist
[T19]	May 2026	Workshop on Technology and Consumer Protection @ IEEE S&P 2026	Workshop
[P1]	May 2026	Panel at the Cryptographic Applications Workshop @ Eurocrypt 2026	Panelist
[T18]	May 2026	Cryptographic Applications Workshop @ Eurocrypt 2026 (with Shannon Veitch)	Workshop

Succinct Arguments from Lattice-based Non-Interactive Linear Commitments
Coming Back from the Knowledge k-RISIS: Building Arguments from k-PRISIS

[T24]	Nov. 2026	Theory of Cryptography Conference (TCC) 2026	Conference
[T17]	May 2026	ZKProof 8 @ Eurocrypt 2026	Workshop

End-to-End Encrypted Collaborative Documents

[T22]	Aug. 2026	USENIX Security Symposium 2026	Conference
[T16]	Mar. 2026	Real World Crypto (RWC) Symposium 2026 (with Zayd Maradni)	Conference
[T13]	Jun. 2025	Media Cybersecurity conference of the European Broadcasting Union	Invited

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

[T21]	Jul. 2026	Privacy-Enhancing Technologies Symposium (PETS) 2026	Conference
[T14]	Jul. 2025	ENSL/CWI/KCL/IRISA Joint Cryptography Seminar	Invited
[T11]	May 2025	Max Planck Institute Security and Privacy Seminar	Invited
[T10]	Mar. 2025	Real World Crypto (RWC) Symposium 2025	Conference

HE-based On-the-Fly MPC, Revisited: Universal Composability, Approximate and Imperfect Computation, Circuit Privacy

[T25]	Dec. 2026	Asiacrypt 2026	Conference

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

[T23]	Aug. 2026	Crypto 2026	Conference
[T15]	Sep. 2025	Technical University of Munich Blockchain Seminar	Invited
[T12]	Jun. 2025	Parisian Cryptography Seminar, ENS rue d'Ulm	Invited
[T9]	Mar. 2025	ZKProof 7 @ RWC 2025	Workshop

Lova: a Lattice-based Folding Scheme from Unstructured Lattices

[T8]	Aug. 2024	COSIC Seminar, KU Leuven	Invited

Verifiable Fully Homomorphic Encryption / Towards Robust FHE for the Real World

[T7]	Mar. 2024	Real World Crypto (RWC) Symposium 2024 (with Alexander Viand)	Conference
[T6]	Jun. 2023	Zurich Information Security & Privacy Center (ZISC) Seminar, ETH Zurich	Invited
[T5]	Mar. 2023	FHE.org conference @ RWC 2023	Workshop
[T4]	Mar. 2023	Guest lecture, Daniele Micciancio's "Advanced Crypto" grad course, UC San Diego	Invited
[T3]	Mar. 2023	UC Berkeley Security Seminar	Invited
[T2]	Mar. 2023	Stanford Security Seminar	Invited
[T1]	Mar. 2023	Security and Privacy Engineering Lab Seminar, EPFL	Invited

Invited Workshops

Mar. 2027	Dagstuhl Seminar 27112: Bridging Formal Guarantees and Real-World Implementations of Zero-Knowledge Proofs	Invite-only Workshop
2024–2026	Workshop on High Assurance Crypto Software (HACS)	Invite-only Workshop

Policy, Civil Society, and Industry Outreach

German Bundestag, Jul. 2026
Expert consultation (Fachgespräch): „Digitale Identitäten"
Invited expert, for MdBs of working group for digital affairs of the German Bundestag's Linksfraktion.

EU Parliament, Dec. 2025
Roundtable: "Age verification in the Digital Single Market: What is Technically Possible, Proportionate, and Realistic?"
Participant, on invitation of MEP Maria Guzenina, Vice-Chair of the Child Rights Intergroup.

Terre des Hommes, Mar.'25–Mar.'26, alphabetical order
Privacy Analysis of a Case Management Tool for a Children Safety NGO
Saiid El Hajj Chehade, **Christian Knabenhans**, and Carmela Troncoso
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.

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

SMPTE MTS'25, Oct. 2025, contribution order
Privacy Vulnerabilities in C2PA Content Provenance Systems: Privacy Analysis and Recommendations for News Media Workflow
Mohamed Badr Taddist, **Christian Knabenhans**, Lucille Verbaere and Carmela Troncoso
Paper accepted and presented at the 2025 Media Technology Summit, a global conference on media technologies, organized by the Society of Motion Picture and Television Engineers (SMPTE).

IBC'25, Sep. 2025, contribution order
Limitations of C2PA in Privacy-Sensitive Applications
Mohamed Badr Taddist, **Christian Knabenhans**, Lucille Verbaere and Carmela Troncoso
Paper accepted and presented at the 2025 International Broadcasting Convention, a global conference for the media, entertainment, and broadcasting industries.

Awards

2026	Internet Defense Prize (25k USD cash prize)	USENIX Security Symposium 2026
2026	Distinguished Paper Runner-Up	USENIX Security Symposium 2026

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.

Academic Service

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.
Speakers: Fernando Virdia, Vadim Lyubashevsky, Gregor Seiler, Jonathan Bootle, Christian Mouchet, Akin Ünal, Lena Heimberger. 30 graduate students, 5 days, 20 000 CHF grant

External reviewer — Asiacrypt'26, Crypto'26, Asiacrypt'25, IEEE S&P'25, Crypto'25, Eurocrypt'24, ACM CCS'23

Member — Prefiltering committee for the EPFL computer science doctoral program and fellowships, 2025

Member — Extraordinary disciplinary commission of EPFL, representative for doctoral students, 2024

Mentor — 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

Teaching

Fall 2024, 2025 — **Computer Security and Privacy** Carmela Troncoso, Edouard Bugnion, Thomas Bourgeat
COM-301 — B.Sc. course — information security, cryptography, security engineering. ≈ 400 students

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

Supervision

Fall 2027 — Iman Attia — On the security and privacy of identity claims in C2PA — M.Sc. thesis
Co-supervised with Lucille Verbaere (European Broadcasting Union).

Spring 2026 — Vladimir Hanin — Private navigation and location services — M.Sc. thesis

Spring 2026 — Théo Houle — Anonymous credentials for public transportation — M.Sc. thesis

Spring 2026 — Arman Kolozyan — End-to-end encryption for broadcasting — Internship (at MPI-SP)
Co-supervised with Zayd Maradni (Max Planck Institute for Security and Privacy).
Related publication: SafeCast: End-to-End Security for Ultra-High-Bitrate Broadcast Media
→ Pre-doctoral researcher at CISPA Helmholtz Center for Information Security

Fall 2025 — Stefan-Gabriel Popescu — Harms and opportunities of the Swiss e-ID system — M.Sc. thesis

Fall 2025 — Lina Mounan — Harms of electronic ID deployments worldwide — M.Sc. semester project
Co-supervised with Boya Wang (EPFL).

Fall 2025 — Derya Cögendez — Implementing private humanitarian aid — M.Sc. semester project
Co-supervised with Boya Wang (EPFL).

Fall 2025 Tobias Rothmann — Formally verifying properties of KZG M.Sc. semester project (at TUM)

Spring 2025 Mohamed Badr Taddist — A security and privacy analysis of C2PA M.Sc. thesis
Co-supervised with Lucille Verbaere (European Broadcasting Union).
→ European Broadcasting Union and Security4Media

Spring 2025 Gustave Charles-Saigne — zkSNARKs for FHE M.Sc. semester project

Spring 2025 Pedro Laginhas Gouveia — zkSNARKs for FHE 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 M.Sc. thesis
Co-supervised with Sylvain Chatel (CISPA).
Related publication: HE-based On-the-Fly MPC, Revisited: Universal Composability, Approximate and Imperfect Computation, Circuit Privacy (Asiacrypt'26)
→ PhD student at Télécom Paris, Institut Polytechnique de Paris

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 lattice proof systems M.Sc. semester project

Spring 2024 Zihan Yu — On the Fiat–Shamir security of PIOP-based arguments M.Sc. semester project
Co-supervised with Ziyi Guan (EPFL).
Related publication: On the Fiat–Shamir Security of Succinct Arguments from Functional Commitments (Crypto'26)
→ PhD student at Yale University

Spring 2024 Zoë Reinke — Understanding parameters of UC-secure zkSNARKs M.Sc. semester project
→ PhD student at ETH Zurich

Spring 2023 Antonio Merino-Gallardo — zkSNARKs for FHE M.Sc. semester project (at ETH)
Related publication: Verifiable Fully Homomorphic Encryption (WAHC'24)
→ PhD student at IBM Research Zurich & Hasso Plattner Institute

Volunteer work

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

Jul. 2022 – Aug. 2021 **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.

07/2022 – 01/2020 **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.

03/2022 – 08/2019 **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.