

David Froelicher

Post-Doctoral Researcher

PERSONAL DATA



Birth: April 26th, 1992

Nationality: Swiss

Languages:

- English | C2

- French | native

- German | B1



(+41) 79 704 16 28

(+1) 617 544 27 40

david@froelicher.net



www.davidfroelicher.com

github.com/froelich

[Google Scholar](#)

[Linkedin](#)



Massachusetts Institute of
Technology (MIT) &
Broad Institute of MIT and
Harvard

RESEARCH INTERESTS

Decentralized systems

Applied cryptography

Security and Privacy for Data Sharing

Privacy-enhancing technologies

Genomic Privacy

CODING SKILLS (main)

Golang, Java, Latex

EDUCATION

**Master of engineering in
communication systems specialized
in IT security**

Ecole Polytechnique Fédérale de
Lausanne | 2016

**Bachelor of engineering in
communication systems**

Ecole Polytechnique Fédérale de
Lausanne | 2014

PROFILE

Post-Doctoral Researcher. I am working with Prof. B. Berger in the Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology (MIT) and with Dr. H. Cho at the Broad Institute of MIT and Harvard. **I am currently working on privacy-preserving federated analytics and genomic privacy by relying on homomorphic encryption, secure multiparty computation, distributed systems and differential privacy.**

I received my PhD from the Ecole Polytechnique Fédérale de Lausanne (EPFL) for my work with Prof. Jean-Pierre Hubaux at the Laboratory for Data Security (LDS) and Bryan Ford at the Decentralized and Distributed Systems Laboratory (DeDiS). I earned my MSc and BSc in Computer Science with a specialisation in IT Security from EPFL in 2016. In 2015, I did a master thesis internship in the NEC research laboratory in Heidelberg, Germany, where I have been involved in the design and implementation of a system enabling proofs of retrievability on deduplicated data.

EXPERIENCE

Post-Doctoral Researcher

MIT & Broad Institute | USA | 2022 - present

[Prof. B. Berger's group](#) in Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology (MIT) and

[Dr. H. Cho's group](#) at the Broad Institute of MIT and Harvard

Post-Doctoral Researcher

EPFL | Switzerland | 2021

Laboratory for data security ([LDS](#), led by Prof. Jean-Pierre Hubaux) and

Decentralized and Distributed Systems Lab ([DeDiS](#), led by Prof. Bryan Ford)

Ph.D. Student

EPFL | Switzerland | 2016 - 2021

Laboratory for data security ([LDS](#), led by Prof. Jean-Pierre Hubaux) and

Decentralized and Distributed Systems Lab ([DeDiS](#), led by Prof. Bryan Ford)

Research Assistant

EPFL | Switzerland | 2016

Laboratory for data security ([LDS](#))

Master Thesis

NEC Laboratories Europe | Heidelberg, Germany | 2015 - 2016

Analysis of Security Primitives for Public Clouds. Implementing Proofs of Retrievability in Deduplicated Storage Systems.

Master Projects

EPFL | Switzerland | 2013- 2014

- Implement a zero-configuration peer-to-peer network for Map Reduce.

- Dynamically display historical data on Google Earth and enable users to navigate through the use of a Kinect.

PhD Thesis

Privacy-Preserving Federated Analytics using Multiparty Homomorphic Encryption
[\[thesis\]](#)[\[slides 1\]](#)[\[slides 2\]](#)

Talks & Awards

Invited Talk in Genomic Privacy & Security Special Session at ISMB 2022

Madison, Wisconsin, USA | 2022
Presentation on Privacy-Preserving Federated Biomedical Analysis with Multiparty Homomorphic Encryption.
[\[website\]](#)[\[talk\]](#)[\[slides\]](#)

7th International Workshop on Genome Privacy and Security (GenoPri'20)

Online | 2020
Presentation on Privacy-Preserving Multi-centric Medical Research with Multi-party Homomorphic Encryption.
[\[website\]](#)[\[talk \(at 1h34\)\]](#)[\[slides\]](#)

Microsoft Private AI Bootcamp

Redmond, Washington, USA | 2019
30 selected Ph.D. students invited to a bootcamp with Microsoft Research.
[\[website\]](#)[\[talk\]](#)[\[tech report\]](#)

IDash Privacy & Security Workshop – Secure Genome Analysis Competition 2019

Indianapolis, Indiana, USA | 2019
Presentation of runner-up solution in Track II: Secure Genotype Imputation using Homomorphic Encryption.
[\[website\]](#) [\[blog\]](#) [\[talk\]](#)

Short Presentation of research interests

Lausanne, Switzerland | 2019
[\[talk\]](#)

PUBLICATIONS (main)

D. Froelicher, J. R. Troncoso-Pastoriza, J. L. Raisaro, M. Cuendet, J. S. Sousa, H. Cho, B. Berger, J. Fellay, and J.-P. Hubaux. “*Truly Privacy-Preserving Federated Analytics for Precision Medicine with Multiparty Homomorphic Encryption*”. Nature Communications, 2021. [\[paper\]](#)

S. Sav, A. Pyrgelis, J. R. Troncoso-Pastoriza, **D. Froelicher**, J.-P. Bossuat, J. S. Sousa and J.-P. Hubaux. “*POSEIDON: Privacy-Preserving Federated Neural Network Learning*”. Network and Distributed Systems Security (NDSS) Symposium 2021. [\[paper\]](#)

D. Froelicher, J. R. Troncoso-Pastoriza, A. Pyrgelis, S. Sav, J. S. Sousa, J.-P. Bossuat, and J.-P. Hubaux. “*Scalable Privacy-Preserving Distributed Learning*.” Privacy Enhancing Technologies Symposium (PETS), volume 3, 2021. (PETS 2021). [\[paper\]](#)[\[talk\]](#)[\[slides\]](#)

M. Kim, A. Harmanci, J.-P. Bossuat, S. Carpov, J. H. Cheon, I. Chillotti, W. Cho, **D. Froelicher**, N. Gama, M. Georgieva, S. Hong, J.-P. Hubaux, D. Kim, K. Lauter, Y. Ma, L. Ohno-Machado, H. Sofia, Y. Son, Y. Song, J. Troncoso-Pastoriza and X. Jiang. “*Ultra-Fast Homomorphic Encryption Models enable Secure Outsourcing of Genotype Imputation*”. Cell Systems, 2021. [\[paper\]](#)

D. Froelicher, M. Misbach, J. R. Troncoso-Pastoriza, J.L. Raisaro, J.-P. Hubaux. “*MedCo²: Privacy-Preserving Cohort Exploration and Analysis*”. Studies in Health Technology and Informatics, 2020.

D. Froelicher, J.R. Troncoso-Pastoriza, J.S. Sousa and J.P. Hubaux, “*Drynx: Decentralized, Secure, Verifiable System for Statistical Queries and Machine Learning on Distributed Datasets.*”, IEEE Transactions on Information Forensics and Security , Vol. 15 , Issue. 1, pp. 3035-3050, 2020. [\[paper\]](#)

D. Froelicher, P. Egger, J. S. Sousa, J. L. Raisaro, Z. Huang, C. Mouchet, B. Ford, and J.-P. Hubaux: “*UnLynx: A Decentralized System for Privacy-Conscious Data Sharing*.” Privacy Enhancing Technologies Symposium (PETS), volume 4, pages 152–170, Minneapolis, USA, 2017. [\[paper\]](#)[\[talk\]](#)[\[slides\]](#)

F. Armknecht, J.-M. Bohli, **D. Froelicher** and G. Karame. “*SPORT: Sharing Proofs of Retrievability across Tenants*.” Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, pages 275-287, 2017. [\[paper\]](#)

Reviewer Activities

Bioinformatics | 2022-present

International Society for Molecular Biology (ISMB) | 2022-present

Privacy Enhancing Technologies Symposium | 2019 & 2021

Digital Signal Processing Journal | 2018-present

EURASIP Journal on Information Security | 2018 - present

Journal of Visual Communication and Image Representation | 2018 - present

International Conference on Information Systems Security and Privacy | 2016

Teaching

Master Thesis Supervision
EPFL | 2019

- "Privacy-Preserving Statistics on Medical Data Using Homomorphic Encryption", John Stephan at Swisscom, Switzerland.

- "Efficient Privacy-Preserving Neural Network Inference for Heart Arrhythmia Detection", Philipp Chervet at CSEM, Switzerland.

Semester Projects Supervision
EPFL | 2017-present

- 1 Bachelor project
- 12 Master projects
- 2 Summer at EPFL projects

Teaching Assistant
EPFL | 2017-present

- Mobile Network, Master
- Information Security & Privacy, Master
- Advanced Topics on Privacy Enhancing Technologies, Master
- Introduction to Object-oriented Programming, Bachelor

Main Projects

Center for Admixture Science and Technology (CAST). 2021-present
CAST will use the largest genomic datasets of individuals with diverse ancestry, in combination with socioeconomic data, to better predict health and disease in admixed individuals. The goal is also to conduct scalable distributed computing using data from millions of individuals across the AoU and MVP compute enclaves.
Partners: UC San Diego, Broad Institute; University of Texas Health; Indiana University; Veterans Administration.

DPPH: Data Protection in Personalized Health funded by the Strategic Focus Area Personalized Health and Related Technologies (PHRT) of the ETH Board. 2018-2021 | Budget: CHF 3M

This project aims at providing a secure and privacy-conscious framework to enable clinical and genomic data sharing and exploitation across a federation of medical institutions, hospitals and research labs.
Academic partners: Fellay Group, DeDiS, LDS, GR-JET (EPFL) and Health Ethics and Policy (ETH). Industrial partners: SDSC.

MedCo: Enabling the Secure and Privacy-Preserving Exploration of Distributed Clinical and *Omics Cohorts in the Swiss Personalized Health Network (SPHN) funded by the PHRT and the SPHN.

2019-2021 | Budget: CHF 0,5 M

This project aims at testing and deploying in operational environments secure and privacy-conscious cohort explorers dealing with distributed clinical and *omics data.

Software Projects (main)

Spindle

<https://github.com/ldsec/spindle> (private) | 2020 - present

Spindle is a distributed system for the secure and federated training and evaluation of machine learning models (linear/logistic regression, neural networks) on data from multiple sources. It makes use of lattice-based cryptography (*lattigo*). Developed in Golang at the LDS group at EPFL.

iDash solution 2019

<https://github.com/ldsec/idash2020> (private) | 2019

Homomorphic encryption-based realization of a client-server privacy-preserving solution for genotype imputation based on the lattice-based homomorphic encryption scheme CKKS. Solution presented in the Homomorphic Encryption track of the iDash Secure Genome Processing Challenge in its 2019 edition (third place). Developed in Golang at the LDS group, EPFL.

Lattigo

<https://github.com/ldsec/lattigo>

Lattigo is a Go package implementing centralized and multiparty lattice-based cryptographic primitives. Developed in Golang at the LDS group, EPFL.

MedCo

<https://medco.epfl.ch>

MedCo is the first operational system that makes sensitive medical-data available for research in a simple, privacy-conscious and secure way. It enables hundreds of clinical sites to collectively protect their data and to securely share

Recreation

Cycling, tennis, badminton,
football, squash, ski, guitar, travel

them with investigators, without single points of failure. The core module is developed in Golang, with additional modules and connectors in Javascript, Java and Scala.

Drynx

<https://github.com/ldsec/drynx>

Drynx is a library implementing secure multiparty protocols, homomorphic encryption, zero-knowledge proofs and blockchains in order to support a decentralized system that enables privacy-preserving statistical queries and the training and evaluation of machine-learning regression models on distributed datasets. It provides data confidentiality and individuals' privacy, and ensures the correctness of the computations, protects data providers' privacy and guarantees robustness of query results. Developed in Golang at the LDS group, EPFL.

UnLynx

<https://github.com/ldsec/unlynx>

Unlynx is a library implementing interactive protocols to perform distributed cryptographic operations such as key switching and Neff shuffle. The developed prototype is at the core of the operational software, MedCo, that is being deployed at the Swiss University Hospitals. Developed in Golang at the LDS group, EPFL.