David Froelicher

Postdoctoral Researcher

PERSONAL DATA

Birth: April 26th, 1992
Nationality: Swiss
Languages:
- English | fluent
- French | native
- German | basic

(+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

Summary

14 publications in top-tier conferences and journals, e.g., IEEE S&P, PETs, NDSS, Nature Communications

2 patents

Supervised 19 students
Participated in teaching of 4 classes over 5 years

Research led to the creation of a startup and 2 softwares used in applications

PROFILE

Postdoctoral Researcher. I am collaborating with Prof. B. Berger at the Computer Science and Artificial Intelligence Laboratory (CSAIL) at the Massachusetts Institute of Technology (MIT), as well as with Dr. H. Cho at the Broad Institute of MIT and Harvard. **Currently, my research focuses on privacy-preserving federated analytics, machine learning, and genomic privacy. I am designing novel secure and distributed solutions, leveraging applied cryptography techniques such as homomorphic encryption and secure multiparty computation.**

EXPERIENCE & EDUCATION

Postdoctoral Researcher
MIT & The Broad Institute of MIT and Harvard | 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, now at Yale University

Postdoctoral 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's Degree
Ecole Polytechnique Fédérale de Lausanne | 2014 - 2016
Master of engineering in communication systems specialized in IT security

Bachelor's Degree
Ecole Polytechnique Fédérale de Lausanne | 2010 - 2014
Bachelor of engineering in communication systems

PUBLICATIONS

H. Smajlovic*, **D. Froelicher***, B. Berger, H. Cho, and I. Numanagic. "*A versatile and efficient programming framework for secure federated biomedical computation".* Under submission.

M. Hong*, **D. Froelicher***, R. Magner, V. Popic, B. Berger, and H. Cho. "*Secure Discovery of Genetic Relatives across Large-Scale and Distributed Genomic Datasets".* Accepted at Recomb 2024.

H. Cho, **D. Froelicher**, J. Chen, M. Edupalli, A. Pyrgelis, J. R. Troncoso-Pastoriza, J.-P. Hubaux, B. Berger. *"Secure and Federated Genome-Wide Association Studies for Biobank-Scale Datasets".* Under revision at Nature Genetics. [paper]

D. Froelicher, H. Cho, M. Edupalli, J. S. Sousa, J.-P. Bossuat, A. Pyrgelis, J. R. Troncoso-Pastoriza, B. Berger and J.-P. Hubaux. *"Scalable and Privacy-Preserving Federated Principal Component Analysis".* IEEE Security and Privacy (IEEE S&P) 2023. [paper, arxiv, trailer video, video]

S. Mendelsohn, **D. Froelicher**, D. Loginov, D. Bernick, B. Berger, H. Cho (2023). "*sfkit: A Web-Based Toolkit for Secure and Federated Genomic Analysis*". Nucleic Acids Research 2023. [paper, website]

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]

J.R. Troncoso-Pastoriza, **D. Froelicher**, P. Hu, A. Aloufi and J.P. Hubaux. "*Privacy-Preserving Data Sharing and Computation Across Multiple Data Providers with Homomorphic Encryption.*" Protecting Privacy through Homomorphic Encryption, 65-80. [book]

D. Froelicher, M. Misbach, J. R. Troncoso-Pastoriza, J.L. Raisaro, J.-P. Hubaux. *"MedCo^2: 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]

Patents

D. Froelicher, J.R. Troncoso-Pastoriza, A. Pyrgelis, S. Sav, J.A. Gomes de Sá e Sousa, J.P. Hubaux, J.P. Bossuat. System and Method for Privacy-Preserving Distributed Training of Machine Learning Models on Distributed Datasets. Patent No:WO2021223873 (A1) EPFL (2021).

S. Sav, J.R. Troncoso-Pastoriza, A. Pyrgelis, **D. Froelicher**, J.A. Gomes de Sá e Sousa, J.P. Bossuat, J.-P. Hubaux. System and Method for Privacy-Preserving Distributed Training of Neural Network Models on Distributed Datasets. Patent No:WO2022042848 (A1). EPFL (2022).

PhD Thesis

Privacy-Preserving Federated Analytics using Multiparty Homomorphic Encryption
[thesis][slides - private defense][slides - public defense]

Talks & Awards

Among Winners at IDash Privacy & Security Workshop – Secure Genome Analysis Competition 2023
Yale University, USA | 2019; Secure Relative Detection in (Forensic) Databases [website]

Invited Talk in the Translational Medical Informatics track at ISMB 2023
Lyon, France | 2023; Enabling collaborative analysis of genomic data silos with privacy [slides][poster]

Runner-up Team for Finale Phase of the U.S. PETS Prize Challenge
London, UK | 2023; Privacy-preserving federated learning for pandemic forecasting [website]

Winning Team for Phase 1 of the U.S. PETS Prize Challenge
London, UK | 2022; Privacy-preserving federated learning for pandemic forecasting [website]

Seminar Lecture at the Institute for IT Security at Lübeck University
Online | 2023**:** Privacy-Preserving Federated Analytics with Multiparty Homomorphic Encryption [slides]

Invited Talk in Genomic Privacy & Security Special Session at ISMB 2022
Madison, Wisconsin, USA | 2022; Privacy-Preserving Federated Biomedical Analysis with Multiparty Homomorphic Encryption. [website][talk][slides]

Flash Talk in 2022 Annual NHGRI Centers of Excellence in Genomic Science Meeting
Durham, NC, USA | 2022; Secure and Federated Genome-Wide Association Studies [website]

7th International Workshop on Genome Privacy and Security (GenoPri'20)
Online | 2020; Privacy-Preserving Multi-centric Medical Research with Multi-party Homomorphic Encryption. [website][talk (at 1h34)][slides]

Microsoft Private AI Bootcamp
Redmond, Washington, USA | 2019; Among selected Ph.D. students invited to a bootcamp with Microsoft Research. [website][talk][tech report]

Among Winners at IDash Privacy & Security Workshop 2019
Indianapolis, USA | 2019; Secure Genotype Imputation using Homomorphic Encryption. [website] [blog]

Short Presentation of Research
Lausanne, Switzerland | 2019; [talk]

Research Initiatives

NIH Grant for *privacy-preserving genomic medicine at scale*. 2022-present

The major goals of this project are to develop and drive the use of privacy technologies for complex and integrative tasks at the forefront of genomic medicine to address the pressing needs in the biomedical community for broader data sharing.

Partners: MIT, The Broad Institute of MIT and Harvard.

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.

Teaching

PhD Student Supervision MIT | 2021-present

- *"Secure Discovery of Genetic Relatives across Large-Scale Distributed Datasets",* Matt Hong
- *"A versatile and efficient programming framework for secure federated biomedical computation",* Haris Smajlovic

Master Thesis Supervision EPFL | 2019

- *"Privacy-Preserving Statistics on Medical Data Using Homomorphic Encryption"*, J. Stephan at Swisscom, Switzerland.
- *"Efficient Privacy-Preserving Neural Network Inference for Heart Arrhythmia Detection"*, P. Chervet at CSEM, Switzerland.

Semester Projects Supervision EPFL | 2017-2021

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

Teaching Assistant EPFL | 2017-2021

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

Academic Service & Reviewer Activities

Member of the program committee or the editorial board for:

RECOMB-PRIEQ 2024

International Society for Molecular Biology (ISMB) 2024

Reviewer (or sub-reviewer) for:

IEEE S&P | 2023-present

PLOS Genetics | 2023-present

Nature Communications | 2023-present

Genome Research | 2023-present

Recomb | 2023-present

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

Software Projects

SF-GWAS

https://github.com/hhcho/sfgwas | 2022 - present

Software for secure and federated genome-wide association studies. Combines multiparty homomorphic encryption and secure multiparty computation to efficiently perform complex linear algebra operations on encrypted matrices, thus enabling the secure implementation of complex federated genomic analysis. Main language: Golang.

U.S. PETS Prize Challenge

https://github.com/hhcho/muscat | 2023

Software for our team's (MusCAT) solution to the U.S. PETs Prize Challenge (Pandemic Forecasting). Multi-scale federated system for privacy-preserving pandemic risk prediction combining homomorphic encryption (using Golang) and differential privacy (using Python) in the *flower* python framework.

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 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.

Recreation

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