David Froelicher

4th year Ph.D. candidate at EPFL

EPFL IC IINFCOM LDS
BC 254 (Bâtiment BC)
Station 14
CH-1015 Lausanne
Switzerland

David.froelicher@epfl.ch
www.davidfroelicher.com
https://people.epfl.ch/david.froelicher
https://github.com/froelich
+41 79 704 16 28

Summary

- **4th year Ph.D. candidate at EPFL**
- **Passionate researcher in decentralized systems, applied crypto and privacy-enhancing technologies.**
- **Languages: English (full proficiency); French (mother tongue); German: B1**
- **Good programming skills (GoLang, Java, C++, C, Python, Scala, Latex)**

Experience

2016 - Today	**PHD at EPFL, Lausanne, Switzerland** *Laboratory for data security (LDS) and Decentralized and Distributed Systems Lab (DeDiS)*
2016	**Research Assistant at EPFL, Lausanne, Switzerland** *Laboratory for data security (LDS)*
2015-2016	**Master Thesis in NEC Laboratories Europe, Heidelberg, Germany** *Analysis of Security Primitives for Public Clouds. Implementing Proofs of Retrievability in Deduplicated Storage Systems.*
2014	**Peer-to-peer infrastructure with a Map Reduce API** *Implement a peer-to-peer network in order to use it without configuration to do Map Reduce computations.*
2013-2014	**Master project at EPFL :** *In collaboration with an History Museum, we had to implement a database (MySQL) and display the results on Google Earth. We were then able to move and select on the map by using a Kinect in order to show the result. We used Google Earth API and Kinect API.*

Formation

2014 - 2016	**Ecole Polytechnique Fédérale de Lausanne,** Master of engineering in communication systems specialised in IT security.
2010 - 2014	**Ecole Polytechnique Fédérale de Lausanne**, Bachelor of engineering in communication systems
2007 - 2010	**Gymnase de Morges**, Certificat de maturité (with advanced maths)
1998 – 2007	**Collège d'Aubonne** , Certificat études secondaire

Main Projects

2018 – Today	**DPPH: Data Protection in Personalized Health** funded by the Strategic Focus Area Personalized Health and Related Technologies (PHRT) of the ETH Board. 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 *Budget:* CHF 3M
2019 - Today	**MedCo: Enabling the Secure and Privacy-Preserving Exploration of Distributed Clinical and *Omics Cohorts in the Swiss Personalized Health Network** funded by the Swiss Personalized Health and Related Technologies strategic focus area and the Swiss Personalized Health Network. This project aims at testing and deploying in operational environments secure and privacy-conscious cohort explorers dealing with distributed clinical and *omics data. *Budget*: CHF 0,5 M

Other Activities

2018 - Today	**External Reviewer for Privacy Enhancing Technologies Symposium 2019**
2018 - Today	**Reviewer for Digital Signal Processing Journal**
2017 - Today	**Reviewer for EURASIP Journal on Information Security**
2015	**Reviewer for the ICISSP conference 2016** *International Conference on Information Systems Security and Privacy (www.icissp.org)*

Publications List

2019 — **David Froelicher**, Juan Ramón Troncoso-Pastoriza, Joao Sa Sousa, Jean-Pierre Hubaux. Drynx: Decentralized, Secure, Verifiable System for Statistical Queries and Machine Learning on Distributed Datasets. Submitted to IEEE. Trans. on Information Forensics and Security, 2019. https://arxiv.org/abs/1902.03785

2017 — **David Froelicher,** Patricia Egger, Joao Sa Sousa, Jean Louis Raisaro, Zhicong Huang, Christian Mouchet, Bryan Ford, and Jean-Pierre Hubaux. Unlynx: a decentralized system for privacy-conscious data sharing. Proceedings on Privacy Enhancing Technologies, 2017(4):232– 250, 2017.

2017 — Frederik Armknecht, Jens-Matthias Bohli, **David Froelicher** and Ghassan 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.

Talks

2019 — Presentation of runner-up solution at iDash Privacy & Security Workshop – Secure Genome Analysis Competition 2019. Track II: Secure Genotype Imputation using Homomorphic Encryption

2019 — Short presentation of research interest
https://portal.klewel.com/watch/webcast/epfl-ic-research-day-2019/talk/QaZfKsX6MjKKAX9zBgWWwV/

2017 — Presentation of UnLynx at the Privacy Enhancing Technologies Conference in Minneapolis, USA, 2017.
https://www.youtube.com/watch?v=UBXz8XghrjI&index=28&list=PLWSQygNuIsPf349Bl-ls2T3EelyJA9DS5

Software Projects

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

Lattigo library: https://github.com/ldsec/lattigo Lattice-based homomorphic encryption library implementing centralized and distributed versions of BFV and CKKS. Developed in Golang at the LDS group, EPFL, Switzerland.

MedCo: Enabling Privacy-Conscious Exploration of Distributed Clinical and Genomic Data.
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. Developed at the LDS group, EPFL, Switzerland.

Drynx library: https://github.com/ldsec/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 at the LDS group, EPFL, Switzerland.

Unlynx library: https://github.com/ldsec/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.

Teaching Experience

2019 — Co-supervisor of 2 Master Theses at EPFL:
- John Stephan (internship at Swisscom, Switzerland), "Privacy-Preserving Statistics on Medical Data Using Homomorphic Encryption".
- Philipp Chervet, (internship at CSEM, Switzerland), "Efficient Privacy-Preserving Neural Network Inference for Heart Arrhythmia Detection".

2017-2019 — Supervision of 7 semester projects and doctoral semester projects and 1 summer internships at EPFL.
Teaching assistant for:
- Mobile network (master course at EPFL)
- Information security and privacy (master course at EPFL)
- Advanced topics on privacy enhancing technologies (master course at EPFL)
- Introduction to object-oriented programming (bachelor course at EPFL)

Recreation

Cycling, football, tennis, badminton, squash, uni-hockey, ski, guitar, travel, reading, TV shows