Alexander Viand

Address: ETH Zurich
Applied Cryptography Group
CNB H 106
Universitätstrasse 6
8902 Zurich
Phone: +41 44 632 02 73
email: alexander.viand@inf.ethz.ch
website: viand.ch

Research Interests

I am interested in useable security and privacy, privacy enhancing technologies, and the interactions between these technologies and society.

In my research, I work with secure computation technologies including Fully Homomorphic Encryption, Secure Multi-Party Computation and Zero-Knowledge Proofs. I am trying to make these techniques more accessible to non-experts by developing new systems, tools and abstractions.

Education

Current **ETH Zurich**, Doctoral Student in Computer Science
May 2017 *Thesis advisors:* Prof. Dr. Kenneth Paterson, Dr. Anwar Hithnawi

September 2014 **ETH Zurich**, Master of Science in Computer Science
– March 2017 *Master Thesis: "Privacy-preserving Cloud Computation using FHE"*

September 2011 **ETH Zurich**, Bachelor of Science in Computer Science
– September 2014 *Master Thesis: "Distributed Fail-Safe Monitoring"*

Work Experience

Current | **ETH Zurich, Applied Cryptography Group**
Since May 2017 | Doctoral Student and Research Assistant

August 2021 | **Intel**
– January 2022 | Research Internship | "Fully Homomorphic Encryption Engineer"

2013 – 2016 | **ETH Zurich, Chair of Information Technology and Education**
Teaching Assistant | *Course:* "Theoretical Computer Science"

2014 | **ETH Zurich, Chair of Programming Methodology**
Teaching Assistant | *Course:* "Formal Methods and Functional Programming"

2012 – 2013 | **Ausbildungs- und Beratungszentrum für Informatikunterricht**
Teaching Assistant for "Programming for Children (LOGO)" courses.

Publications

- Alberto Ibarrondo and **Alexander Viand**
  Pyfhel: PYthon For Homomorphic Encryption Libraries
  9th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC '21). Online, November 2021
- Travis Morrison, Bijeeta Pal, Sarah Scheffler, **Alexander Viand** (alphabetical order)
  Private Outsourced Translation for Medical Data
  In "Protecting Privacy through Homomorphic Encryption", K. Lauter, W. Dai, K. Laine, editors, Springer, 2021
- Lukas Burkhalter*, Nicolas Küchler*, **Alexander Viand**, Hossein Shafagh, Anwar Hithnawi
  Zeph: Cryptographic Enforcement of End-to-End Data Privacy
  15th USENIX Symposium on Operating Systems Design and Implementation (OSDI '21). Online, July 2021
- **Alexander Viand**, Patrick Jattke and Anwar Hithnawi
  SoK: Fully Homomorphic Encryption Compilers
  42nd IEEE Symposium on Security and Privacy (SP '21). Online, May 2021
- Lukas Burkhalter, Anwar Hithnawi, **Alexander Viand**, Hossein Shafagh and Sylvia Ratnasamy
  TimeCrypt: Encrypted Data Stream Processing at Scale with Cryptographic Access Control
  17th USENIX Symposium on Networked Systems Design and Implementation (NSDI '20). Santa Clara, CA, February 2020.
- Lukas Burkhalter, **Alexander Viand**, Anwar Hithnawi and Hossein Shafagh.
  Robust Secure Aggregation for Privacy-Preserving Federated Learning with Adversaries
  Workshop on Privacy-Preserving Machine Learning (PPML '19). London, Great Britain, November 2019
- **Alexander Viand** and Hossein Shafagh
  Marble: Making Fully Homomorphic Encryption Accessible to All
  6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC '18). Toronto, Canada, October 2018

Professional Activities

- Reviewer | *29th World Wide Web Conference (WWW '20). Tapei, Taiwain, April 2020.*
- President | *Scientific Staff Association at the Department of Computer Science at ETH Zurich, 2018-2021.*

Supervised Students

- Moritz Winger | *MSc Thesis "Automated Hybrid Parameter Selection & Circuit Analysis for FHE", 2021.*
- Fabio Bertschi | *BSc Thesis "Private ML as a Service for Natural Language Processing", 2021.*
- Patrick Jattke | *MSc Thesis "Advanced Optimization Strategies for the Marble FHE Compiler", 2020.*
- Ulla Aeschbacher | *MSc Thesis "An Accessible High-Level Language for Advanced Cryptography", 2020.*
- Mario Stöckli | *BSc Thesis "Improving the Marble Fully Homomorphic Encryption Framework", 2019.*
- M. Niederberger | *MSc Thesis "Variational Autoencoder KnowledgeTransfer", 2019.*
- Alexandre Connat | *MSc Thesis "Differentially Private Decentralized Machine Learning Framework", 2019.*
- Pascal Schärli | *BSc Project "Re:Versi - Move Analysis for Reversi", 2018.*

Languages

German: Native
English: Fluent (ILR Level 4+)