Anwar Hithnawi

hithnawi@inf.ethz.ch pps-lab.com

Research Interests

Data Privacy, Privacy-Preserving Systems, Secure Computation, Applied Cryptography, Systems Security

Academic Appointments

Research Group Leader (PI), Computer Science Department, ETH Zurich 2020 –Present
Postdoctoral Researcher, EECS, UC Berkeley 2017 – 2019

Education

Ph.D. in Computer Science, ETH Zurich, Switzerland 2017
M.Sc. in Computer Science, RWTH Aachen University, Germany 2011
B.Eng. in Computer Systems Engineering, Birzeit University, Palestine 2008

Honors, Awards, & Major Grants

Since assuming the role of PI in 2020, I have secured grants and awards totaling **$ 1.685 million** in funding.

- Google Research Award, **Sole PI**, Funding: **75K $** 2023
  Title: "Unified Compiler Design for Polynomial and Non-Polynomial FHE"
- Rising Stars in EECS 2021
- Facebook Research Award, **Sole PI**, Funding: **100K $** 2021
  Title: "Cryptographic Enforcement of End-to-End Data Privacy"
- SRC Hardware Security Solicitation Research Grant, **Sole PI**, Funding: **270K $** 2021
  Title: "Compiler Designs for Fully Homomorphic Encryption"
- ETH Research Grant, **Sole PI**, Funding: **240K $** 2021
  Title: "Cryptographic Enforcement for End-to-End Data Privacy"
- SNSF Ambizione Grant, **Sole PI**, Funding: **1M $** 2020
  Title: "Secure and Robust Federated Learning"
- SNSF Postdoctoral Fellowship 2017
- N2Women Young Researcher Fellowship 2014
- Google Anita Borg Scholarship 2011
- DAAD Scholarship for Master's Studies 2009
- Google Research Award. Funding: **30K $** 2009
  I co-authored with PI Prof. Yahya a proposal based on my bachelor thesis that received this award.

Publications

Refereed Conference Publications

[1] **Cohere: Managing Differential Privacy in Large Scale Systems**
pdf *Nicolas Küchler, Emanuel Opel, Hidde Lycklama, Alexander Viand, Anwar Hithnawi*
IEEE S&P (Oakland) 2024

[2] **RoFL: Robustness of Secure Federated Learning**
pdf *Hidde Lycklama*, Lukas Burkhalter*, Alexander Viand, Nicolas Küchler, Anwar Hithnawi*
IEEE S&P (Oakland) 2023

[3] **HECO: Fully Homomorphic Encryption Compiler**
pdf *Alexander Viand, Patrick Jattke, Miro Haller, Anwar Hithnawi*
USENIX Security 2023

[4] **VF-PS: How to Select Important Participants in Vertical Federated Learning, Efficiently and Securely?**
pdf *Jiawei Jiang, Lukas Burkhalter, Fangcheng Fu, Bolin Ding, Bo Du, Anwar Hithnawi, Bo Li, Ce Zhang*
NeurIPS 2022, (**Spotlight**).

[5] **Zeph: Cryptographic Enforcement of End-to-End Data Privacy**
pdf *Lukas Burkhalter*, Nicolas Küchler*, Alexander Viand, Hossein Shafagh, Anwar Hithnawi*
USENIX OSDI 2021

[6] **SoK: Fully Homomorphic Encryption Compilers**
pdf *Alexander Viand, Patrick Jattke, Anwar Hithnawi*
IEEE S&P (Oakland) 2021

[7] **Droplet: Decentralized Authorization and Access Control for Encrypted Data Streams**
pdf *Hossein Shafagh, Lukas Burkhalter, Sylvia Ratnasamy, Anwar Hithnawi*
USENIX Security 2020

[8] **TimeCrypt: Encrypted Data Stream Processing at Scale with Cryptographic Access Control**
pdf *Lukas Burkhalter, Anwar Hithnawi, Alexander Viand, Hossein Shafagh, Sylvia Ratnasamy*
USENIX NSDI 2020

[9] **Secure Sharing of Partial Homomorphic Encrypted IoT Data**
pdf *Hossein Shafagh, Anwar Hithnawi, Lukas Burkhalter, Pascal Fischli, Simon Duquennoy*
ACM SenSys 2017

[10] **CrossZig: Combating Cross-Technology Interference in Low-power Wireless Networks**
pdf *Anwar Hithnawi, Su Li, Hossein Shafagh, James Gross, Simon Duquennoy*
ACM IPSN 2016

[11] **Talos: Encrypted Query Processing for the Internet of Things**
pdf *Hossein Shafagh, Anwar Hithnawi, Andreas Dröscher, Simon Duquennoy, Wen Hu*
ACM SenSys 2015

[12] **TIIM: Technology-Independent Interference Mitigation for Low-power Wireless Networks**
pdf *Anwar Hithnawi, Hossein Shafagh, Simon Duquennoy*
ACM IPSN 2015

[13] **A Receiver-Based 802.11 Rate Adaptation Scheme with On-Demand Feedback**
pdf *Florian Schmidt, Anwar Hithnawi, Oscar Punal, Jamess Gross, Klaus Wehrle*
IEEE PIMRC 2012

Pre-prints

[14] **A Critical Analysis of FHE Integrity Approaches**
pdf *Alexander Viand*, Christian Knabenhans*, Anwar Hithnawi*

[15] **Verifiable Fully Homomorphic Encryption**
pdf *Alexander Viand*, Christian Knabenhans*, Anwar Hithnawi*

[16] **Holding Secrets Accountable: Auditing Private Machine Learning Algorithms**
pdf *Hidde Lycklama, Nicolas Küchler, Alexander Viand, Anwar Hithnawi*

[17] **CoVault: Secure Selective Analytics of Sensitive Data for the Public Good**
pdf *Roberta De Viti, Isaac Sheff , Noemi Glaeser,Baltasar Dinis, Rodrigo Rodrigues, Jonathan Katz, Bobby Bhattacharjee, Anwar Hithnawi, Deepak Garg, Peter Druschel*

Refereed Workshop Publications

[18] **Bridging the Gap between Privacy Incidents and PETs**
pdf *Shannon Veitch, Lena Csomor, Alexander Viand, Anwar Hithnawi, Bailey Kacsmar*
HotPETs 2023, (**Best Talk Award**).

[19] **Robust Secure Aggregation for Privacy-Preserving Federated Learning with Adversaries**
pdf *Hidde Lycklama, Nicolas Küchler, Alexander Viand, Emanuel Opel, Lukas Burkhalter, Anwar Hithnawi*
ML Safety Workshop at NeurIPS 2022

[20] **Robust Secure Aggregation for Privacy-Preserving Federated Learning with Adversaries**
pdf *Lukas Burkhalter, Alexander Viand, Matthias Lei, Hossein Shafagh, Anwar Hithnawi*
Privacy Preserving Machine Learning Workshop 2019

[21] **Towards Blockchain-based Auditable Storage and Sharing of IoT Data**
pdf *Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, Simon Duquennoy*
ACM Cloud Computing Security Workshop 2017

[22] **Privacy-preserving Quantified Self: Encrypted Sharing & Processing of Encrypted Small Data**
pdf *Hossein Shafagh, Anwar Hithnawi*
ACM MobiArch Workshop 2017

[23] **Controlled Interference Generation for Wireless Coexistence Research**
pdf *Anwar Hithnawi, Vaibhav Kulkarni, Su Li, Hossein Shafagh*
Software Radio Implementation Forum 2015

[24] **Understanding the Impact of Cross Technology Interference on IEEE 802.15.4**
pdf *Anwar Hithnawi, Hossein Shafagh, Simon Duquennoy*
ACM WiNTECH Workshop 2014

Invited Talks

- Security and Robustness of Collaborative Learning Systems, **UC Berkeley** 2023
- Security and Robustness of Collaborative Learning Systems, **MLSys Workshop on CL** 2023
- Security and Robustness of Collaborative Learning Systems, **ZISC Seminar** 2023
- Security and Robustness of Collaborative Learning Systems, **University St.Gallen** 2023
- Useable Fully Homomorphic Encryption: Opportunities & Challenges, **Intel Labs** 2022
- Security and Robustness of Collaborative Learning Systems, **FLOW Research Seminar** 2022
- Security and Robustness of Collaborative Learning Systems, **MBZUAI Workshop on CL** 2022
- Systems Designs for End-to-End Privacy, **Meta Labs** 2022
- Systems Designs for End-to-End Privacy, **Columbia University** 2022
- Systems Designs for End-to-End Privacy, **CISPA** 2022
- Systems Designs for End-to-End Privacy, **Max Planck** 2022
- Cryptographic Enforcement of End-to-End Data Privacy, **Brown University** 2021
- Cryptographic Enforcement of End-to-End Data Privacy, **University of Wisconsin-Madison** 2021
- Compiler Design for Fully Homomorphic Encryption, **Intel Labs** 2021
- Encrypted Data Stream Processing at Scale, **UC Berkeley** 2019
- Encrypted Data Stream Processing at Scale, **VMware Research** 2019
- Encrypted Data Stream Processing at Scale, **Intel Labs** 2019

Advising

Ph.D. Students:

- Nicolas Küchler 2020-present
- Hidde Lycklama 2021-present
- Lukas Burkhalter (now Cryptography Engineer at Proton) 2018-2022
  Thesis: Privacy-Centric Systems for Stream Data Processing
  Committee: Anwar Hithnawi (ETH), Kenny Paterson (ETH), Peter Druschel (MPI-SWS), Srdjan Capkun (ETH)
  🏆 Microsoft Research Ph.D. Award
- Alexander Viand (now Cryptography Researcher at Intel Labs) 2019-2023
  Thesis: Useable Fully Homomorphic Encryption
  Committee: Anwar Hithnawi (ETH), Kenny Paterson (ETH), Raluca Ada Popa (UC Berkeley)

Master's and Undergraduate Students:

- Emanuel Opel 2021-present
- Isha Gupta 2022-present

- Yu-Shan Wei 2023-present
- Christian Knabenhans (now Ph.D. student at EPFL) 2022-2023
- Miro Haller (now Ph.D. student at UCSD) 2022
- Lena Csomor (now CS High School Teacher at Kantonsschule Zurcher) 2022
- Patrick Jattke (now Ph.D. student at ETH Zurich) 2020
- Nicolas Küchler (now Ph.D. student at ETH Zurich) 2020
- Hidde Lycklama (now Ph.D. student at ETH Zurich) 2020
- Yonathan Fisseha (now Ph.D. student at the University of Michigan) 2019
- Liangcheng Yu (now Ph.D. student at the University of Pennsylvania) 2017
  🏆 Thesis Awarded ZKS Grant
- Matthias Lei (now Senior Consultant at Innovation Process Technology) 2016
- Michel Kaporin (now Software Engineer at ti&m) 2016
- Lukas Burkhalter (now Ph.D. student at ETH Zurich) 2016
  🏆 Thesis Awarded ETH Medal
- Dominic Plangger (now Lead Engineer at xorlab) 2015
- Su Li (now Ph.D. student at EPFL) 2014
- Vaibhav Kulkarni (now Ph.D. student at the University of Lausanne) 2014
  🏆 Thesis Awarded ZKS Grant

Software and Adoption

- **HECO**: https://github.com/MarbleHE/HECO
  Intel adopted HECO for its upcoming FHE accelerator. **Google** is currently actively involved in our efforts to standardize intermediate representations (IRs) across the FHE community and is transitioning its compiler to an MLIR-based one following the HECO architecture.
- **Zeph**: https://github.com/pps-lab/zeph-artifact
- **RoFL**: https://github.com/pps-lab/rofl-project-code
- **Cohere**: https://github.com/pps-lab/privacy-management
- **Droplet**: https://github.com/dropletchain/droplet-engine
- **TimeCrypt**: https://github.com/TimeCrypt/timecrypt
- **FHE Compilers**: https://github.com/MarbleHE/SoK
- **Verifiable FHE**: https://github.com/zkFHE/

Teaching

Co-Instructor, Seminar on Systems Security Spring 2023

Teaching Assistant:

- Informatics II for Electrical Engineers Spring 2013, 2014, 2015, 2016, 2017
- Ubiquitous Computing Seminar Spring 2014, 2015
- Ubiquitous Computing Spring 2014
- Distributed Systems Fall 2012, 2015

Outreach

- Mentor, Network of Women in CS (CSNOW) Mentoring Program, ETH Zurich. 2021
- Invited Panelist, Panel for Woman in Computer Science, ETH Zurich. 2017
- Organization Committee and Mentor, Discovery Semester for Refugees, ETH Zurich. 2017
- Scholarship Applications Reviewer, Grace Hopper Celebration of Women in Computing. 2016
- N2Women Board Member, Co-chair N2Women Mentoring Program. 2015
- Organizer of the N2Women Event at ACM MobiCom. 2014

Service

- Publication Chair: ACM IPSN'15
- Program Committee: Middleware'23, IEEE Internet of Safe Things'20, Shadow ACM IPSN'15
- Reviewer: Communications of the ACM'22, ACM Transactions on Privacy and Security'20, ACM HotNets'19, ACM MSWiM'16, Elsevier ComCom'14, IEEE LCN'14, WoT'13.
- Conference Organization: Chair for Demos and Posters of UbiComp'13, Chair of the Design Exhibition of ISWC'13

Languages

English, Arabic, German