Wenting Zheng

Curriculum Vitae

wenting@cmu.edu
wzheng.github.io

Interests

Computer systems security, applied cryptography

Current positions

2021–Present	**Assistant Professor**, *Carnegie Mellon University*, Pittsburgh, PA.
2021–Present	**Co-Founder and Chief Scientist**, *Opaque Systems*, San Francisco, CA.

Education

2014–2020	**Ph.D.**, *University of California, Berkeley*, Berkeley, CA. Advisors: Raluca Ada Popa and Ion Stoica
2013–2014	**Masters of Engineering**, *Massachusetts Institute of Technology*, Cambridge, MA. Advisor: Barbara Liskov
2009–2013	**Bachelor of Science**, *Massachusetts Institute of Technology*, Cambridge, MA. Electrical Engineering and Computer Science

Awards

2023	**Google Research Scholar**.
2023	**NSF CAREER**.
2022	**IEEE Euro S&P 2022 Distinguished Paper Award**.
2019	**Invited Participant to EECS Rising Stars Workshop**.
2017-2018	**IBM Ph.D. Fellowship**.
2014-2016	**Berkeley Fellowship**.

Publications

ADI: Adversarial Dominating Inputs in Vertical Federated Learning Systems.
Qi Pang, Yuanyuan Yuan, Shuai Wang, Wenting Zheng
To appear, IEEE S&P 2023

Silph: A Framework for Scalable and Accurate Generation of Hybrid MPC Protocols.
Edward Chen, Jinhao Zhu, Alex Ozdemir, Fraser Brown, Riad Wahby, Wenting Zheng.
To appear, IEEE S&P 2023

CostCO: An Automatic Cost Modeling Framework for Secure Multi-Party Computation.
Vivian Fang, Lloyd Brown, William Lin, Wenting Zheng, Aurojit Panda, Raluca Ada Popa.
IEEE Euro S&P 2022

Cerebro: A Platform for Multi-Party Cryptographic Collaborative Learning.
Wenting Zheng, Ryan Deng, Weikeng Chen, Raluca Ada Popa, Aurojit Panda, Ion Stoica.
USENIX Security 2021

Delphi: A Cryptographic Inference Service for Neural Networks.
Pratyush Mishra, Ryan Lehmkuhl, Akshayaram Srinivasan, Wenting Zheng, Raluca Ada Popa.
USENIX Security 2020

Helen: Maliciously Secure Coopetitive Learning for Linear Models.
Wenting Zheng, Raluca Ada Popa, Joseph E. Gonzalez, Ion Stoica.
IEEE S&P 2019

DIZK: Distributing Zero Knowledge Proof Systems.
Howard Wu, Wenting Zheng, Alessandro Chiesa, Raluca Ada Popa, Ion Stoica.
USENIX Security 2018

High Accuracy Approximation of Secure Multiparty Neural Network Training.
Daniel Ho, Xin Wang, Wenting Zheng, Joseph Gonzalez, Raluca Ada Popa, and Ion Stoica.
AISys 2017

MiniCrypt: Reconciling Encryption and Compression for Big Data Stores.
Wenting Zheng, Frank Li, Raluca Ada Popa, Ion Stoica, Rachit Agarwal.
EuroSys 2017

Opaque: An Oblivious and Encrypted Distributed Analytics Platform.
Wenting Zheng, Ankur Dave, Jethro Beekman, Raluca Ada Popa, Joseph Gonzalez, Ion Stoica.
NSDI 2017

SCL: Simplfying Distributed SDN Control Planes.
Aurojit Panda, Wenting Zheng, Xiaohe Hu, Arvind Krishnamurthy, Scott Shenker.
NSDI 2017

Fast Databases with Fast Durability and Recovery through Multicore Parallelism.
Wenting Zheng, Stephen Tu, Eddie Kohler, Barbara Liskov.
OSDI 2014

Speedy Transactions in Multicore In-Memory Databases.
Stephen Tu, Wenting Zheng, Eddie Kohler, Barbara Liskov, Samuel Madden.
SOSP 2013

Theses

Sharing without Showing: Building Secure Collaborative Systems.
Wenting Zheng.
Ph.D. dissertation, 2020

Fast Checkpoint and Recovery Techniques for an In-Memory Database.
Wenting Zheng.
M.Eng. thesis, 2014

Selected Talks

March 2022 **Sharing without Showing: Building Systems for Secure Collaborative Computation**.
Samsung Forum

August 2019 **Helen: Maliciously Secure Coopetitive Learning for Linear Models**.
PPML Workshop, CRYPTO

May 2019 **Sharing without Showing: Enabling Secure Collaborative Learning via Cryptography**.
Workshop on Inference for Multi-Messenger Astrophysics

May 2019 **Helen: Maliciously Secure Coopetitive Learning for Linear Models**.
IEEE S&P 2019

May 2019 **Helen: Maliciously Secure Multi-Party Training**.
Bay Are Crypto Day

April 2018 **Opaque: An Oblivious and Encrypted Distributed Analytics Platform**.
Stanford University Networking Seminar

October 2017 **Opaque: An Oblivious and Encrypted Distributed Analytics Platform**.
Yahoo Research

August 2017 **Opaque: An Oblivious and Encrypted Distributed Analytics Platform**.
Intel-NSF CPS Security Workshop

May 2017 **MiniCrypt: Reconciling Encryption and Compression for Big Data Stores**.
EuroSys 2017

April 2017 **Opaque: An Oblivious and Encrypted Distributed Analytics Platform**.
NSDI 2017

February 2017 **Opaque: A Data Analytics Platform with Strong Security**.
Spark Summit

October 2014 **Fast Databases with Fast Durability and Recovery Through Multicore Parallelism**.
AMP Lab Cloud Seminar

October 2014 **Fast Databases with Fast Durability and Recovery Through Multicore Parallelism**.
OSDI 2014

Professional activities

PC member, *NSDI 2024.*

PC member, *CCS 2023.*

PC member, *USENIX Security 2022.*

PC member, *SysTEX 2022*.

PC member, *NSDI 2022*.

PC member, *OSDI 2021*.

PC member, *MLSys 2021*.

External reviewer, *HotNets 2019*.

External reviewer, *PoPETS 2019*.

Outreach

2019-2020 **Co-Founder and Organizer**, *Diversifying Access to Research in Engineering (DARE)*.
DARE (dare.berkeley.edu) is a UC Berkeley program created to match undergraduate students with research opportunities in electrical engineering and/or computer science. We place a heavy emphasis on outreach to diversity and under-represented applicants. DARE's goal is to make EECS research more readily accessible and encourage diversity within the department.

Open-Source Software

Opaque: An Encrypted Analytics System.
github.com/ucbrise/opaque
Overview: Opaque is a package for Apache Spark SQL that enables encryption for DataFrames using Intel SGX trusted hardware. The aim is to enable analytics on sensitive data in an untrusted cloud. Once the contents of a DataFrame are encrypted, subsequent operations will run within SGX enclaves. This software is based on the NSDI 2017 paper of the same name.
Impact: IBM Research deployed Opaque, and Ericsson and Alibaba used Opaque for internal use cases. Microsoft is contributing to our open source effort. Currently, Microsoft's Azure Confidential Computing and Scotiabank have a contract to deploy anti-money laundering on top of Opaque and a secure learning project from the RISELab.

DIZK.
github.com/scipr-lab/dizk
Overview: DIZK is a Java library for distributed zero knowledge proof systems. The library implements distributed polynomial evaluation/interpolation, computation of Lagrange polynomials, and multi-scalar multiplication. Using these scalable arithmetic subroutines, the library provides a distributed zkSNARK proof system that enables verifiable computations of up to billions of logical gates, far exceeding the scale of previous state-of-the-art solutions.
Impact: Gnosis, a blockchain company, announced that they are planning to use DIZK to build a decentralized scalable on-chain exchange.