Weikeng Chen

Ph.D. candidate in EECS, UC Berkeley, expected to graduate in Spring 2022

Personal Information

EMAIL: weikengchen@berkeley.edu
GITHUB: @weikengchen

Education

2017- PhD student at UC Berkeley (GPA 4.0 / 4.0),
expected graduation: Spring 2022,
Advisor: Prof. Raluca Ada Popa.

2017-2019 Master of Science in Computer Science, UC Berkeley.

2013-2017 Honor Bachelor in Engineering in Information Security, USTC, China,
with GPA 3.99 / 4.3 (ranked 1 out of ≈ 300 students)
with *summa cum laude*, Guomoruo Scholarship
and National Information Security Scholarship.

Related experience

My work can be separated into two aspects: (1) designs of cryptographic algorithms and protocols for real-world applications and (2) efficient implementations of these protocols.

Implementations and applications for zero-knowledge proofs (ZKP).

My project on reducing participation costs in blockchain system consists of significant contributions to the implementations of zero-knowledge proofs protocols.

In my project on recursive ledger (in submission), we implement recursive ZKP protocols for a large family of recent primitives, as well as develop a platform that can are general enough to express more recent primitives that are based on different techniques. Our work is written in Rust.

One of my ongoing projects involve the use of recent works QuickSilver and Virgo, two most efficient ZKP systems today. We have made some improvements in Virgo.

Platforms and applications for secure multiparty computation (MPC).

I have several projects that build applications using MPC: (1) N-for-1-Auth (in submission) for usable distributed authentication, (2) Cerebro (USENIX Security '21) for secure collaborative learning, and (3) Metal (NDSS '20) for metadata-hiding storage.

I am familiar with the common protocols in secure computation, both the ones based on garbled circuits (i.e., Yao's protocol) and the ones based on the SPDZ protocol. In addition, we made improvements to these tools for many real-world settings, both in the algorithm perspective and in the implementation perspective.

Efficient implementations of cryptographic algorithms.

These projects make contributions to the open-source MPC and ZKP platforms.

(1) In N-for-1-Auth we assemble garbled circuits for more efficient AES implementations and for many TLS functionalities (GitHub repo: n-for-1-auth/circuits), and improve the state-of-the-art MPC platform to support many different inputs and outputs, which are quite novel and are needed for deployment (GitHub repo: n-for-1-auth/emp-agmpc-flex-in-out).

(2) In recursive ledger we implement a constraint system for a modern ZKP protocol, Marlin, and our techniques are general enough to support other ZKP protocol in the similar region. The code is in the following repos written in Rust: arkworks-rs/pcd and arkworks-rs/ivls. I am also a core member of the ZKP platform, arkworks-rs.

(3) In Cerebro (USENIX Security '21) we implement many optimizations for collaborative learning. Our code has been open-sourced as part of the MC2 platform mc2-project. Our specific contributions are in our forks of SCALE-MAMBA and MP-SPDZ.

(4) In Metal (NDSS '20) I implement a very new encryption algorithm that is extremely fast and has many nice properties. This website summarizes our open-source efforts: oblivious.app code is open-sourced: . In addition, I also optimize a MPC platform, obliv-c, to support TLS encryption and more secure Yao's protocol.

Skills

Coding: an extensive use of Rust, C++/C.

Cryptography: familiar with algorithms and their implementations related to MPC and ZKP (e.g., modern OT, modern garbling) and with elliptic curves (e.g., computation-efficient curves like Ristretto, pairing-friendly curves).

Publication

- N-for-1 Auth: N-wise Decentralized Authentication via One Authentication.
  Weikeng Chen, Ryan Deng, and Raluca Ada Popa.
  In submission to S&P 2022.
  IACR ePrint 2021/342.
- Reducing Participation Costs via Incremental Verification for Ledger Systems.
  Weikeng Chen, Alessandro Chiesa, Emma Dauterman, and Nicholas P. Ward.
  (The author list is alphabetically ordered.)
  In submission to CRYPTO 2021.
  IACR ePrint 2020/1522.
- Cerebro: A Platform for Multi-Party Cryptographic Collaborative Learning.
  Wenting Zheng, Ryan Deng, Weikeng Chen, Raluca Ada Popa, Aurojit Panda, and Ion Stoica.
  USENIX Security 2021 (USENIX Security Symposium).
- Metal: A Metadata-Hiding File-Sharing System.
  Weikeng Chen and Raluca Ada Popa.
  NDSS 2020 (Network and Distributed System Security Symposium).
  IACR ePrint 2020/083.
  Technical Report UCB/EECS-2020-11, UC Berkeley.
- Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage.
  Kaiping Xue, Weikeng Chen, Wei Li, Jianan Hong, and Peilin Hong.
  TIFS 2018 (IEEE Transactions on Information Forensics and Security).
- TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud.
  Jianan Hong, Kaiping Xue, Yingjie Xue, Weikeng Chen, David S. L. Wei, Nenghai Yu, and Peilin Hong.
  TSC 2017 (IEEE Transactions on Services Computing).
- Exploring a Service-Based Normal Behaviour Profiling System for Botnet Detection.
  Weikeng Chen, Xiao Luo, and A. Nur Zincir-Heywood.

AnNet 2017 (IEEE/IFIP International Workshop on Analytics for Network and Service Management).

- A Privacy-Preserving and Real-Time Traceable Power Request Scheme for Smart Grid.
  Qingyou Yang, Jianan Hong, Kaiping Xue, Weikeng Chen, Xiang Zhang, and Hao Yue.
  ICC 2017 (IEEE International Conference on Communications).

Teaching

Spring 2019	Co-head GSI for CS161 Computer Security
Fall 2018	GSI for CS161 Computer Security

Selected Scholarships, Grants, and Awards

Graduate	Berkeley Graduate Division Conference Travel Grant (2020)
	EECS Fellowship Award (2017 - 2018)
	(funded through Jim Gray Fellowship and J. K. Zee Fellowship)
Undergraduate	Guomoruo Scholarship (2016, highest award to undergraduates)
	National Cybersecurity Scholarship for Undergrads (2016)
	National Scholarship (2014)

Talks and Poster Presentations

Metal: A Metadata-Hiding File-Sharing System

- The 26th Network and Distributed System Security Symposium (NDSS 2020).
- RISELab Open House 2018.
- RISELab Retreat Winter 2019, Summer 2018.

UC Berkeley International GSI Teaching Conference Panelist

- Fall 2020, Fall 2019.

Services

Graduate	Member of the Engineering Library Student Committee (2020)
	Graduate Application Student Reviewer (2018)
Undergraduate	President of the Information Security Student Union (2016)
	President of the Information Security Club (2015)