Weikeng Chen

Research Partner, L2 Iterative

PhD, EECS UC Berkeley (2022)

Personal Information

EMAIL: w.k@berkeley.edu
GITHUB: @weikengchen
TWITTER: @weikengchen

To book a time with me: https://calendarbridge.com/book/weikeng

Work Experience

2023- Research Partner of L2 Iterative

We invest in emerging blockchain technologies, in particular infrastructure projects in layer-2 and in zero-knowledge proofs (ZKP). We focus on companies in pre-seed, seed, or series-A stages. My day-to-day work involves research in the broad cryptography + blockchain space and technical due diligence. I am active in the community of ZKP developers and researchers. Our portfolio companies include EigenLayer, Taiko, Eclipse, Sui, Linera, Polyhedra, Primv, and Cedro Finance.

2021-2023 Chief Scientist of Discreet Labs

We work on zero-knowledge proofs for privacy payments like Zcash, with technical innovations in zero-knowledge proof systems: address compatibility (see *"The inspection model for zero-knowledge proofs and efficient Zerocash with secp256k1 keys"*, https://eprint.iacr.org/2022/1079) and TurboPlonk for SNARK-friendly hash function (see *"An efficient verifiable state for zk-EVM and beyond from the Anemoi hash function"*, https://eprint.iacr.org/2022/1487).

We developed highly efficient application-specific PLONK proof system. According to the benchmark (https://github.com/zkspeedtest/), our system is 3.7× more efficient than Zcash Orchard, 8.2× more efficient than Espresso CAPE, 9.5× more efficient than Zcash Sapling, 13× more efficient than Anoma, and 14.7× more efficient than Ironfish.

2021-2023 Co-founder of DZK Labs

I worked on application-specific ZKP and their acceleration (https://bit.ly/delendum-talk-app-specific). We have worked on hardware building blocks for Aleo mining, as shown in area-minimized elliptic curve compute units (in our efabless shuttle project "Thumblina").

DZK has also done research in the more software side, mostly notably, application-specific curves (https://eprint.iacr.org/2022/1145). Our method has been used in the ZK industry: (1) time-lock encryption (https://twitter.com/timoethey/status/1625971627082088459) by ChainSafe (https://chainsafe.io/), which implements many cross-chain bridges and (2) recursion for STARK (https://github.com/hashcloak/Lokum) by HashCloak, going to be implemented in Cairo, for recursing a STARK proof.

Last year, DZK has worked on ZPrize, with Aleo, Polygon, AMD, and Jump Crypto. We are the architect for the MSM FPGA track (https://www.zprize.io/prizes/accelerating-msm-operations-on-gpu-fpga) and the NTT FPGA track (https://www.zprize.io/prizes/accelerating-ntt-operations-on-an-fpga).

Education

2017-2022 Doctor of Philosophy in Computer Science, UC Berkeley
advised by Prof. Raluca Ada Popa, with GPA 4.0 / 4.0

2017-2019 Master of Science in Computer Science, UC Berkeley,
with GPA 4.0 / 4.0.

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 Cybersecurity Scholarship for Undergrads

Publication

At UC Berkeley and after graduation, I did research in zero-knowledge proofs and secure multiparty computation, with a focus of efficient cryptographic implementations.

My advisor is Raluca Ada Popa (https://people.eecs.berkeley.edu/~raluca/, co-founder of Opaque Systems, working on trusted execution environment [TEE] and secure multiparty computation [MPC]).

I also work with Alessandro Chiesa (https://ic-people.epfl.ch/~achiesa/, co-founder of Starkware) on zero-knowledge proofs when he was at UC Berkeley.

- HOLMES: Efficient Distribution Testing for Secure Collaborative Learning
  Ian Chang, Katerina Sotiraki, Weikeng Chen, Murat Kantarcioglu, and Raluca Ada Popa
  USENIX Security 2023
- MPCAuth: Multi-Factor Authentication for Distributed-Trust Systems
  Sijun Tan, Weikeng Chen, Ryan Deng, and Raluca Ada Popa
  IEEE S&P 2023
- An Efficient Verifiable State for zk-EVM and Beyond From the Anemoi Hash Function
  Jianwei Liu, Harshad Patil, Akhil Sai Peddireddy, Kevin Singh, Haifeng Sun, Huachuang Sun, and Weikeng Chen
  IACR ePrint 2022/1487
- Yafa-108/146: Implementing ed25519-Embedding Cocks-Pinch Curves in arkworks-rs
  Rami Akeela and Weikeng Chen
  IACR ePrint 2022/1145
- The Inspection Model for Zero-Knowledge Proofs and Efficient Zerocash with Secp256k1 Keys
  Huachuang Sun, Haifeng Sun, Kevin Singh, Akhil Sai Peddireddy, Harshad Patddil, Jianwei Liu, and Weikeng Chen
  (reverse alphabetical order)
  IACR ePrint 2022/1079
- Reducing Participation Costs via Incremental Verification for Ledger Systems
  Weikeng Chen, Alessandro Chiesa, Emma Dauterman, and Nicholas P. Ward
  (alphabetical order)
  IACR ePrint 2020/1522
- Titanium: A Metadata-Hiding File-Sharing System with Malicious Security
  Weikeng Chen, Thang Hoang, Jorge Guajardo, and Attila A. Yavuz
  NDSS 2022
- 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
  PPML @ CRYPTO 2021

- Metal: A Metadata-Hiding File-Sharing System
  Weikeng Chen and Raluca Ada Popa
  NDSS 2020
- 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
- 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
- Exploring a Service-Based Normal Behaviour Profiling System for Botnet Detection
  Weikeng Chen, Xiao Luo, and A. Nur Zincir-Heywood
  AnNet 2017
- 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