Hao Chung

✉ haochung@andrew.cmu.edu ◇ https://chunghao.github.io

Education

Carnegie Mellon University — Pittsburgh, Pennsylvania, USA
Ph.D. Candidate in Electrical and Computer Engineering — 02/2021 - Present

- Advisor: Elaine Shi
- Research Interests: Mechanism Design, Blockchain, Quantum Cryptography

National Taiwan University — Taipei, Taiwan
M.S. in Electrical Engineering — 09/2016 - 06/2018

- Advisor: Kai-Min Chung and Chen-Mou Cheng (co-advised)
- Thesis: *Analysis and Comparison of Security Proofs of Quantum Key Distribution*

National Taiwan University — Taipei, Taiwan
B.S. in Physics (minor in Philosophy) — 09/2012 - 06/2016

Work Experience

NTT Research — Sunnyvale, California, USA
Research Intern in Cryptography — 05/2023 - 08/2023

- Advisor: Vipul Goyal

Academia Sinica — Taipei, Taiwan
Research Assistant — 09/2019 - 02/2021

- Advisor: Kai-Min Chung

DEXON Foundation — Taipei, Taiwan
Blockchain Researcher — 09/2018 - 05/2019

Publications

[8] **Rapidash: Foundations of Side-Contract-Resilient Fair Exchange**
Hao Chung, Elisaweta Masserova, Elaine Shi, Sri AravindaKrishnan Thyagarajan
In Science of Blockchain Conference (**SBC**), 2024.

[7] **Collusion-Resilience inTtransaction Fee Mechanism Design**
Hao Chung, Tim Roughgarden, Elaine Shi
In ACM Conference on Economics and Computation (**EC**), 2024.

[6] **Maximizing Miner Revenue in Transaction Fee Mechanism Design**
Ke Wu, Elaine Shi, Hao Chung (randomized author order)
In Innovations in Theoretical Computer Science (**ITCS**), 2024.

[5] **What Can Cryptography Do For Decentralized Mechanism Design**
Elaine Shi, Hao Chung, Ke Wu (randomized author order)
In Innovations in Theoretical Computer Science (**ITCS**), 2023.

[4] **Foundations of Transaction Fee Mechanism Design**
Hao Chung, Elaine Shi
In ACM-SIAM Symposium on Discrete Algorithms (**SODA**), 2023.
Best DeFi Papers Award at ACM CCS Workshop on Decentralized Finance and Security (DeFi), 2024.
Also selected for "Highlights Beyond EC," special plenary session at 23rd ACM Conference on Economics and Computation (**EC**), 2022.

[3] **On the Impossibility of Key Agreements from Quantum Random Oracles**
Per Austrin, Hao Chung, Kai-Min Chung, Shiuan Fu, Yao-Ting Lin, Mohammad Mahmoody
In proceedings of The 42nd International Cryptology Conference (**CRYPTO**), 2022.

[2] **Round Efficient Secure Multiparty Quantum Computation with Identifiable Abort**
Bar Alon and Hao Chung, Kai-Min Chung, Mi-Ying Huang, Yi Lee, Yu-Ching Shen
In proceedings of The 41st International Cryptology Conference (**CRYPTO**), 2021.

[1] **Fair Byzantine Agreements for Blockchains**
Po-Chun Kuo, Hao Chung, Tzu-Wei Chao, Chen-Mou Cheng
In **IEEE Access**, vol. 8, pp. 70746-70761, 2020, doi: 10.1109/ACCESS.2020.2986824.

Talks

Collusion-Resilience in Transaction Fee Mechanism Design
ACM Conference on Economics and Computation, New Haven, USA 07/11/2024
CMU Secure Blockchain Summit, Pittsburgh, USA 04/16/2024

Maximizing Miner Revenue in Transaction Fee Mechanism Design
Innovations in Theoretical Computer Science, Berkeley, USA 02/01/2024

What Can Cryptography Do for Decentralized Mechanism Design
Institute of Information Science, Academia Sinica, Taipei, Taiwan 02/22/2024

Rapidash: Foundations of Side-Contract-Resilient Fair Exchange
The Science of Blockchain Conference 2024, New York City, USA 08/09/2024
IC3 Blockchain Camp, New York City, USA 06/17/2023
CMU Secure Blockchain Summit, Pittsburgh, USA 05/08/2023
CryptoEconDay @ Consensus, Austin, USA 04/25/2023
Institute of Information Science, Academia Sinica, Taipei, Taiwan 12/30/2022
Crypto Economics Security Conference 2022, Berkeley, USA 10/31/2022

Foundations of Transaction Fee Mechanism Design
ACM CCS Workshop on DeFi, Salt Lake City, USA 10/18/2024
ACM-SIAM Symposium on Discrete Algorithms, Florence, Italy 01/24/2023
The Science of Blockchain Conference 2022, Palo Alto, USA 08/29/2022
UCSB Defi-Crypto Seminar, Remote 05/27/2022
Institute of Information Science, Academia Sinica, Taipei, Taiwan 01/11/2022
CMU Theory Lunch, Pittsburgh, USA 11/17/2021

Introduction to Quantum Computing
ChungHwa Telecom, New Taipei City, Taiwan 10/19/2019, 12/08/2020
National Chung-Shan Institute of Science and Technology, Taoyuan City, Taiwan 09/06/2017, 09/13/2017

Teaching Experience

Teaching Assistant Fall 2022, Fall 2023
Foundations of Blockchains (15435/18435) at CMU
Instructor: Elaine Shi

Instructor April 2021
Boot Camp for Quantum Computing at ChungHwa Telecom

Teaching Assistant Summer 2017
Summer School for Cryptography at Academia Sinica
Instructor: Julie Tzu-Yueh Wang, Yu-Chi Chen, Chia-Liang Sun

Reviewing Activities

External Reviewer (journal)

Journal of Cryptology, Management Science, Designs Codes and Cryptography

External Reviewer (conference)

Asiacrypt 2024, STOC 2024, S&P 2024, SODA 2024, Eurocrypt 2024, Financial Crypto 2024, PKC 2024, QIP 2023, CRYPTO 2023, FOCS 2022, CCS 2021, Eurocrypt 2021, S&P 2021, TCC 2021

Professional Services

Program Committee of Financial Cryptography and Data Security (FC) 2025

Co-organizer of the Tutorial: Transaction Fee Mechanism Design at EC 2024