

# HAO CHUNG

✉ [haochung@andrew.cmu.edu](mailto:haochung@andrew.cmu.edu) ♦  <https://chunghao.github.io>

## CURRENT POSITION

---

### Carnegie Mellon University

Ph.D. in Electrical and Computer Engineering

Pittsburgh, Pennsylvania, USA

02/2021 - Present

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

## EDUCATION

---

### National Taiwan University

M.S. in Electrical Engineering

Taipei, Taiwan

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

B.S. in Physics (minor in Philosophy)

Taipei, Taiwan

09/2012 - 06/2016

## WORK EXPERIENCE

---

### Academia Sinica

Research Assistant

Taipei, Taiwan

09/2019 - 02/2021

- Advisor: Kai-Min Chung

### DEXON Foundation

Blockchain Researcher

Taipei, Taiwan

09/2018 - 05/2019

## PUBLICATIONS

---

- [6] **What Can Cryptography Do For Decentralized Mechanism Design**  
Elaine Shi, Hao Chung, Ke Wu (randomized author order)  
In submission. Preprint version: [arXiv:2209.14462](https://arxiv.org/abs/2209.14462).
- [5] **Rapidash: Foundations of Side-Contract-Resilient Fair Exchange**  
Hao Chung, Elisaweta Masserova, Elaine Shi, Sri Aravinda Krishnan Thyagarajan  
In submission. Preprint version: [Cryptology ePrint Archive, Paper 2022/1063](https://eprint.iacr.org/2022/1063).
- [4] **Foundations of Transaction Fee Mechanism Design**  
Hao Chung, Elaine Shi  
In ACM-SIAM Symposium on Discrete Algorithms (**SODA**), 2023.  
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](https://doi.org/10.1109/ACCESS.2020.2986824).

## TALKS

---

### **Foundations of Transaction Fee Mechanism Design**

The Science of Blockchain Conference 2022, USA	08/29/2022
UCSB Defi-Crypto Seminar, USA	05/27/2022
Institute of Information Science, Academia Sinica, Taiwan	01/11/2022
CMU Theory Lunch, USA	11/17/2021

### **Introduction to Quantum Computing**

ChungHwa Telecom, Taiwan	10/19/2019, 12/08/2020, 04/08/2021
National Chung-Shan Institute of Science and Technology, Taiwan	09/06/2017, 09/13/2017

## TEACHING EXPERIENCE

---

### **Foundations of Blockchains (15435) at CMU**

Pittsburgh, Pennsylvania, USA

Teaching Assistant

08/2022 - 12/2022

### **Summer School for Cryptography in Academia Sinica**

Taipei, Taiwan

Teaching Assistant

07/2017 - 08/2017