Ke Wu

E-mail: kew2@andrew.cmu.edu  Telephone number: +1 410-369-8921
Personal website: kewecs.com

Research Interest

Intersection of cryptography and game theory
Decentralized mechanism design.
Application of game theory in multi-party computation.

Coding theory
Error correcting codes against edit errors.

Education

Ph.D. candidate in Computer Science  Aug 2020 - Jun 2024 (expected)
Carnegie Mellon University
Advisor: Elaine Shi

Ph.D. student in Computer Science  Sep 2019 - Aug 2020
Cornell University
Advisor: Elaine Shi
Transferred to CMU in the second year

M.S. in Computer Science  Aug 2016 - Dec 2017
Johns Hopkins University

B.S. in Mathematics  Sep 2012 - May 2016
Fudan University

Awards

JP Morgan Chase AI Ph.D. Fellowship 2023 - 2024
Awarded to 13 exceptional Ph.D. students worldwide for supporting their novel and impactful thesis work on AI, cryptography, and other related fields.

CMU Cylab Presidential Fellowship 2022 - 2023
Awarded to four high-achieving Ph.D. students pursuing security and/or privacy-related research at CMU per year.

Publications

Unless otherwise noted, the author order is either alphabetical or randomized.

Conference Proceedings

1 Ke Wu, Elaine Shi, and Hao Chung. “Maximizing Miner Revenue in Transaction Fee Mechanism Design”. In: Innovations in Theoretical Computer Science (ITCS). 2024.

2 Elaine Shi, Hao Chung, and Ke Wu. “What Can Crypto Do For Decentralized Mechanism Design?” In: Innovations in Theoretical Computer Science (ITCS). 2023.
3 Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. “Beyond single-deletion correcting codes: substitutions and transpositions”. In: *International Conference on Randomization and Computation (RANDOM)*. 2022.

4 Ilan Komargodski, Shin’ichiro Matsuo, Elaine Shi, and Ke Wu. “log*-Round Game-Theoretically-Fair Leader Election”. In: *International Cryptology Conference (CRYPTO)*. 2022.

5 Ke Wu, Gilad Asharov, and Elaine Shi. “A complete characterization of game-theoretically fair, multi-party coin toss”. In: *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2022.

6 Elaine Shi and Ke Wu. “Non-interactive anonymous router”. In: *International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*. 2021.

7 Ke Wu and Aaron B. Wagner (contribution order). “A practical coding scheme for the BSC with feedback”. In: *International Symposium on Information Theory (ISIT)*. 2021.

8 Kuan Cheng, Bernhard Haeupler, Xin Li, Amirbehshad Shahrasbi, and Ke Wu. “Synchronization strings: Highly efficient deterministic constructions over small alphabets”. In: *Symposium on Discrete Algorithms (SODA)*. 2019.

9 Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. “Edit Errors with Block Transpositions: Deterministic Document Exchange Protocols and Almost Optimal Binary Codes”. In: *International Colloquium on Automata, Languages and Programming (ICALP)*. 2019.

10 Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. “Deterministic document exchange protocols, and almost optimal binary codes for edit errors”. In: *Symposium on Foundations of Computer Science (FOCS)*. 2018.

**Journal Articles**

1 Kuan Cheng, Zhengzhong Jin, Xin Li, and Ke Wu. “Deterministic Document Exchange Protocols and Almost Optimal Binary Codes for Edit Errors”. In: *Journal of the ACM* 69.6 (2022), pp. 1–39.

2 Ryan Gabrys, Venkatesan Guruswami, João Ribeiro, and Ke Wu. “Beyond single-deletion correcting codes: substitutions and transpositions”. In: *IEEE Transactions on Information Theory* 69.1 (2022), pp. 169–186.

**Manuscripts**

1 T-H. Hubert Chung, Elaine Shi, and Ke Wu. *Mechanism Design for Automated Market Makers*. 2023.

2 Pratik Soni, Sri AravindaKrishnan Thyagarajan, and Ke Wu. *Game-Theoretically Fair Multi-Party Sampling*. 2023.

**Invited Talks**

**What Can Cryptography Do For Decentralized Mechanism Design?**

| Event                                      | Date  |
|--------------------------------------------|-------|
| IC3 Blockchain Camp                        | Jun 2023 |
| Carnegie Mellon University, Secure Blockchain Summit | May 2023 |
| Massachusetts Institute of Technology, CSAIL Security Seminar | Mar 2023 |
Beyond Single-Deletion Correcting Codes: Substitutions and Transpositions

log\(^{-r}\)-Round Game-Theoretically-Fair Leader Election

A Complete Characterization of Game-Theoretically Fair, Multi-Party Coin Toss

A Practical Coding Scheme for the BSC with Feedback

Synchronization Strings: Efficient and Fast Deterministic Constructions over Small Alphabets

Professional Experience

Research Intern, NTT Inc. 
Supervisor: Ilan Komargodski 
Conducted research on game-theoretically fair leader election with small round complexity.

Research Assistant, Johns Hopkins University 
Supervisor: Xin Li 
Conducted research on coding theory and cryptography, with a focus on studying error-correcting codes and document exchange protocols for edit errors.

Teaching Experience

Teaching Assistant 
Cornell University CS 4820: Introduction to Algorithms. Instructor: Eva Tardos.

Teaching Assistant 
Cornell University CS 4820: Introduction to Algorithms. Instructor: Elaine Shi.

Teaching Assistant 
CMU 15-356: Introduction to Cryptography. Instructor: Elaine Shi.

Reviewing Activities
Journal Reviewer    Journal of Information Theory
Conference Reviewer FOCS 2022, TCC 2022, SODA 202, EUROCRYPT 2023, TCC 2023, S&P 2024, ITCS 2024.

Professional Services

Co-founder and co-organizer of CMU Cylab Crypto Seminar
Seminar website: https://sites.google.com/view/crypto-seminar
Initiated the seminar series with Elaine Shi in 2020 and co-organized the seminar till now.

Program committee member
Financial Cryptography and Data Security 2024.

CSD Ph.D. admission committee member
Reviewed around 200 applications for the Theory group and the Cryptography group in 2021.