Ke Wu

Assitant Professor, Computer Science and Engineering, University of Michigan
E-mail: kewucse@umich.edu *Telephone number:* +1 410-369-8921
Personal website: kewucs.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 - Apr 2024*
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 Sri AravindaKrishnan Thyagarajan, Pratik Soni, and **Ke Wu**. "Game-Theoretically Fair Distributed Sampling". In: *Annual International Cryptology Conference*. Springer. 2024, pp. 207–239.

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

3 Elaine Shi, Hao Chung, and **Ke Wu**. "What Can Crypto Do For Decentralized Mechanism Design?" In: *Innovations in Theoretical Computer Science (ITCS)*. 2023.

4 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.

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

6 **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.

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

8 **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.

9 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.

10 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.

11 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 Pedro Branco, Pratik Soni, Sri AravindaKrishnan Thyagarajan, and **Ke Wu**. *Privacy-Preserving Game-Theoretically Fair Multi-Party Coin Tossing*. 2025.

2 Hao Chung, **Ke Wu**, and Elaine Shi. *Foundations of Platform-Assisted Auctions*. arXiv preprint arXiv:2501.03141. 2025.

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

Invited Talks

Game-Theoretically Fair Distributed Sampling

CRYPTO — Aug 2024
University of Sydney, Decentralized Science Seminar, — Oct 2024
UMich Theory Seminar, — Nov 2024
MangoDB, — Nov 2024

What Can Cryptography Do For Decentralized Mechanism Design?

IC3 Blockchain Camp — Jun 2023
Carnegie Mellon University, Secure Blockchain Summit — May 2023
Massachusetts Institute of Technology, CSAIL Security Seminar — Mar 2023
ITCS — Jan 2023
UC Berkeley, Sky Security Seminar — Nov 2022
Carnegie Mellon University, Theory Lunch — Nov 2022

Beyond Single-Deletion Correcting Codes: Substitutions and Transpositions

RANDOM — Sep 2022

$\log^*$-Round Game-Theoretically-Fair Leader Election

CRYPTO — Aug 2022

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

EUROCRYPTO — May 2022
PL&Crypto workshop — May 2022
Stanford University, Security Seminar — May 2022
Carnegie Mellon University, Theory Lunch — Apr 2022
Bar-Ilan University, Theory Seminar — Dec 2021

A Practical Coding Scheme for the BSC with Feedback

ISIT — Jan 2021

Synchronization Strings: Efficient and Fast Deterministic Constructions over Small Alphabets

SODA — Jan 2019
University of Maryland, Theory Seminar — Dec 2018
Johns Hopkins University, Theory Seminar — Dec 2018

Professional Experience

Research Intern, NTT Inc. *May 2021 - Aug 2021*
Supervisor: Ilan Komargodski
Conducted research on game-theoretically fair leader election with small round complexity.

Research Assistant, Johns Hopkins University *Feb 2018 - Mar 2019*
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

Instructor
UMich EECS 475: Introduction to Cryptography. Fall 2024
UMich EECS 598: Foundation of Distributed Consensus and Blockchains. Sprnig 2025

Teaching Assistant *Fall 2019*
Cornell University CS 4820: Introduction to Algorithms. Instructor: Eva Tardos.

Teaching Assistant *Spring 2020*
Cornell University CS 4820: Introduction to Algorithms. Instructor: Elaine Shi.

Teaching Assistant *Fall 2021*
CMU 15-356: Introduction to Cryptography. Instructor: Elaine Shi.

Reviewing Activities

Journal Reviewer	Journal of Information Theory
Conference Reviewer	FOCS 2022, TCC 2022, SODA 2023, EUROCRYPT 2023, TCC 2023, FC 2024, S&P 2024, ITCS 2024, FC 2025.

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.
Financial Cryptography and Data Security 2025.

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