Mingxun Zhou

Email : mingxunz@andrew.cmu.edu

wuwuz.github.io

Interests: Information Security and Privacy, Applied Cyptography, Machine Learning

Education

Carnegie Mellon University Pittsburgh, US

- *Ph.D. in Computer Science* *Feb. 2021 - Present*

Peking University Beijing, China

- *Bachelor of Science (Honored) in Computer Science* *Sep. 2016 - Jul. 2020*
  - **Turing Class**: First honor class

Working Experience

NTT Research Cryptography and Information Security Lab USA

- *Research Intern, Oblivious Algorithm Design* *Jun. 2022 - Aug. 2022*

The University of Hong Kong Hong Kong SAR, China

- *Research Assistant, Privacy-preserving Data Aggregation* *Jun. 2021 - Aug. 2021*

Shanghai Qizhi Institute Shanghai, China

- *Research Assistant, High Performance Blockchain Network Research* *Aug. 2020 - Feb. 2021*

Publications

1. Ashrujit Ghoshal, **Mingxun Zhou**, Bo Peng, & Elaine Shi. *Pseudorandom Functions with Weak Programming Privacy and Applications to Private Information Retrieval.* EUROCRYPT 2025.
2. **Mingxun Zhou**, Elaine Shi, & Giulia Fanti. *Pacmann: Efficient Private Approximate Nearest Neighbor Search.* ICLR 2025.
3. **Mingxun Zhou**, Elaine Shi, & Giulia Fanti. *Conan: Distributed Proofs of Compliance for Anonymous Data Collection.* CCS 2024.
4. Ashrujit Ghoshal, **Mingxun Zhou**, & Elaine Shi. *Efficient Pre-processing PIR Without Public-Key Cryptography*, EUROCRYPT 2024.

   Primary author with randomized order.
5. **Mingxun Zhou**, Mengshi Zhao, T-H. Hubert Chan, & Elaine Shi.*Advanced Composition Theorems for Differential Obliviousness.* ITCS 2024.
6. **Mingxun Zhou**, Andrew Park, Elaine Shi & Wenting Zheng. *Piano: Extremely Simple, Single-Server PIR with Sublinear Server Computation.* IEEE S&P 2024.
7. **Mingxun Zhou**, Elaine Shi, T-H. Hubert Chan, & Shir Maimon. *A Theory of Composition for Differential Obliviousness.* EUROCRYPT, 2023.
8. **Mingxun Zhou**, Wei-Kai Lin, Yiannis Tselekounis, & Elaine Shi. *Optimal Single-Server Private Information Retrieval.* EUROCRYPT, 2023.
9. **Mingxun Zhou***, Liyi Zeng*, Yilin Han, Peilun Li, Fan Long, Dong Zhou, Ivan Beschastnikh, & Ming Wu. *Mercury: Fast Transaction Broadcast in High Performance Blockchain System.* IEEE INFOCOM, 2023.

   *Equal contribution.
10. **Mingxun Zhou**, Tianhao Wang, T-H. Hubert Chan, Giulia Fanti, & Elaine Shi. *Locally Differentially Private Sparse Vector Aggregation.* IEEE S&P, 2022.
11. Charlie Hou*, **Mingxun Zhou***, Yan Ji., Phil Daian, Florian Tramer, Giulia Fanti, & Ari Juels. *SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning.* NDSS, 2021.

    *Equal contribution.
12. Minmei Wang*, **Mingxun Zhou***, Shouqian Shi, & Chen Qian. *Vacuum Filters : More Space-Efficient and Faster Replacement for Bloom and Cuckoo Filters.* VLDB, 2020.

    *Equal contribution.

Preprints and Other Research Projects

1. **Mingxun Zhou**, & Elaine Shi. *The Power of the Differentially Oblivious Shuffle in Distributed Privacy Mechanisms.* 2022.

Open Source Projects

1. *Pacmann: Efficient Private Approximate Nearest Neighbor Search*, 2024.

   https://github.com/privsearch/private-search-temp

2. *Conan: Distributed Proofs of Compliance for Anonymous Data Collection*, 2024.

   https://github.com/wuwuz/conan-open/

3. *QuarterPIR: Efficient Pre-processing PIR Without Public-Key Cryptography*, 2024.

   https://github.com/wuwuz/QuarterPIR/

4. *Piano: Extremely Simple, Single-Server PIR with Sublinear Server Computation*, 2023.

   https://github.com/wuwuz/Piano-PIR-new

5. *Mercury: Fast Transaction Broadcast in High-Performance Blockchain System*, 2022.

   https://github.com/wuwuz/P2PNetwork

6. *Locally Differentially Private Sparse Vector Aggregation*, 2022.

   https://github.com/wuwuz/sparse-vector-aggregation

7. *SquirRL: Automating Attack Analysis on Blockchain Incentive Mechanisms with Deep Reinforcement Learning*, 2021.

   https://github.com/wuwuz/SquirRL

8. *Vacuum Filters: More Space-Efficient and Faster Replacement for Bloom and Cuckoo Filters*, 2020.

   https://github.com/wuwuz/Vacuum-Filter

Invited Talks

1. *Recent Progress in Preprocessing Private Information Retrieval.*

   Presented at S&P '24, Eurocrypt '24, CMU Blockchain Summit '23, JHU, Cornell Tech, HKU, PKU, SJTU, UC Berkeley, Brown.

2. *Proof of Compliance for Anonymous Messages.*

   Presented at Crypto PPML Workshop '23, CMU Blockchain Summit '24.

3. *Optimal Single Server Private Information Retrieval.*

   Presented at Eurocrypt '23, CMU Theory Lunch '22, CMU Crypto Seminar '22.

4. *Composition Theory for Differential Obliviousness.*

   Presented at Eurocrypt '23, ITCS '24, CMU Theory Lunch '22.

5. *The Power of the Differentially Oblivious Shuffle in Distributed Privacy Mechanisms.*

   Presented at Google Federated Learning Workshop '22, Crypto PPML Workshop '22, FORC '22.

6. *Locally Differentially Private Sparse Vector Aggregation.*

   Presented at IEEE S&P '22.

7. *Reinforcement Learning for Blockchain Incentive Analysis.*

   Presented at IJTCS '21.

Competitions

International Collegiate Programming Contest, Regional Gold Medal, *ICPC Foundation*	Oct. 2018
National Olympiad of Informatics, Gold Medal, *China Computer Federation*	Aug. 2015

Awards and Honors

CyLab Presidential Fellowship, *CMU*	Aug. 2023
Outstanding Dissertation for Bachelor's Degree (**Top 10** in the EECS school), *PKU*	Jun. 2020
Turing Benteng Scholarship, *PKU*	Nov. 2019
Kwang-Hua Scholarship (**Top 3** in class, ∼**1%** of students), *PKU*	Dec. 2018
Chuang-Long Ke Scholarship, *PKU*	Dec. 2017
Dean Scholarship for Freshman, *PKU*	Sep. 2016