[Updated on August 31, 2024]

Xiao Liang

xiao-liang.com
github.com/xiao-liang
xiaoliang@cuhk.edu.hk

Research Interests

I am interested in Cryptography and its intersections with related fields such as Quantum Computing, Computational Complexity, and Computer Security. My work has concentrated on theoretical fundamentals, including Zero-Knowledge Protocols, Secure Multi-Party Computation, Non-Malleability, and Digital Signatures, as well as their practical applications, such as Secure Spectrum Allocation and Plausibly Deniable Storage.

Experience

The Chinese University of Hong Kong, Shatin, Hong Kong Sept., 2024 to current
Assistant Professor

NTT Research, Sunnyvale, USA March, 2023 to March, 2024
Postdoctoral Fellow (Supervisor: Vipul Goyal)

Rice University, Houston, USA July, 2022 to Feb., 2023
Postdoctoral Associate (Co-advised by Kai-Min Chung and Nai-Hui Chia)

Indiana University Bloomington, Bloomington, USA Nov., 2021 to June, 2022
Postdoctoral Fellow (Co-advised by Kai-Min Chung and Nai-Hui Chia)

Max Planck Institute (Security and Privacy), Bochum, German July, 2021 to Oct., 2021
Research Visitor (Host: Giulio Malavolta)

University of California, Berkeley, Berkeley, USA May to Aug., 2019
Research Visitor (Host: Sanjam Garg)

University of California, Berkeley, Berkeley, USA May to Aug., 2018
Research Visitor (Host: Sanjam Garg)

Education

Stony Brook University, Stony Brook, NY, USA 2016–2021
Ph.D. in Computer Science (Advisor: Omkant Pandey) GPA: 3.96/4.00

Stony Brook University, Stony Brook, NY, USA 2014–2016
M.S. in Applied Mathematics GPA: 4.00/4.00

Beijing Institute of Technology, Beijing, China 2010–2014
Bachelor of Economics in International Economy and Trade GPA: 91/100 (Ranked 1st/73)

Scholarships and Awards

- **University Fellowship**, Stony Brook University 2016–2019
- **Excellent Student Scholarship** (awarded for three times), Beijing Institute of Technology 2012–2014
- **National Scholarship**, Ministry of Education of China 2012
- **Straight-A Scholarship**, Beijing Institute of Technology 2012

- **First Prize**, The 2nd Mathematics Competition at Beijing Institute of Technology 2011
- **Second Prize**, The 22nd Beijing College Students Mathematics Competition 2011

Professional Services

- **Program Committee:** ITC (2023)
- **Journal Reviewer:** Theoretical Computer Science (2024), IEEE Transactions on Dependable and Secure Computing (2021), ACM Transactions on Storage (2019)
- **External Reviewer:** STOC (2024), FOCS (2022, 2024), Crypto (2020–2024), Eurocrypt (2020, 2022-2024), TCC (2018–2024), QIP (2023), QCrypt (2023, 2024), Asiacrypt (2019, 2021-2023), ITC (2020), PKC (2020, 2022, 2024), TQC (2023, 2024), AQIS (2024), SCN (2022)

Publications

(In accordance with the tradition of theoretical computer science, authors are listed in alphabetical order.)

[12] **A New Approach to Post-Quantum Non-Malleability**
Xiao Liang, Omkant Pandey, and Takashi Yamakawa
The 64th IEEE Symposium on Foundations of Computer Science (FOCS 2023)

[11] **On Concurrent Multi-Party Quantum Computation**
Vipul Goyal, Xiao Liang, and Giulio Malavolta
The 43rd International Cryptology Conference (Crypto 2023)
The 13th International Conference on Quantum Cryptography (QCrypt 2023)

[10] **A New Approach to Efficient Non-Malleable Zero-Knowledge**
Allen Kim, Xiao Liang, and Omkant Pandey
The 42nd International Cryptology Conference (Crypto 2022)

[9] **Post-Quantum Simulatable Extraction with Minimal Assumptions: Black-Box and Constant-Round**
Nai-Hui Chia, Kai-Min Chung, Xiao Liang, and Takashi Yamakawa
The 42nd International Cryptology Conference (Crypto 2022)

[8] **SoK: Plausibly Deniable Storage**
Chen Chen, Xiao Liang, Bogdan Carbunar, and Radu Sion (Authors are ordered by contributions)
The 22nd Privacy Enhancing Technologies Symposium (PETS 2022)

[7] **A Note on the Post-Quantum Security of (Ring) Signatures**
Rohit Chatterjee, Kai-Min Chung, Xiao Liang, and Giulio Malavolta
The 25th International Conference on Practice and Theory of Public-Key Cryptography (PKC 2022)

[6] **Towards a Unified Approach to Black-Box Constructions of Zero-Knowledge Proofs**
Xiao Liang and Omkant Pandey
The 41st International Cryptology Conference (Crypto 2021)

[5] **Compact Ring Signatures from Learning with Errors**
Rohit Chatterjee, Sanjam Garg, Mohammad Hajiabadi, Dakshita Khurana, Xiao Liang, Giulio Malavolta, Omkant Pandey, and Sina Shiehian
The 41st International Cryptology Conference (Crypto 2021)

[4] **Black-Box Constructions of Bounded-Concurrent Secure Computation**
Sanjam Garg, Xiao Liang, Omkant Pandey, and Ivan Visconti
The 12th International Conference on Security and Cryptography for Networks (SCN 2020)

[3] **Improved Black-Box Constructions of Composable Secure Computation**
Rohit Chatterjee, Xiao Liang, and Omkant Pandey
The 47th International Colloquium on Automata, Languages, and Programming (ICALP 2020)

[2] **Random Walks and Concurrent Zero-Knowledge**
Anand Aiyer, Xiao Liang, Nilu Nalini, and Omkant Pandey
The 18th International Conference on Applied Cryptography and Network Security (ACNS 2020)

[1] **ProCSA: Protecting Privacy in Crowdsourced Spectrum Allocation**
Max Curran, Xiao Liang, Himanshu Gupta, Omkant Pandey, and Samir Das (Authors are ordered by contributions)
The 24th European Symposium on Research in Computer Security (ESORICS 2019)

Invited Talks

(This list does not include the conference talks I have delivered.)

On Concurrent Multi-Party Quantum Computation
- Invited Talk at Centrum Wiskunde & Informatica (Oct. 27th, 2023)

A New Approach to Post-Quantum Non-Malleability
- Invited Talk at Stanford University (April 21st, 2023)
- Invited Talk at Texas Crypto Day (Dec. 2nd, 2022)
- Invited Talk at New York University (Sept. 28th, 2022)

Alice's Adventure in Quantum Wonderland
- A Rump Session Talk at Crypto 2022 (Aug. 16th, 2022)

The Watrous Post-Quantum Zero-Knowledge Proof: A Tutorial
- Invited Talk at at Max-Planck Institute (Aug. 2nd, 2021)

Other Projects

A Study on the Management Model of China's Nursing Homes with Examples from Beijing
Jingru Du and Xiao Liang
Foreign Investment in China, 2013(6): 138-140 (Published in Chinese)

Training Data Reduction for Recursive Tensor Neural Network 2015 Fall
(Collaborator: Niranjan Balasubramanian and Ankit Gupta)
- Propose a method to simplify the parsing tree, saving 40% of labeling work while maintaining the same level of accuracy.
- Code to measure the performance of these models on different length of phrases and type of nodes.
- Contribute to the StonyBrookNLP/stingysentiment on GitHub.