

## RESEARCH INTERESTS

---

I am interested in (classical and quantum) cryptography. My research has been focused on Zero-Knowledge Protocols, Secure Multi-Party Computation, Non-Malleability, and Digital Signatures.

## EXPERIENCE

---

<b>Rice University</b> , Houston, USA Postdoctoral Associate (Co-advised by Nai-Hui Chia and Kai-Min Chung)	July, 2022 to Current
<b>Indiana University Bloomington</b> , Bloomington, USA Postdoctoral Fellow (Co-advised by Nai-Hui Chia and Kai-Min Chung)	Nov., 2021 to June, 2022
<b>Max Planck Institute (Security and Privacy)</b> , Bochum, German Visiting Scholar (Host: Giulio Malavolta)	July, 2021 to Oct., 2021
<b>University of California, Berkeley</b> , Berkeley, USA Research Visitor (Host: Sanjam Garg)	May to Aug., 2019
<b>University of California, Berkeley</b> , Berkeley, USA Research Visitor (Host: Sanjam Garg)	May to Aug., 2018

## EDUCATION

---

<b>Stony Brook University</b> , Stony Brook, NY, USA Ph.D. in Computer Science (Advisor: Omkant Pandey)	2016–2021 GPA: 3.96/4.00
<b>Stony Brook University</b> , Stony Brook, NY, USA M.S. in Applied Mathematics	2014–2016 GPA: 4.00/4.00
<b>Beijing Institute of Technology</b> , Beijing, China B.S. in Economics	2010–2014 GPA: 91/100 (Ranked 1st/73)
<b>City University of Hong Kong</b> , Kowloon, Hong Kong Visiting Student in the College of Business	2013 Spring

## SCHOLARSHIPS AND AWARDS

---

• <b>University Fellowship</b> , Stony Brook University	2016–2019
• <b>Excellent Student Scholarship</b> (awarded for three times), Beijing Institute of Technology	2012–2014
• <b>National Scholarship</b> , Ministry of Education of China	2012
• <b>Straight-A Scholarship</b> , Beijing Institute of Technology	2012
• <b>First Prize</b> , The 2nd Mathematics Competition at Beijing Institute of Technology	2011
• <b>Second Prize</b> , The 22nd Beijing College Students Mathematics Competition	2011
• <b>Third Prize</b> , The 7th Challenge Cup Beijing College Students Extracurricular Academic Science and Technology Competition	2011

## PROFESSIONAL SERVICES

---

- **Reviewer:** ACM Transactions on Storage (2019), IEEE Transactions on Dependable and Secure Computing (2021)
- **Subreviewer:** FOCS (2022), Crypto (2020–2022), Eurocrypt (2020, 2022), TCC (2018–2022), Asiacrypt (2019, 2021, 2022), ITC (2020), PKC (2020, 2022), SCN (2022)

## PUBLICATIONS

---

- [11] **A New Approach to Efficient Non-Malleable Zero-Knowledge**  
Allen Kim, Xiao Liang, and Omkant Pandey  
*The 42nd International Cryptology Conference (CRYPTO 2022)*
- [10] **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)*
- [9] **SoK: Plausibly Deniable Storage**  
Chen Chen, Xiao Liang, Bogdan Carbutar, and Radu Sion  
*The 22nd Privacy Enhancing Technologies Symposium (PETS 2022)*
- [8] **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 2021)*
- [7] **Towards a Unified Approach to Black-Box Constructions of Zero-Knowledge Proofs**  
Xiao Liang and Omkant Pandey  
*The 41st International Cryptology Conference (CRYPTO 2021)*
- [6] **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)*
- [5] **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)*
- [4] **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)*
- [3] **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)*
- [2] **ProCSA: Protecting Privacy in Crowdsourced Spectrum Allocation**  
Max Curran, Xiao Liang, Himanshu Gupta, Omkant Pandey, and Samir Das  
*The 24th European Symposium on Research in Computer Security (ESORICS 2019)*
- [1] **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)

## LANGUAGES

---

- **Mandarin:** Native Proficiency
- **English:** Professional Working Proficiency (TOEFL Score: 109/120)

## SKILLS

---

- **Programming:** Python, C++, R, Matlab
- **SAS:** SAS Certified Advanced Programmer for SAS

## NON-CRYPTOGRAPHIC PROJECTS

---

### **Training Data Reduction for Recursive Tensor Neural Network** 2015 Fall

(Collaborator: Niranjana 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.

### **Analysis of China's Agricultural Exports Using ARIMA & Clustering Model** 2014

(My Bachelor Thesis)

- Construct an ARIMA(1,2,1) model to predict the short-term export of agricultural products.
- Conduct Hierarchical Clustering with 19 main products using IBM SPSS.
- Provide policy-making advice based on analysis of trade structure.