Xiao Liang

xiao-liang.com
github.com/xiao-liang
liang1@cs.stonybrook.edu

Research Interests

I am interested in cryptography. My research has been focused on Zero-Knowledge Protocols, Secure Multi-Party Computation and Non-Malleability, with an emphasis on black-box techniques.

Education

Stony Brook University, Stony Brook, NY, USA — 2016–Current
Ph.D. in Computer Science (Advisor: Omkant Pandey) — GPA: 3.95/4.00

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
B.S. in Economics — GPA: 91/100 (Ranked 1st/73)

City University of Hong Kong, Kowloon, Hong Kong — 2013 Spring
Visiting Student in the College of Business

Scholarships and Awards

- **University Fellowship**, Stony Brook University — 2016–2019
- **Excellent Student Scholarship** (three times), Beijing Institute of Technology — 2013–2018
- **National Scholarship**, Ministry of Education of China — 2012
- **Straight-'A' Scholarship**, Beijing Institute of Technology — 2012
- **1st Prize**, the 2nd Mathematics Competition at Beijing Institute of Technology — 2011
- **Silver Medal**, the 22nd Beijing College Students Mathematics Competition — 2011
- **3rd Prize**, the 7th "Challenge Cup" Beijing College Students Extracurricular Academic Science and Technology Competition — 2011

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

Professional Service

Subreviewer: TCC (2018, 2019, 2020), ACM Transactions on Storage (2019), Asiacrypt (2019), Eurocrypt (2020), PKC (2020), ITC (2020), Crypto (2020, 2021)

Publications

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

[2] **Improved Black-Box Constructions of Composable Secure Computation**
Rohit Chatterjee, Xiao Liang, 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, Omkant Pandey
The 18th International Conference on Applied Cryptography and Network Security (**ACNS**), 2020

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

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

Non-Cryptographic Projects

Training Data Reduction for Recursive Tensor Neural Network 2015 Fall
(*Collaborator: Niranjan Balasubramanian, 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, 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.