Peihan Miao

665 Soda Hall
Computer Science Division
University of California at Berkeley
Berkeley, CA 94720

Email: peihan@cs.berkeley.edu
https://people.eecs.berkeley.edu/~peihan/

Education

University of California at Berkeley, USA — Aug 2014 $\sim$ Present
Ph.D., Computer Science

- Advisor: Sanjam Garg
- GPA: **4.0**/4.0

Shanghai Jiao Tong University, China — Sept 2010 $\sim$ July 2014
B.S., Computer Science (ACM Honors Class)

- Overall GPA **3.87**/4.0 (**91.5**/100) Major GPA **3.96**/4.0 (**93.4**/100)
- Rank **1st** in the ACM Honors Class

Publications

Cut-and-Choose for Garbled RAM.
Peihan Miao.
Manuscript, available at http://eprint.iacr.org/2016/907.pdf.

Obfuscation from Low Noise Multilinear Maps.
Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Pratyay Mukherjee.
Manuscript, available at http://eprint.iacr.org/2016/599.pdf.

Laconic Oblivious Transfer and its Applications.
Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou.
In *Proceedings of the 37th International Cryptology Conference* (**CRYPTO**) 2017.

Decentralized Anonymous Micropayments.
Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Miao, Ian Miers, and Pratyush Mishra.
In *Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques* (**EUROCRYPT**) 2017.

Secure Multiparty RAM Computation in Constant Rounds.
Sanjam Garg, Divya Gupta, Peihan Miao, and Omkant Pandey.
In *Proceedings of the 14th IACR Theory of Cryptography Conference* (**TCC**) 2016-B.

Nordhaus-Gaddum-Type Problems for Lines in Hypergraphs.
Xiaomin Chen, and Peihan Miao.
Discrete Applied Mathematics (2016).

Secretary Markets with Local Information.

Ning Chen, Martin Hoefer, Marvin Künnemann, Chengyu Lin, and Peihan Miao.
In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming* (**ICALP**) 2015.

Graph Metric with No Proper Inclusion Between Lines.
Xiaomin Chen, Guangda Huzhang, Peihan Miao, and Kuan Yang.
Discrete Applied Mathematics (2015).

Number of Lines in Hypergraphs.
Pierre Aboulker, Adrian Bondy, Xiaomin Chen, Ehsan Chiniforooshan, Vašek Chvátal, and Peihan Miao.
Discrete Applied Mathematics (2014).

Research Experience

Research Intern at Microsoft Research, Redmond May $\sim$ Aug 2017

- *Mentor*: Melissa Chase.
- *Topics*: Privacy and security protection of genomic data. Theoretical foundations of Intel Software Guard Extensions (SGX).

Visiting Student at Simons Institute, Berkeley May $\sim$ Aug 2015

- Attending the summer program on cryptography.

Research Assistant at Nanyang Technological University, Singapore Aug 2013 $\sim$ Jan 2014

- *Mentor*: Ning Chen.
- *Topics*: Generalized secretary problem. Network formation game.

Studies in Combinatorics and Graph Theory Feb 2013 $\sim$ June 2014

- *Mentors*: Xiaomin Chen, and Vašek Chvátal.
- *Topics*: Generalization of the De Bruijn-Erdős theorem. Nordhaus-Gaddum type problems for lines in hypergraphs.

Visiting Student at Microsoft Research Asia, Shanghai, China Feb $\sim$ June 2013

- *Mentor*: Pinyan Lu.
- *Topic*: Optimal auction and pricing in Bayesian setting.

Talks

Laconic Oblivious Transfer and its Applications.
Invited talk at *NY CryptoDay*. Columbia University, New York, Sept 15, 2017.

Laconic Oblivious Transfer and its Applications.
Conference talk at *the 37th International Cryptology Conference (CRYPTO)*, University of California, Santa Barbara, Aug 20 – 24, 2017.

Laconic Oblivious Transfer and its Applications.
Invited talk at *UW Theory Seminar*, University of Washington, Seattle, July 28, 2017.

Laconic Oblivious Transfer and its Applications.

Invited talk at *China Theory Week*. Shanghai, China, July 17 – 20, 2017.

Laconic Oblivious Transfer and its Applications.
Invited talk at *Bay Area Crypto Day*. Visa Research, Palo Alto, April 21, 2017.

Laconic Oblivious Transfer and its Applications.
Contributed talk at *the Theory and Practice of Multi-Party Computation Workshop*. Bristol, United Kingdom, April 3 – 7, 2017.

Secure Multiparty RAM Computation in Constant Rounds.
Conference talk at *the 14th IACR Theory of Cryptography Conference (TCC)*. Beijing, China, Oct 31 – Nov 3, 2016.

Decentralized Anonymous Micropayments.
Lightning talk at *the 5th Women in Theory Workshop*. Simons Institute, Berkeley, May 22 – 25, 2016.

Cut-and-Choose for Garbled RAM.
Invited talk at *Bay Area Crypto Day.* UC Berkeley, Nov 20, 2015.

Secretary Markets with Local Information.
Conference talk at *the 42nd International Colloquium on Automata, Languages, and Programming (ICALP)*. Kyoto, Japan, July 6 – 10, 2015.

Teaching Experience

- Fall 2017: Graduate Student Instructor for CS170, Efficient Algorithms and Intractable Problems.
- Fall 2016: Graduate Student Instructor for CS276, Cryptography.
- Fall 2012 & Spring 2014: Teaching Assistant for CS026, Set Theory and Mathematical Logic.
- Fall 2012 & Spring 2013: Assistant Coach in Shanghai Jiao Tong University ACM-ICPC Teams.

Honors and Awards

- **Department Fellowship**, EECS, UC Berkeley, 2014
- **Zhiyuan Outstanding Student Scholarship**, Shanghai Jiao Tong University, 2014
- **Outstanding Graduate of Shanghai Jiao Tong University**, 2014
- **Google Anita Borg Scholarship**, 2013 (21 undergraduates in China)
- **Tencent Innovation Scholarship**, 2012 (1 student in the ACM Honor Class)
- **Academic Excellence Scholarship (First-Class)**, Shanghai Jiao Tong University, 2012 & 2011 (top 1%)
- **National Scholarship**, 2011 (highest scholarship in China, top 1%)
- ACM-ICPC (International Collegiate Programming Contest) Asia Regional
  - **3rd place** in Pacific Northwest Regional, 2014
  - **2nd place** in Hsinchu Site & **Gold medal** in Beijing Site, 2011
  - **4th place** in Jakarta Site & **Best Female Team** in Hangzhou Site, 2010
- **Best Female Contestant** in the National Olympiad in Informatics, China, 2009 (1 female in China)