Peihan Miao

Address: 115 Waterman St, 4th floor, Providence, RI 02912
Email: peihan_miao@brown.edu
Homepage: https://sites.google.com/view/peihanmiao/

RESEARCH INTERESTS

Theoretical and Applied **Cryptography**, Security, Theoretical Computer Science.

My research focuses on the development, implementation, and evaluation of novel techniques for achieving efficient **secure multi-party computation** on large-scale datasets, from both **theoretical** and **applied** perspectives, aiming to bridge the gap between theory and practice.

EMPLOYMENT

Brown University, Providence, RI — Aug 2022 – Present
Assistant Professor, Department of Computer Science

University of Illinois Chicago, Chicago, IL — Aug 2020 – July 2022
Assistant Professor, Department of Computer Science

Visa Research, Palo Alto, CA — July 2019 – Aug 2020
Staff Research Scientist, Advanced Cryptography Group

EDUCATION

University of California, Berkeley, Berkeley, CA — Aug 2014 – May 2019
Ph.D., Computer Science
- Advisor: Sanjam Garg
- Dissertation: *Towards Secure Computation with Optimal Complexity*

Shanghai Jiao Tong University, Shanghai, China — Sept 2010 – June 2014
B.S., Computer Science (ACM Honors Class)
- Ranked **1st** in the ACM Honors Class

PUBLICATIONS

(Authors are ordered alphabetically.)

Conference Proceedings

1. **Updatable Private Set Intersection.**
   Saikrishna Badrinarayanan, Peihan Miao, and Tiancheng Xie.
   In *Proceedings of the 22nd Privacy Enhancing Technologies Symposium* (**PoPETS**) 2022.
2. **Amortizing Rate-1 OT and Applications to PIR and PSI.**
   Melissa Chase, Sanjam Garg, Mohammad Hajiabadi, Jialin Li, and Peihan Miao.
   In *Proceedings of the 19th Theory of Cryptography Conference* (**TCC**) 2021.
3. **Multi-Party Threshold Private Set Intersection with Sublinear Communication.**
   Saikrishna Badrinarayanan, Peihan Miao, Srinivasan Raghuraman, and Peter Rindal.
   In *Proceedings of the 24th International Conference on Practice and Theory of Public-Key Cryptography* (**PKC**) 2021.
4. **Private Set Intersection in the Internet Setting From Lightweight Oblivious PRF.**
   Melissa Chase, and Peihan Miao.
   In *Proceedings of the 40th International Cryptology Conference* (**CRYPTO**) 2020.
5. **Two-Sided Malicious Security for Private Intersection-Sum with Cardinality.**
   Peihan Miao, Sarvar Patel, Mariana Raykova, Karn Seth, and Moti Yung.
   In *Proceedings of the 40th International Cryptology Conference* (**CRYPTO**) 2020.
6. **Cut-and-Choose for Garbled RAM.**
   Peihan Miao.

In *Proceedings of the Cryptographers' Track at the RSA Conference* (**CT-RSA**) 2020.

7. **PASTA: PASsword-based Threshold Authentication.**
   Shashank Agrawal, Peihan Miao, Payman Mohassel, and Pratyay Mukherjee.
   In *Proceedings of the 25th ACM Conference on Computer and Communications Security* (**CCS**) 2018.
8. **Two-Round Multiparty Secure Computation Minimizing Public Key Operations.**
   Sanjam Garg, Peihan Miao, and Akshayaram Srinivasan.
   In *Proceedings of the 38th International Cryptology Conference* (**CRYPTO**) 2018.
9. **Obfuscation from Low Noise Multilinear Maps.**
   Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Pratyay Mukherjee.
   In *Proceedings of the 19th International Conference on Cryptology in India* (**INDOCRYPT**) 2018.
10. **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.
11. **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.
12. **Secure Multiparty RAM Computation in Constant Rounds.**
    Sanjam Garg, Divya Gupta, Peihan Miao, and Omkant Pandey.
    In *Proceedings of the 14th Theory of Cryptography Conference* (**TCC**) 2016-B.
13. **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.

Journal Articles

14. **Secretary Markets with Local Information.**
    Ning Chen, Martin Hoefer, Marvin Künnemann, Chengyu Lin, and Peihan Miao.
    Distributed Computing (2019).
15. **Nordhaus-Gaddum-Type Problems for Lines in Hypergraphs.**
    Xiaomin Chen, and Peihan Miao.
    Discrete Applied Mathematics (2016).
16. **Graph Metric with No Proper Inclusion Between Lines.**
    Xiaomin Chen, Guangda Huzhang, Peihan Miao, and Kuan Yang.
    Discrete Applied Mathematics (2015).
17. **Number of Lines in Hypergraphs.**
    Pierre Aboulker, Adrian Bondy, Xiaomin Chen, Ehsan Chiniforooshan, Vašek Chvátal, and Peihan Miao.
    Discrete Applied Mathematics (2014).

Workshop Papers

18. **Improved Multi-Party Fixed-Point Multiplication.**
    Saikrishna Badrinarayanan, Eysa Lee, Peihan Miao, and Peter Rindal.
    CRYPTO Affiliated Event: The 3rd Privacy-Preserving Machine Learning Workshop (**PPML**) 2021.
19. **Efficient Leakage Resilient Secret Sharing.**
    Peihan Miao, Akshayaram Srinivasan, and Prashant Nalini Vasudevan.
    NIST Threshold Cryptography Workshop 2019.

PATENTS

1. **Updatable Private Set Intersection.**
   Saikrishna Badrinarayanan, Peihan Miao, and Tiancheng Xie.

International Publication No.: WO 2022/076038 A1. Publication Date: April 14, 2022.

2. **Round-Efficient Fully Secure Solitary Multi-Party Computation with Honest Majority.**
   Saikrishna Badrinarayanan, Peihan Miao, Pratyay Mukherjee, and Divya Ravi.
   Publication No.: US 2021/0391987 A1. Publication Date: December 16, 2021.
3. **Password Based Threshold Token Generation.**
   Shashank Agrawal, Peihan Miao, Payman Mohassel, and Pratyay Mukherjee.
   Publication No.: US 2021/0243026 A1. Publication Date: August 5, 2021.

FUNDING AND GRANTS

Meta Privacy Enhancing Technologies Award Aug 2022

- **Title:** Fast, Robust, and Scalable Privacy Preserving Data Analytics
- **PIs: Peihan Miao** (PI) and Mohammad Hajiabad (co-PI)

NSF National Science Foundation CNS-2055358 (SaTC) June 2021 – May 2024

- **Title:** Expanding the Realm of Oblivious Transfer: New Tools for Cryptography
- **PIs:** Mohammad Hajiabadi (PI) and **Peihan Miao** (co-PI)

DPI Discovery Partners Institute Science Team Seed Grant Sept 2020 – Feb 2022

- **Title:** Privacy in the Era of Big Data
- **PIs:** Lenore Zuck (lead PI, *UIC*), Ugo Buy (*UIC*), Oluwasanmi Koyejo (*UIUC*), **Peihan Miao** (*UIC*), and Madhusudan Parthasarathy (*UIUC*)

HONORS AND AWARDS

- **Meta Privacy Enhancing Technologies Award**, 2022.
- Named in **Rising Stars in EECS**, 2017 (top female graduates and postdocs in EE and CS).
- **Department Fellowship**, EECS, UC Berkeley, 2014.
- **Zhiyuan Outstanding Student Scholarship**, Shanghai Jiao Tong University, 2014 (10 students).
- **Outstanding Graduate of Shanghai Jiao Tong University**, 2014.
- **Google China Anita Borg Scholarship**, 2013 (21 female undergraduates in China).
- **Tencent Innovation Scholarship**, 2012 (1 student in the ACM Honors Class).
- **Academic Excellence Scholarship (First-Class)**, Shanghai Jiao Tong University, 2010 – 2012 (top 1%).
- **National Scholarship**, 2011 (highest scholarship in China, top 1%).
- ACM International Collegiate Programming Contest (ICPC)
  - **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 (NOI), China, 2009 (top female).

TEACHING

Instructor, Brown University

- CSCI 1515: Applied Cryptography Spring 2023
- CSCI 2952L: Special Topics in Secure Computation Fall 2022

Instructor, University of Illinois Chicago

- CS494: Introduction to Cryptography Fall 2021
- CS594: Secure Computation Spring 2021

– CS494: Introduction to Cryptography — Fall 2020

Graduate Teaching Assistant, University of California, Berkeley
– CS194: Undergraduate Cryptography — Spring 2019
– CS170: Efficient Algorithms and Intractable Problems — Fall 2017
– CS276: Graduate Cryptography — Fall 2016

Undergraduate Teaching Assistant, Shanghai Jiao Tong University
– CS026: Set Theory and Mathematical Logic — Fall 2012 & Spring 2014

Student Coach, Shanghai Jiao Tong University
– ACM International Collegiate Programming Contest (ICPC) Team — Fall 2012 & Spring 2013

Student Coach, Changzhou Senior High School
– National Programming Contest Team — Fall 2009 & Spring 2010

MENTORING

Ph.D. Students:
– Chao Wu (*Brown University*) — Spring 2021 – Present

M.S. Students:
– Max Tromanhauser (*Brown University*) — Fall 2022 – Present
– Shweta Srinivasan (*University of Illinois Chicago*) — Summer 2021 – Spring 2022

Undergraduate Students:
– Xinyi Shi (*Shanghai Jiao Tong University*) — Fall 2021 – Present
– Ruofan Xu (*Shanghai Jiao Tong University*) — Fall 2021 – Present

Interns at Visa Research:
– Tiancheng Xie (*University of California, Berkeley*) — Summer 2020
– Divya Ravi (*Indian Institute of Science*) — Spring 2020

UNIVERSITY SERVICE

- **Ph.D. Admissions Committee**, CS Department, *Brown Univesrity* — 2022 – 2023
- **Graduate Committee**, CS Department, *University of Illinois Chicago* — 2021 – 2022
- **Ph.D. Admissions Committee**, CS Department, *University of Illinois Chicago* — 2020 – 2021
- **Ph.D. Admissions Committee**, EECS Department, *University of California, Berkeley* — 2017 – 2018
- **Co-Organizer**, Theory Group Student Retreat, *University of California, Berkeley* — 2016 – 2018
- **Organizer**, Theory Group Student Seminar, *University of California, Berkeley* — 2015 – 2017

PROFESSIONAL SERVICE

Workshop Co-Organizer:
– **Mentoring Workshop and Videos** (affiliated workshop of **CRYPTO** 2021)

Conference Program Committee:
– **EUROCRYPT** 2022
International Conference on the Theory and Applications of Cryptology and Information Security
– **CRYPTO** 2021
International Cryptology Conference
– **PKC** 2021
International Conference on Practice and Theory of Public-Key Cryptography

– **AsiaCCS** 2021
ACM ASIA Conference on Computer and Communications Security
– **PPML** 2021 (**@CCS**), 2020 (**@NeurIPS**)
Privacy Preserving Machine Learning Workshop

Grant Panelist:

– **NSF SaTC** 2022
National Science Foundation Secure and Trustworthy Cyberspace Program

External Reviewer:

– **Conference Reviewer:**
CRYPTO 2022, 2020, 2019, 2017, 2016, 2015; **EUROCRYPT** 2020, 2019, 2018 2017; **ASIACRYPT** 2022, 2021, 2020, 2019, 2018, 2017, 2016, 2015; **PKC** 2020, 2019, 2018, 2017, 2016; **TCC** 2021, 2019, 2018, 2017, 2016; **CCS** 2020, 2019, 2016; **FOCS** 2022; **STOC** 2016; **ICALP** 2014; **CT-RSA** 2023; **SCN** 2016; **CANS** 2016; **CESC** 2019.
– **Journal Reviewer: Journal of Cryptology** 2021
– **Grant Reviewer:**
Natural Sciences and Engineering Research Council of Canada (NSERC) 2023
Israel Science Foundation (ISF) 2022
Discovery Partners Institute (DPI) Science Team Seed Grant 2021

TALKS

Updatable Private Set Intersection.
– Invited talk at *Google Crypto Seminar*, New York, NY Nov 2022

Secure Multi-Party Computation: From Theory to Practice.
– Invited talk at *Nature Forum on Empowering Data as A New Asset*, Virtual Dec 2022
– Invited talk at *Harvard CMSA Interdisciplinary Science Seminar*, Virtual Apr 2022
– Seminar talk at *University of Michigan*, Ann Arbor, MI Mar 2022
– Seminar talk at *University of Virginia*, Charlottesville, VA Mar 2022
– Seminar talk at *University of California, Santa Barbara*, Santa Barbara, CA Feb 2022
– Seminar talk at *Brown University*, Virtual Feb 2022
– Seminar talk at *Rutgers University*, Virtual Feb 2022
– Seminar talk at *Pennsylvania State University*, Virtual Feb 2022

Amortizing Rate-1 OT and Applications to PIR and PSI.
– Conference talk at *the 19th Theory of Cryptography Conference (TCC)*, Virtual Nov 2021

Multi-Party Threshold Private Set Intersection with Sublinear Communication.
– Conference talk at *the 24th International Conference on Practice and Theory of Public-Key Cryptography (PKC)*, Virtual May 2021

Private Set Intersection in the Internet Setting From Lightweight Oblivious PRF.
– Conference talk at *the 40th International Cryptology Conference (CRYPTO)*, Virtual Aug 2020

New Results in Private Set Intersection.
– Invited talk at *UC Berkeley Crypto Seminar*, Virtual Aug 2020
– Seminar talk at *Google Crypto Seminar*, New York, NY Oct 2018

Cut-and-Choose for Garbled RAM.
– Conference talk at *Cryptographers' Track at the RSA Conference (CT-RSA)*, San Francisco, CA Feb 2020
– Invited talk at *Bay Area Crypto Day*, University of California, Berkeley, CA Nov 2015

PASTA: PASsword-based Threshold Authentication.
– Invited talk at *Microsoft Research*, Redmond, WA June 2019

- Invited talk at *Baidu Research*, Sunnyvale, CA Dec 2018
- Conference talk at *the 25th ACM Conference on Computer and Communications Security (CCS)*, Toronto, Canada Oct 2018
- Seminar talk at *Google Crypto Seminar*, New York, NY Oct 2018

Two-Round Multiparty Secure Computation Minimizing Public Key Operations.

- Invited talk at *Baidu Research*, Sunnyvale, CA Dec 2018
- Conference talk at *the 38th International Cryptology Conference (CRYPTO)*, University of California, Santa Barbara, CA Aug 2018
- Seminar talk at *Google Crypto Seminar*, New York, NY Aug 2018
- Invited talk at *Bay Area Crypto Day*, Stanford University, CA May 2018
- Seminar talk at *VISA Research Crypto Seminar*, Palo Alto, CA Mar 2018

Laconic Oblivious Transfer and its Applications.

- Lightning talk and poster session at *Rising Stars in EECS*, Stanford University, CA Nov 2017
- Invited talk at *NY CryptoDay*, Columbia University, New York, NY Sept 2017
- Conference talk at *the 37th International Cryptology Conference (CRYPTO)*, University of California, Santa Barbara, CA Aug 2017
- Invited talk at *UW Theory Seminar*, University of Washington, Seattle, WA July 2017
- Invited talk at *China Theory Week*, Shanghai, China July 2017
- Seminar talk at *Microsoft Research Crypto Seminar*, Redmond, WA June 2017
- Contributed talk at *the Theory and Practice of Multi-Party Computation (TPMPC) Workshop*, Bristol, United Kingdom Apr 2017
- Invited talk at *Bay Area Crypto Day*, Visa Research, Palo Alto, CA Apr 2017

Secure Multiparty RAM Computation in Constant Rounds.

- Conference talk at *the 14th Theory of Cryptography Conference (TCC)*, Beijing, China Nov 2016

Decentralized Anonymous Micropayments.

- Lightning talk at *the 1st Blockchain Technologies Summer School*, Corfu, Greece June 2016
- Lightning talk at *the 5th Women in Theory (WIT) Workshop*, Simons Institute, CA May 2016

Secretary Markets with Local Information.

- Conference talk at *the 42nd International Colloquium on Automata, Languages, and Programming (ICALP)*, Kyoto, Japan July 2015

INTERN EXPERIENCE

Google, New York, NY July – Oct 2018
Mentors: Dr. Mariana Raykova, Dr. Karn Seth, Dr. Moti Yung

Facebook, Menlo Park, CA May – July 2018
Mentor: Dr. Kevin Lewi

Visa Research, Palo Alto, CA Feb – Apr 2018
Mentor: Dr. Payman Mohassel

Microsoft Research, Redmond, WA May – Aug 2017
Mentor: Dr. Melissa Chase