Fermi Ma

Personal

Email: fermima@alum.mit.edu
Website: fermima.com

Research Areas

My primary research area is cryptography. I am particularly interested in the interplay between quantum information, interactive protocols, and computational hardness.

Employment

Simons-Berkeley Postdoctoral Fellow & Simons Quantum Postdoctoral Fellow
Simons Institute & UC Berkeley (September 2021–present)
Hosts: Prof. Umesh Vazirani and Prof. Alessandro Chiesa

Education

Ph.D. in Computer Science, Princeton University (September 2021)
Advisor: Prof. Mark Zhandry
Thesis: Quantum Security and Fiat-Shamir for Cryptographic Protocols

M.A. in Computer Science, Princeton University (September 2017)
Advisor: Prof. Mark Zhandry

B.S. in Mathematics, Massachusetts Institute of Technology (June 2015)
GPA: 4.93/5.00

Visits & Internships

- Visiting Graduate Student, Simons Institute (Spring 2020)
  Program: "Lattices: Algorithms, Complexity, and Cryptography"
- Research Intern, NTT Research (October 2019–August 2021)
  Host: Dr. Justin Holmgren and Prof. Mark Zhandry
- Visiting Graduate Student, UC Berkeley EECS Department (August 2019–May 2020)
  Host: Prof. Alessandro Chiesa
- Visiting Graduate Student, Simons Institute (Fall 2019)
  Program: "Proofs, Consensus, and Decentralizing Society"
- Research Intern, Visa Research (June–September 2019)
  Hosts: Dr. Pratyay Mukherjee, Dr. Daniel Masny, and Dr. Yilei Chen

– Visiting Graduate Student, IDC Herzliya FACT Center (January–February 2019)
Hosts: Prof. Alon Rosen and Prof. Elette Boyle

– Research Intern, SRI International (June–September 2018)
Host: Dr. Tancrède Lepoint

Papers

1. Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier
   Alessandro Chiesa, Fermi Ma, Nicholas Spooner, and Mark Zhandry
   FOCS 2021 (62nd Annual Symposium on Foundations of Computer Science)
   QCRYPT 2021
   ePrint: ia.cr/2021/334

2. One-Way Functions Imply Secure Computation in a Quantum World
   James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma
   CRYPTO 2021 (41st Annual International Cryptology Conference)
   QIP 2021 (24th Annual Conference on Quantum Information Processing)
   - one of three papers in QIP 2021 selected for a **long plenary talk**.

   QCRYPT 2021 invited talk
   ePrint: ia.cr/2020/1487

3. On The Round Complexity of Secure Quantum Computation
   James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma
   CRYPTO 2021 (41st Annual International Cryptology Conference)
   QIP 2021 (24th Annual Conference on Quantum Information Processing)
   QCRYPT 2021
   ePrint: ia.cr/2020/1471

4. Does Fiat-Shamir Require a Cryptographic Hash Function?
   Yilei Chen, Alex Lombardi, Fermi Ma, and Willy Quach
   CRYPTO 2021 (41st Annual International Cryptology Conference)
   ePrint: ia.cr/2020/915

5. Leakage-Resilient Key Exchange and Two-Seed Extractors
   Xin Li, Fermi Ma, Willy Quach, and Daniel Wichs
   CRYPTO 2020 (40th Annual International Cryptology Conference)
   ePrint: ia.cr/2020/771

6. Affine Determinant Programs: A Framework for Obfuscation and Witness Encryption

   James Bartusek, Yuval Ishai, Aayush Jain, Fermi Ma, Amit Sahai, and Mark Zhandry)

   ITCS 2020 (Innovations in Theoretical Computer Science 2020)

   ePrint: ia.cr/2020/889

7. On the (In)security of Kilian-Based SNARGs

   James Bartusek, Liron Bronfman, Justin Holmgren, Fermi Ma, and Ron D. Rothblum

   TCC 2019 (Theory of Cryptography Conference 2019)

   ePrint: ia.cr/2019/997

8. Public-Key Function Private Hidden Vector Encryption and More

   James Bartusek, Brent Carmer, Abhishek Jain, Zhengzhong Jin, Tancrède Lepoint, Fermi Ma, Tal Malkin, Alex J. Malozemoff, and Mariana Raykova

   ASIACRYPT 2019 (25th Annual International Conference on the Theory and Application of Cryptology and Information Security)

   ePrint: ia.cr/2019/746

9. The Distinction Between Fixed and Random Generators in Group-Based Assumptions

   James Bartusek, Fermi Ma, and Mark Zhandry

   CRYPTO 2019 (39th Annual International Cryptology Conference).

   ePrint: ia.cr/2019/202

10. New Techniques for Obfuscating Conjunctions

    James Bartusek, Tancrède Lepoint, Fermi Ma, and Mark Zhandry

    EUROCRYPT 2019 (38th Annual International Conference on the Theory and Applications of Cryptographic Techniques)

    ePrint: ia.cr/2018/936

11. Return of GGH15: Provable Security Against Zeroizing Attacks

    James Bartusek, Jiaxin Guan, Fermi Ma, and Mark Zhandry

    TCC 2018 (Theory of Cryptography Conference 2018)

    ePrint: ia.cr/2018/511

12. The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks

    Fermi Ma and Mark Zhandry

    TCC 2018 (Theory of Cryptography Conference 2018)

    ePrint: ia.cr/2017/946

13. Encryptor Combiners: A Unified Approach to Multiparty NIKE, (H)IBE, and Broadcast Encryption

    Fermi Ma and Mark Zhandry

    ePrint: ia.cr/2017/152

Talks

1. Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier
   - Tel Aviv University and Weizmann Seminar (April 2021)
   - Cornell Crypto Seminar (April 2021)
   - NTT Research (April 2021)
   - MIT Cryptography and Information Seminar (May 2021)
   - QCRYPT 2021 (August 2021)
2. Does Fiat Shamir Require a Cryptographic Hash Function?
   - UIUC Cryptography Group (November 2020)
   - NTT Research (August 2020)
   - CRYPTO 2021 (August 2021)
3. On the (In)security of Kilian-Based SNARGs
   - Tokyo Crypto Day (December 2019)
   - Charles River Crypto Day (November 2019)
4. Public-Key Function Private Hidden Vector Encryption and More
   - ASIACRYPT 2019 Conference Talk (December 2019)
5. The Distinction Between Fixed and Random Generators in Group-Based Assumptions
   - CRYPTO 2019 Conference Talk (August 2019)
6. Affine Determinant Programs: A New Approach to Obfuscation
   - New Roads to Cryptopia Workshop, a CRYPTO 2019 affiliated event (August 2019)
7. New Techniques for Obfuscating Conjunctions
   - EUROCRYPT 2019 Conference Talk (May 2019)
   - New York Crypto Day (May 2019)
   - UC Berkeley Cryptography Seminar (February 2019)
   - Weizmann Institute of Science Cryptography Seminar (February 2019)
   - Technion Theory Lunch (January 2019)

- IDC Herzliya (January 2019)
- SRI International (August 2018)

8. The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks
   - TCC 2018 Conference Talk (November 2018)
   - UCLA Cryptography Seminar (April 2018)
9. Encryptor Combiners: A Unified Approach to Multiparty NIKE, (H)IBE, and Broadcast Encryption
   - Princeton General Exam (May 2017)

Teaching

- COS 533: Advanced Cryptography (Fall 2017), Assistant in Instruction for Prof. Mark Zhandry.
- COS 433: Cryptography (Spring 2017), Assistant in Instruction for Prof. Mark Zhandry.
- COS 521: Advanced Algorithms (Fall 2016), Assistant in Instruction for Prof. Sanjeev Arora and Dr. Pravesh Kothari.

Service

I have been an external reviewer for the following conferences: CRYPTO (2018, 2019, 2020, 2021), EUROCRYPT (2019, 2020, 2021), ASIACRYPT (2019, 2020), TCC (2017, 2019, 2020, 2021), PKC (2018, 2021), STOC (2019, 2020, 2021), SODA (2020), ITCS (2019, 2021), QCRYPT (2021).

In Spring 2019, I organized the cryptography reading group at Princeton.

In Spring 2020, I helped organize the "Quantum Cryptography for Dummies" lecture series at the Simons Institute as part of the "Lattices: Algorithms, Complexity, and Cryptography" program. I gave lectures on Grover's algorithm and post-quantum commitments to audiences of 15-25 cryptographers.

References

Prof. Mark Zhandry (advisor). Email: mzhandry@princeton.edu

Prof. Alessandro Chiesa. Email: alexch@berkeley.edu

Dr. Justin Holmgren. Email: holmgren@alum.mit.edu

Dr. Tancrède Lepoint. Email: tancrede.lepoint@gmail.com