Fermi Ma

Personal

Email: fermima1@gmail.com
Website: https://fermima.com

Research Area

My research focuses on quantum computing and its implications for cryptography, complexity theory, and physics.

Employment

Simons-Berkeley Postdoctoral Fellow & Simons Quantum Postdoctoral Fellow
Simons Institute & UC Berkeley (September 2021–present)
Hosts: Prof. Umesh Vazirani (September 2021–present) and Prof. Alessandro Chiesa (September 2021–August 2022)

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

Papers

Authors on all papers are in alphabetical order, unless otherwise noted.

1. How to Construct Random Unitaries

   Fermi Ma and Hsin-Yuan Huang

   (author ordering by contribution)

   In Submission

2. A One-Query Lower Bound for Unitary Synthesis and Breaking Quantum Cryptography

   Alex Lombardi, Fermi Ma, and John Wright

   STOC 2024 (56th Annual ACM Symposium on Theory of Computing)

QIP 2024 (27th Annual Conference on Quantum Information Processing)

3. Commitments to Quantum States

   Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry

   STOC 2023 (55th Annual ACM Symposium on Theory of Computing)

   QIP 2023 (26th Annual Conference on Quantum Information Processing)

   Invited to the SICOMP Special Issue for STOC 2023

4. Post-Quantum Zero Knowledge, Revisited (Or: How to Do Quantum Rewinding Undetectably)

   Alex Lombardi, Fermi Ma, and Nicholas Spooner

   FOCS 2022 (63rd Annual Symposium on Foundations of Computer Science)

   QIP 2023 (26th Annual Conference on Quantum Information Processing)

5. Succinct Classical Verification of Quantum Computation

   James Bartusek, Yael Kalai, Alex Lombardi, Fermi Ma, Giulio Malavolta, Vinod Vaikuntanathan, Thomas Vidick, and Lisa Yang

   CRYPTO 2022 (42nd Annual International Cryptology Conference)

6. 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)

   QIP 2022 (25th Annual Conference on Quantum Information Processing)

   Invited to the SICOMP Special Issue for FOCS 2021

7. 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.

8. 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)

9. Does Fiat-Shamir Require a Cryptographic Hash Function?

   Yilei Chen, Alex Lombardi, Fermi Ma, and Willy Quach

   CRYPTO 2021 (41st Annual International Cryptology Conference)

10. Leakage-Resilient Key Exchange and Two-Seed Extractors

    Xin Li, Fermi Ma, Willy Quach, and Daniel Wichs

    CRYPTO 2020 (40th Annual International Cryptology Conference)

11. 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)

12. 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)

13. 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)

14. 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).

15. 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)

16. Return of GGH15: Provable Security Against Zeroizing Attacks

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

    TCC 2018 (Theory of Cryptography Conference 2018)

17. 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)

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

    Fermi Ma and Mark Zhandry

Talks

Slides and recordings of my talks are available at fermima.com

1. How to Construct Random Unitaries
   - UT Austin (Nov 2024)
   - Simons Quantum Colloquium (Nov 2024)
   - Stanford QFARM Workshop on Thermalization and Quantum Information (Oct 2024)
   - Institute for Advanced Study (Aug 2024)
   - Simons Workshop on Pseudorandom Unitaries (May 2024)
2. Pseudorandom States and the Purification Trick
   - Simons Workshop on Pseudorandom States and Unitaries (Mar 2024)
3. A One-Query Lower Bound for Unitary Synthesis and Breaking Quantum Cryptography
   - QIP 2024 (Jan 2024)
   - Stanford Theory Lunch (Dec 2023)
   - Waterloo Quantum Innovators Workshop (Nov 2023)
   - MIT Theory of Computation Colloquium (Nov 2023)
4. Quantum Commitments and Black Hole Radiation Decoding
   - Simons Quantum Summer Cluster Workshop (Jul 2023)
5. Commitments to Quantum States
   - Minimal Complexity Assumptions for Cryptography Workshop at the Simons Institute (May 2023)
   - Stanford (Jan 2023)
   - Charles River Crypto Day (Dec 2022)
6. Post-Quantum Zero Knowledge, Revisited
   - QIP 2023 (Feb 2023)
   - FOCS 2022 (Nov 2022)
7. Quantum Rewinding Tutorial
   - IPAM Graduate Summer School on Post-quantum and Quantum Cryptography (Jul 2022)
   - Quantum and Lattices Joint Reunion Workshop at the Simons Institute (Jun 2022)
8. Post-Quantum Succinct Arguments: Breaking the Quantum Rewinding Barrier
   - QIP 2022 (Mar 2022)

- Simons Quantum Colloquium (Oct 2021)
- QCRYPT 2021 (Aug 2021)
- MIT Cryptography and Information Seminar (May 2021)
- NTT Research (Apr 2021)
- Cornell Crypto Seminar (Apr 2021)
- Tel Aviv University and Weizmann Seminar (Apr 2021)

9. Does Fiat Shamir Require a Cryptographic Hash Function?
   - CRYPTO 2021 (Aug 2021)
   - UIUC Cryptography Group (Nov 2020)
   - NTT Research (Aug 2020)
10. On the (In)security of Kilian-Based SNARGs
    - Tokyo Crypto Day (Dec 2019)
    - Charles River Crypto Day (Nov 2019)
11. Public-Key Function Private Hidden Vector Encryption and More
    - ASIACRYPT 2019 (Dec 2019)
12. The Distinction Between Fixed and Random Generators in Group-Based Assumptions
    - CRYPTO 2019 (Aug 2019)
13. Affine Determinant Programs: A New Approach to Obfuscation
    - New Roads to Cryptopia Workshop, a CRYPTO 2019 affiliated event (Aug 2019)
14. New Techniques for Obfuscating Conjunctions
    - EUROCRYPT 2019 (May 2019)
    - New York Crypto Day (May 2019)
    - UC Berkeley Cryptography Seminar (Feb 2019)
    - Weizmann Institute of Science Cryptography Seminar (Feb 2019)
    - Technion Theory Lunch (Jan 2019)
    - IDC Herzliya (Jan 2019)
    - SRI International (Aug 2018)
15. The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks
    - TCC 2018 (Nov 2018)
    - UCLA Cryptography Seminar (Apr 2018)

Service

I have served on (or will serve on) the following program committees: QIP 2025, TCC 2024, CRYPTO 2023, ITCS 2023, Quantum Cryptography Workshop (QCW) at ASIACRYPT 2022, TCC 2022, CRYPTO 2022.