Fermi Ma

Personal

Department of Computer Science, Princeton University
194 Nassau Street, Princeton, NJ 08540, USA
Birthdate: January 7, 1994
Email: fermima@alum.mit.edu
Website: https://cs.princeton.edu/~fermim
Citizenship: United States

Education

Ph.D. Candidate in Computer Science, Princeton University (present)
Advisor: Prof. Mark Zhandry

M.A. in Computer Science, Princeton University (September 2017)
Advisor: Prof. Mark Zhandry · GPA: 3.9/4.0

B.S. in Mathematics, Massachusetts Institute of Technology (June 2015)
GPA: 4.9/5.0

Experience

Research Intern, NTT Research (October 2019–present)

Visiting Graduate Student, UC Berkeley EECS Department (August 2019–present)
Host: Prof. Alessandro Chiesa

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

Publications

- "Affine Determinant Programs: A Framework for Obfuscation and Witness Encryption" (with James Bartusek, Yuval Ishai, Aayush Jain, Amit Sahai, and Mark Zhandry), *Innovations in Theoretical Computer Science (ITCS 2020)*.
- "On the (In)security of Kilian-Based SNARGs" (with James Bartusek, Liron Bronfman, Justin Holmgren, and Ron D. Rothblum), *Theory of Cryptography Conference (TCC 2019)*. ePrint: https://ia.cr/2019/997
- "Public-Key Function Private Hidden Vector Encryption and More" (with James Bartusek, Brent Carmer, Abhishek Jain, Zhengzhong Jin, Tancrède Lepoint, Tal Malkin, Alex J. Malozemoff, and Mariana Raykova), *25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2019)*. ePrint: https://ia.cr/2019/746

- "The Distinction Between Fixed and Random Generators in Group-Based Assumptions" (with James Bartusek and Mark Zhandry), *39th Annual International Cryptology Conference (CRYPTO 2019)*. ePrint: `https://ia.cr/2019/202`
- "New Techniques for Obfuscating Conjunctions" (with James Bartusek, Tancrède Lepoint, and Mark Zhandry), *38th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019)*. ePrint: `https://ia.cr/2018/936`
- "Return of GGH15: Provable Security Against Zeroizing Attacks" (with James Bartusek, Jiaxin Guan, and Mark Zhandry), *Theory of Cryptography Conference (TCC 2018)*. ePrint: `https://ia.cr/2018/511`
- "The MMap Strikes Back: Obfuscation and New Multilinear Maps Immune to CLT13 Zeroizing Attacks" (with Mark Zhandry), *Theory of Cryptography Conference (TCC 2018)*. ePrint: `https://ia.cr/2017/946`
- "Arboral Satisfaction: Recognition and LP Approximation" (with Erik D. Demaine, Varun Ganesan, Vladislav Kontsevoi, Qipeng Liu, Quanquan Liu, Ofir Nachum, Aaron Sidford, Erik Waingarten, and Daniel Ziegler), *Information Processing Letters Volume 127, pages 1-5, 2017*.
- "The Fewest Clues Problem" (with Erik D. Demaine, Ariel Schvartzman, Erik Waingarten, and Scott Aaronson), *Proceedings of the 8th International Conference on Fun with Algorithms, 12:1-12:12, 2016. Invited to a special issue of Theoretical Computer Science*.
- "You Should Be Scared of German Ghost" (with Erik D. Demaine, Matt Susskind, and Erik Waingarten), *Journal of Information Processing, volume 23, number 3, pages 293-298, 2015*.
- "Playing Dominoes is Hard, Except by Yourself" (with Erik D. Demaine and Erik Waingarten), *Proceedings of the 7th International Conference on Fun with Algorithms, pages 137-146, 2014*.

Preprints

- "Encryptor Combiners: A Unified Approach to Multiparty NIKE, (H)IBE, and Broadcast Encryption" (with Mark Zhandry), ePrint: `https://ia.cr/2017/152`

Talks

- "On the (In)security of Kilian-Based SNARGs"
  - *Charles River Crypto Day, November 2019*.
- "Affine Determinant Programs: A New Approach to Obfuscation"
  - *New Roads to Cryptopia Workshop, a CRYPTO 2019 affiliated event, August 2019*.
- "New Techniques for Obfuscating Conjunctions"
  - *SRI International, August 2018*.
  - *IDC Herzliya, January 2019*.
  - *Technion Theory Lunch, January 2019*.

  - *Weizmann Institute of Science Cryptography Seminar, February 2019*
  - *UC Berkeley Cryptography Seminar, February 2019*
  - *New York Crypto Day, May 2019*
- "A Weak Model for the CLT13 Multilinear Maps"
  - *UCLA Cryptography Seminar, April 2018.*
- "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: TCC 2017, PKC 2018, CRYPTO 2018, CT-RSA 2018, EUROCRYPT 2019, STOC 2019, CRYPTO 2019, ASIACRYPT 2019, TCC 2019, ITCS 2019.

At Princeton, I ran the cryptography reading group for the spring 2019 semester.

References

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

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