Mahimna Kelkar

mahimna@cs.cornell.edu | cs.cornell.edu/~mahimna

Education

Cornell University *Aug 2018 - Present*
Ph.D. in Computer Science
Research Focus: Applied Cryptography and Foundations of Security for Decentralized Systems
Advisor - Ari Juels

Purdue University *Aug 2015 - May 2018*
Bachelor of Science in Computer Science, Mathematics, and Statistics *GPA: 4.0/4.0*
Graduated Honors with Highest Distinction

Representative Publications

— Order-Fairness for Byzantine Consensus. CRYPTO 2020.
Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels.
— Themis: Fast, Strong Order-Fairness in Byzantine Consensus. CCS 2023.
Mahimna Kelkar, Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan.
— Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts. IEEE S&P 2023.
Kushal Babel*, Philip Daian*, Mahimna Kelkar*, and Ari Juels.
— MPC-Friendly Symmetric Cryptography from Alternating Moduli: Candidates, Protocols, and Applications. CRYPTO 2021.
Itai Dinur, Steven Goldfeder, Tzipora Halevi, Yuval Ishai, Mahimna Kelkar**, Vivek Sharma, Greg Zaverucha (alphabetical author ordering).
— Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets. In Submission.
Mahimna Kelkar, Kushal Babel, Phillip Daian, James Austgen, Vitalik Buterin, and Ari Juels.

Honors

2023 **Google Collaboration Grant** (with Yuval Ishai)
2021 **Best Paper Award at APKC 2022** for the Permissionless order-fairness paper
2021 **Smart Contract Research Forum Impact Award** for the Clockwork Finance paper
2021-2022 **Ethereum-IC3 PhD Fellowship**
2018 **Outstanding Statistics Student**, Purdue University
2014 **Indian National Mathematics Olympiad Scholar**

Research Visits and Internships

2022 - pres **Offchain Labs Research** (Part time) mentored by Ed Felten
Summer 2023 **a16zcrypto Research** hosted by Joseph Bonneau, Valeria Nikolaenko, and Tim Roughgarden
Spring 2022 **Technion** hosted by Yuval Ishai
Summer 2021 **Novi (Facebook) Research**
Summer 2020 **Google Research** hosted by Mariana Raykova and Karn Seth
Summer 2018 **Sandia National Labs**

Professional Service

Program Committee FC 2024, DeFi@FC {2023, 2024}
External Reviewer FC 2020, CRYPTO {2020, 2021, 2024}, Eurocrypt 2022, DISC 2022, CCS 2022, USENIX Security 2020, DES Journal, AFT 2023, PODC 2024

All Publications and Preprints

* denotes equal first-author contribution
** denotes alphabetical author ordering

19. [In Submission] DAO Decentralization: Voting-Bloc Entropy, Bribery, and Dark DAOs. arxiv.org/abs/2311.03530.
James Austgen, Andrés Fábrega, Sarah Allen, Kushal Babel, Mahimna Kelkar, and Ari Juels.
18. [In Submission] Complete Knowledge: Preventing Encumbrance of Cryptographic Secrets. ia.cr/2023/044.
Mahimna Kelkar*, Kushal Babel*, Philip Daian*, James Austgen, Vitalik Buterin, and Ari Juels.

---

17. **[CCS 2024]** Computationally Secure Aggregation and Private Information Retrieval in the Shuffle Model.
Adrià Gasón, Yuval Ishai, Mahimna Kelkar**, Baiyu Li, Yiping Ma, Mariana Raykova.
16. **[CCS 2024]** Interactive Authentication. ia.cr/2022/1682.
Deepak Maram, Mahimna Kelkar, and Ittay Eyal.
15. **[CRYPTO 2024]** Compressing Unit-Vector Correlations via Sparse Pseudorandom Generators.
Amit Agarwal, Elette Boyle, Niv Gilboa, Yuval Ishai, Mahimna Kelkar**, Yiping Ma.
14. [FC 2024] GoAT: File Geolocation via Anchor Timestamping. ia.cr/2021/697.
Deepak Maram, Iddo Bentov, Mahimna Kelkar, and Ari Juels.
13. [FC 2024] Truncator: Time-space Tradeoff of Cryptographic Primitives. ia.cr/2021/697.
Foteini Baldimtsi, Konstantinos Chalkias, Panagiotis Chatzigiannis, and Mahimna Kelkar**.
12. **[CCS 2023]** Lanturn: Measuring Economic Security of Smart Contracts Through Adaptive Learning.
ia.cr/2023/1338.
Kushal Babel, Mojan Javaheripi, Yan Ji, Mahimna Kelkar, Farinaz Koushanfar, and Ari Juels.
11. **[CCS 2023]** Themis: Fast, Strong Order-Fairness in Byzantine Consensus. ia.cr/2021/1465.
Mahimna Kelkar, Soubhik Deb, Sishan Long, Ari Juels, and Sreeram Kannan.
10. [WPES 2023] Zef: Low-latency, Scalable, Private Payments. ia.cr/2022/083.
Mathieu Baudet, Alberto Sonnino, Mahimna Kelkar, and George Danezis
9. [AFT 2023] Buying Time: Latency Racing vs. Bidding for Transaction Ordering. arxiv.org/abs/2306.02179
Akaki Mamageishvili, Mahimna Kelkar, Jan Christoph Schlegel, and Edward Felten.
8. [AFT 2023] STROBE: Streaming Threshold Random Beacons. ia.cr/2021/1643.
Donald Beaver, Konstantinos Chalkias, Mahimna Kelkar**, Lefteris Kokoris Kogias, Kevin Lewi, Ladi de Naurois, Valeria Nikolaenko, Arnab Roy, and Alberto Sonnino.
7. **[CRYPTO 2023]** One-Message Secure Reductions: On the Cost of Converting Correlations. ia.cr/2023/1225.
Yuval Ishai, Mahimna Kelkar**, Varun Narayanan, and Liav Zafar.
6. **[IEEE S&P 2023]** Clockwork Finance: Automated Analysis of Economic Security in Smart Contracts.
ia.cr/2021/1147. Smart Contract Research Forum Impact Award.
Kushal Babel*, Philip Daian*, Mahimna Kelkar*, and Ari Juels.
5. **[USENIX Security 2022]** Secure Poisson Regression ia.cr/2021/208.
Mahimna Kelkar, Phi Hung Le, Mariana Raykova, and Karn Seth.
4. [APKC 2022] Order-Fair Consensus in the Permissionless Setting. ia.cr/2021/139. Best Paper Award.
Mahimna Kelkar, Soubhik Deb, and Sreeram Kannan
3. **[CRYPTO 2021]** MPC-Friendly Symmetric Cryptography from Alternating Moduli: Candidates, Protocols, and Applications. ia.cr/2021/885.
Itai Dinur, Steven Goldfeder, Tzipora Halevi, Yuval Ishai, Mahimna Kelkar**, Vivek Sharma, and Greg Zaverucha.
2. **[CRYPTO 2020]** Order-Fairness for Byzantine Consensus. ia.cr/2020/269.
Mahimna Kelkar, Fan Zhang, Steven Goldfeder, and Ari Juels.
1. [ESORICS 2019] Flexible Signatures: Making Authentication Suitable for Real-Time Environments. ia.cr/2018/343.
Duc V. Le, Mahimna Kelkar, and Aniket Kate.