Hemanta K. Maji

homepage email

Research Interests

Cryptography, Information theory.

Education

2005–2011 Ph.D. in Computer Science, University of Illinois, Urbana-Champaign, Thesis Title: On Computational Intractability Assumptions in Cryptography.
(Advisor: Manoj Prabhakaran)

2000–2004 B.Tech. in Computer Science, Indian Institute of Technology, Kanpur, B.Tech. Project Title: Solving Traveling Salesman Problem in Classical and Quantum paradigm.
(Best B.Tech. Project Award)

Major Appointments

2023–present Associate Professor, Department of Computer Science, Purdue University, West Lafayette

2015–2023 Assistant Professor, Department of Computer Science, Purdue University, West Lafayette

2013–2015 Post-doctoral Researcher (Center Fellow), Department of Computer Science, University of California, Los Angeles & Center for Encrypted Functionalities

2011–2013 Post-doctoral Researcher (Computing Innovation Fellow), Department of Computer Science, University of California, Los Angeles

Publications

Book Chapters

1. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: Complexity of Multi-Party Computation Functionalities. Secure Multi-Party Computation, 2013, 249–283.

Journal Publications

1. Kalyan Garapaty, Hemanta K. Maji, Daniel Lokshtanov, Alex Pothen: The Chromatic Number of Squares Of Random Graphs. Special Issue on Applied Combinatorial Methods in the Journal of Combinatorics (JOC), 2022

2. Donghang Lu, Albert Yu, Aniket Kate, Hemanta K. Maji: Polymath: Low-Latency MPC via Secure Polynomial Evaluations and Its Applications. Proceedings on Privacy Enhancing Technologies, 2022(1): 396-416 (2022)

3. Hemanta K. Maji: Computational Hardness of Collective Coin-Tossing Protocols. Entropy 23(1): 44 (2021)

Conference Publications

Historical acceptance rates (TCC, CHES, PKC, FSE, ASIACRYPT, EUROCRYPT, CRYPTO)

1. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Xiuyu Ye: Constructing Leakage-resilient Shamir's Secret Sharing: Over Composite Order Fields. EUROCRYPT, 2024, .

2. Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, Hai H. Nguyen: Randomized Functions with High Round Complexity. TCC, 2023, .

3. Donghang Lu, Albert Yu, Aniket Kate, Hemanta K. Maji: IM: Secure Interval Membership Testing and Applications to Secure Comparison. Euro S&P, 2023, 757-772.

4. Saugata Basu, Hamidreza Amini Khorasgani, Hemanta K. Maji, Hai H. Nguyen: Geometry of Secure Two-party Computation. FOCS, 2022, 1035-1044.

5. Hamidreza Amini Khorasgani, Hemanta K. Maji, Hai H. Nguyen: Secure Non-interactive Simulation: Feasibility and Rate. EUROCRYPT, 2022, 767-796.

6. Hamidreza Amini Khorasgani, Hemanta K. Maji, Hai H. Nguyen: Secure Non-Interactive Simulation from Arbitrary Joint Distribution. TCC, 2022, .

7. emanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, Albert Yu: Leakage-Resilient Linear Secret-sharing against Arbitrary Bounded-size Leakage Family. TCC, 2022, .

8. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, Albert Yu: Tight Estimate of the Local Leakage Resilience of the Additive Secret-sharing Scheme and its Consequences. Conference on Information-Theoretic Cryptography (ITC), 2022, 16:1-16:19.

9. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Mingyuan Wang: Improved Bound on the Local Leakage-resilience of Shamir's Secret Sharing. IEEE International Symposium on Information Theory (ISIT), 2022, .

10. Hemanta K. Maji, Mingyuan Wang: Computational Hardness of Optimal Fair Computation: Beyond Minicrypt. CRYPTO, 2021, 33-63.

11. Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang: On Leakage Resilient Secret Sharing. CRYPTO, 2021, 779-808.

12. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang: Leakage-resilient Secret-sharing Schemes against Physical-bit Leakage. EUROCRYPT, 2021, 344-374.

13. Alexander R. Block, Simina Brânzei, Hemanta K. Maji, Himanshi Mehta, Tamalika Mukherjee, Hai H. Nguyen: P_4-free Partition and Cover Numbers & Applications. Conference on Information-Theoretic Cryptography (ITC), 2021, 16:1-16:25.

14. Donald Q. Adams, Hemanta K. Maji, Hai H. Nguyen, Minh L. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang: Lower Bounds for Leakage-Resilient Secret Sharing Schemes against Probing Attacks. IEEE International Symposium on Information Theory (ISIT), 2021, 976-981.

15. Hemanta K. Maji, Himanshi Mehta, Mingyuan Wang: Efficient Distributed Coin-tossing Protocols. IEEE International Symposium on Information Theory (ISIT), 2021, 2852-2857.

16. Hamidreza Amini Khorasgani, Hemanta K. Maji, Mingyuan Wang: Optimally-secure Coin-tossing against a Byzantine Adversary. IEEE International Symposium on Information Theory (ISIT), 2021, 2858-2863.

17. Hemanta K. Maji, Mingyuan Wang: Black-Box Use of One-Way Functions is Useless for Optimal Fair Coin-Tossing. CRYPTO, 2020, 593–617.

18. Xin Cheng, Hemanta K. Maji, Alex Pothen: Graphs with Tunable Chromatic Numbers for Parallel Coloring. SIAM Workshop on Combinatorial Scientific Computing (CSC), 2020, 54–64.

19. Divya Gupta, Hemanta K. Maji, Mingyuan Wang: Explicit Rate-1 Non-malleable Codes for Local Tampering. CRYPTO, 2019, 435–466.

20. Hamidreza Amini Khorasgani, Hemanta K. Maji, Tamalika Mukherjee: Estimating Gaps in Martingales and Applications to Coin-Tossing: Constructions and Hardness. Theory of Cryptography Conference (TCC), 2019, 333–355.

21. Divya Gupta, Hemanta K. Maji, Mingyuan Wang: Non-malleable Codes Against Lookahead Tampering. INDOCRYPT, 2018, 307–328.

22. Alexander R. Block, Hemanta K. Maji, Hai H. Nguyen: Secure Computation with Constant Communication Overhead Using Multiplication Embeddings. INDOCRYPT, 2018, 375–398.

23. Alexander R. Block, Divya Gupta, Hemanta K. Maji, Hai H. Nguyen: Secure Computation Using Leaky Correlations (Asymptotically Optimal Constructions). Theory of Cryptography Conference (TCC), 2018, 36–65.

24. Alexander R. Block, Hemanta K. Maji, Hai H. Nguyen: Secure Computation Based on Leaky Correlations: High Resilience Setting. CRYPTO, 2017, 3–32.

25. Amisha Jhanji, Hemanta K. Maji, Raphael Arkady Meyer: Characterizing optimal security and round-complexity for secure OR evaluation. IEEE International Symposium on Information Theory (ISIT), 2017, 2703–2707.

26. Tianhao Wang, Huangyi Ge, Omar Chowdhury, Hemanta K. Maji, Ninghui Li: On the Security and Usability of Segment-based Visual Cryptographic Authentication Protocols. ACM Conference on Computer and Communications Security (CCS), 2016, 603–615.

27. Dakshita Khurana, Hemanta K. Maji, Amit Sahai: Secure Computation from Elastic Noisy Channels. EUROCRYPT, 2016, 184–212.

28. Dakshita Khurana, Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, Amit Sahai: All Complete Functionalities are Reversible. EUROCRYPT, 2016, 213–242.

29. Vipul Goyal, Yuval Ishai, Hemanta K. Maji, Amit Sahai, Alexander A. Sherstov: Bounded-Communication Leakage Resilience via Parity-Resilient Circuits. FOCS, 2016, 1–10.

30. Divesh Aggarwal, Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran: Optimal Computational Split-state Non-malleable Codes. Theory of Cryptography Conference (TCC), 2016, 393–417.

31. Jean-Sébastien Coron, Craig Gentry, Shai Halevi, Tancrède Lepoint, Hemanta K. Maji, Eric Miles, Mariana Raykova, Amit Sahai, Mehdi Tibouchi: Zeroizing Without Low-Level Zeroes: New MMAP Attacks and their Limitations. CRYPTO, 2015, 247–266.

32. Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran: Explicit Non-malleable Codes Against Bit-Wise Tampering and Permutations. CRYPTO, 2015, 538–557.

33. Divya Gupta, Yuval Ishai, Hemanta K. Maji, Amit Sahai: Secure Computation from Leaky Correlated Randomness. CRYPTO, 2015, 701–720.

34. Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran: A Rate-Optimizing Compiler for Non-malleable Codes Against Bit-Wise Tampering and Permutations. Theory of Cryptography Conference (TCC), 2015, 375–39.

35. Dakshita Khurana, Hemanta K. Maji, Amit Sahai: Black-Box Separations for Differentially Private Protocols. ASIACRYPT, 2014, 386–405.

36. Daniel Kraschewski, Hemanta K. Maji, Manoj Prabhakaran, Amit Sahai: A Full Characterization of Completeness for Two-Party Randomized Function Evaluation. EUROCRYPT, 2014, 659–676.

37. Mohammad Mahmoody, Hemanta K. Maji, Manoj Prabhakaran: Limits of random oracles in secure computation. ITCS, 2014, 23–34.

38. Yuval Ishai, Hemanta K. Maji, Amit Sahai, Jürg Wullschleger: Single-use OT combiners with near-optimal resilience. IEEE International Symposium on Information Theory (ISIT), 2014, 1544–1548.

39. Mohammad Mahmoody, Hemanta K. Maji, Manoj Prabhakaran: On the Power of Public-Key Encryption in Secure Computation. Theory of Cryptography Conference (TCC), 2014, 240–264.

40. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: A Unified Characterization of Completeness and Triviality for Secure Function Evaluation. INDOCRYPT, 2012, 40–59.

41. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: Attribute-Based Signatures. CT-RSA, 2011, 376–392.

42. Vipul Goyal, Hemanta K. Maji: Stateless Cryptographic Protocols. FOCS, 2011, 678–687.

43. Hemanta K. Maji, Manoj Prabhakaran: The Limits of Common Coins: Further Results. INDOCRYPT, 2011, 344–358.

44. Hemanta K. Maji, Pichayoot Ouppaphan, Manoj Prabhakaran, Mike Rosulek: Exploring the Limits of Common Coins Using Frontier Analysis of Protocols. Theory of Cryptography Conference (TCC), 2011, 486–503.

45. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: A Zero-One Law for Cryptographic Complexity with Respect to Computational UC Security. CRYPTO, 2010, 595–612.

46. Hemanta K. Maji, Manoj Prabhakaran, Amit Sahai: On the Computational Complexity of Coin Flipping. FOCS, 2010, 613–622.

47. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: Cryptographic Complexity Classes and Computational Intractability Assumptions. ICS, 2010, 266–289.

48. Hemanta K. Maji, Manoj Prabhakaran, Mike Rosulek: Complexity of Multi-party Computation Problems: The Case of 2-Party Symmetric Secure Function Evaluation. Theory of Cryptography Conference (TCC), 2009, 256–273.

49. Raghavendra Udupa, Hemanta K. Maji: Computational Complexity of Statistical Machine Translation. EACL, 2006, .

50. Tanveer A. Faruquie, Hemanta K. Maji, Raghavendra Udupa: A New Decoding Algorithm for Statistical Machine Translation: Design and Implementation. ALENEX/ANALCO, 2005, 180–194.

51. Raghavendra Udupa, Hemanta K. Maji: Theory of Alignment Generators and Applications to Statistical Machine Translation. IJCAI, 2005, 1142–1147.

52. Raghavendra Udupa, Tanveer A. Faruquie, Hemanta K. Maji: An Algorithmic Framework for Solving the Decoding Problem in Statistical Machine Translation. COLING, 2004, 631–637.

53. Hemanta K. Maji, Prateek Jain: Generic System to Evolve Memory and Recall Based Fuzzy Controllers for Anytime Learning. IICAI, 2003, 1364–1373.

Unpublished Drafts & Manuscripts under Preparation

1. Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Xiuyu Ye: Security of Shamir's Secret-sharing against Physical Bit Leakage: Secure Evaluation Places (pdf)

2. Aniket Kate, Hemanta K. Maji, Hai H. Nguyen, Albert Yu: Unconditional Security using (Random) Anonymous Bulletin Board (pdf)

3. Shivaram Gopal, S M Ferdous, Alex Pothen, Hemanta K. Maji: A Parallel Algorithm for Maximizing Submodular Functions (pdf)

4. Hamidreza Amini Khorasgani, Hemanta K. Maji, Mingyuan Wang: Coin-tossing with Lazy Defense (pdf)

Awards

2021–2022	Ross–Lynn Research Scholar Grant
2019	Excellence in Research at Purdue Award
2017–2018	Purdue Research Foundation Award
2016	CISE Research Initiation Initiative (CRII) Award
2011, 2012	Computing Innovation Fellow sponsored by Computing Research Association
Spring 2008	Outstanding Teaching Assistant award, University of Illinois, Urbana-Champaign
2005–2006	Andrew & Shana Laursen Fellowship by University of Illinois, Urbana-Champaign
2004	Best B.Tech. Project Award for "Solving Traveling Salesman Problem in Classical and Quantum paradigm"
2001–2004	Aditya Birla Scholar, awarded to 9 undergraduates each year from all IITs for academic excellence
2000–2001	Academic Excellence Award, Indian Institute of Technology, Kanpur
2000	Ranked 35 in Joint Entrance Examination for IIT
1998	2nd rank in Indian National Mathematical Olympiad

Student Mentoring and Teaching Experience

Ph.D. Students	Mingyuan Wang (2017 – 2021) [Postdoctoral researcher, University of California, Berkeley] Hai H. Nguyen (2016 – 2022) [Postdoctoral researcher, ETH-Zurich] Hamidreza Amini Khorasgani (2017 – present) Xiuyu Ye (2021 – present) Albert Yu (2019 — present, joint with Aniket Kate) Ji Hun Hwang (2023 – present) (Mentored) Tamalika Mukherjee (2016 – 2020) (Mentored) Alexander R. Block (2016 – 2019)
Undergraduate & Masters students	Raphael Arkady Meyer (2016 – 2018) [Finalist, CRA Outstanding Undergraduate Researcher Awards 2018] Daniel Yu-Long Xie, (2022 – present) Donald Q. Adams (2020 – 2022) Minh L. Nguyen (2020 – 2022) Albert Yu (2018 – 2019) [joined Ph.D.] Xiuyu Ye (2018 – 2020) [joined Ph.D.] Himanshi Mehta (2018 – 2021) Amisha Jhanji (2016 – 2018) Noah T. Curran (2018) Pongthip Srivarangkul (2018) Adhishree Abhyankar (2017) Marshia Seto (2016) Hanchen Li (2015 – 2016) [Honors Thesis]

Invited Talks and Guest Lectures

1. Geometry of Secure Computation
   - Minimal Complexity Assumption for Cryptography, Simons Workshop, May 2023
   - IIT Bombay and Trust Lab Colloquium, April 2023
   - Midwest Crypto Day, April 2023
2. Local Leakage-resilience of Shamir's Secret-sharing Scheme
   - Crypto Reading Club meeting, NIST, January 2023
3. Secure Non-interactive Simulation
   - Communication, Control and Signal Processing (CCSP) Seminar Series UMD, September 2022
   - Science of Information Seminar
   - Boston University, Spring 2022

- ETH Zurich, Spring 2022
- University of Maryland, Spring 2022
- New York University, May 2022

4. Computational Hardness of Optimal Fair Computation
   - MIT, September 2021
   - GTACS, IDC, May 2021
   - University of Warsaw, Spring 2021
   - Carnegie Melon University Theory Lunch Talk, 2021
   - University of California, Berkeley, Fall 2020
   - Virtual Boston University Security seminar, Fall 2020
   - Michigan-Purdue Theory Seminar, Fall 2020
5. P_4-free Partition and Cover Numbers
   - Science of Information Seminar Series (CSoI), Fall 2020
6. Estimating Large Gaps in Martingales and Applications
   - Invited talk at Statistics Research Colloquium, Purdue–2019
7. Capacity Inversion and its Applications to Secure Computation
   - Invited talk at Allerton–2015
   - Invited talk at Securing Computation Workshop–2015 at Simons Institute,Berkeley, 2015
   - Invited Talk at The Security Seminar at CERIAS, 2016
8. Resilient Building Blocks for Secure Computation
   - Talk at Department of Computer Science, Purdue University, 2015
   - Talk at Department of Computer Science, North Carolina State University, 2015
   - Talk at College of Computing & Informatics, Drexel University, 2015
9. Secure Computation over Leaky Channels
   - Department Colloquium Talk at Department of Computer Science, North Carolina State University, 2014
   - Department Colloquium Talk at Department of Computer Science & Engineering, University of Nebraska–Lincoln, 2014
   - Invited Talk at Allerton–2014
   - Invited Talk at CERIAS Student Association, 2016

10. A Full Characterization of Completeness for Two-party Randomized Function Evaluation
    - Invited talk at New York Theory Day–2014
11. Limits of Random Oracles in Secure Computation
    - Invited talk at Microsoft Research Lab., India, 2012
    - Invited talk at Indian Statistical Institute, Kolkata, 2012
    - Guest Lecture in Advanced Security Course CS–463 in 2011
12. On the Computational Complexity of Coin Flipping
    - Invited talk at Indian Statistical Institute, Kolkata, 2011
    - Invited talk at China Theory Week, 2010
    - Invited talk at Microsoft Research Lab., India, 2010
13. Optimal Generation and Amplification of Trust
    - Grad Expo–2010 at University of Illinois, Urbana-Champaign
14. Complexity of Multi-party Computation Problems: The Case of 2-Party Symmetric Secure Function Evaluation
    - Invited talk at Midwest Theory Day, 2008

Scientific and Academic Service

Guest Editor	Entropy, Special Issue "Recent Advances in Information-theoretic Cryptography," 2021
Topical Advisory Panel Member	Entropy
PC Member	TCC – 2024, ITC – 2024, ASIACRYPT–2023, EUROCRYPT–2023, CRYPTO–2022, EUROCRYPT–2022, ASIACRYPT–2022, Information-theoretic Cryptography–2022, Information-theoretic Cryptography–2020, ASIACRYPT–2019, INDOCRYPT–2018, ICITS–2017, TCC–2016–B, ICITS–2016, PKC–2016, ASIACRYPT–2015, INDOCRYPT–2015, TCC–2013
External Reviewer	IEEE Transactions on Information Theory, Journal of Cryptology, SIAM Journal of Computing, Theoretical Computer Science, FOCS, STOC, CRYPTO, EUROCRYPT, TCC, ASIACRYPT, ICALP, PKC, ICITS, Information-theoretic Cryptography