Arpita **Patra**

Associate Professor · Cryptographer

Department of Computer Science & Automation, Indian Institute of Science, Bangalore 560012, INDIA

(+80) 2293-3566 | arpita@iisc.ac.in, arpitapatra10@gmail.com | https://www.csa.iisc.ac.in/ arpita/ | http://www.csa.iisc.ac.in/ cris/

"Be the change that you want to see in the world."

Position

Indian Institute of Science, Bangalore — *Bangalore, India*

Associate Professor (fast-track promotion), Department of Computer Science and Automation — *May 12, 2020–till date*

Indian Institute of Science, Bangalore — *Bangalore, India*

Assistant Professor, Department of Computer Science and Automation — *May 30, 2014–May 11, 2020*

Education

Indian Institute of Technology (IIT) Madras — *Chennai, India*

Ph.D. in Computer Science and Engineering — *August 2006–May 2010*

- Dissertation Area: Cryptography
- Dissertation Title: Studies on Verifiable Secret Sharing, Byzantine Agreement and Multiparty Computation

Indian Institute of Technology (IIT) Madras — *Chennai, India*

Master of Science (by research) in Computer Science and Engineering — *August 2004–July 2006*

- Dissertation Area: Image Processing
- Dissertation Title: Efficient Methods for Face Recognition and Multimodal Biometry

Haldia Institute of Technology — *West Bengal, India*

Bachelor of Technology in Computer Science and Engineering — *August 2000–July 2004*

- Dissertation Area: Formal methods of verification
- Dissertation Title: Development of Timing Analysis Tool for Asynchronous Systems

Experience

University of Bristol — *Bristol, UK*

Post-doctoral Researcher (Hosted by Prof. Nigel P. Smart) — *September 2012–December 2013*

ETH Zurich — *Zurich, Switzerland*

Post-doctoral Researcher (Hosted by Prof. Ueli Maurer) — *September 2011–August 2012*

Aarhus University — *Aarhus, Denmark*

Post-doctoral Researcher (Hosted by Prof. Ivan Damgård) — *September 2010–August 2011*

Research Interest

My specialisation is in cryptography, a key enabling technology for cybersecurity. In cryptography, my primary focus is on secure multi-party computation (MPC), the standard bearer and holy-grail problem, that permits a collection of data-owners to compute a collaborative result, without any of them gaining any knowledge about the data provided by the other, except what is derivable from the final result of the computation. MPC finds application in any scenario that involve computations on sensitive data from two or more entities. Till date, it has shown demonstrable success in several real-life scenarios, with significant payoff to society. For instance, it has been used– (a) to securely analyze the sensitive salary data of more than 10 millions of employees in the Greater Boston Area in order to calculate pay disparity across gender and race; (b) to train a model on private medical data held by several sources to offer best treatment for diseases like HIV, skin cancer, retinopathy; (c) to compute the probability of two satellites colliding in the space for satellites owned by competing countries; (d) to implement secure auction to find a fair price for sugar-beet in Denmark; (e) to implement online sexual assault reporting platform (allegation escrow) that will detect repeat perpetrators and create pathways to support for victims. Other compelling uses of MPC include disease surveillance, electricity trading markets, scientific discovery, smart-cities, genomics, homeland

and cyber security, global advanced persistent threat identification in corporate network data, tax fraud detection and the numerous applications in medicine, finance sector, self-driven automobiles that fall under secure machine learning and prediction.

My secondary interest lies in the area of fault-tolerant distributed computing that includes classic problems such as Byzantine Agreement aka BA (and its close relative broadcast). BA that allows a set of distrusting parties to jointly reach agreement on their private inputs even in the face of a coalition of cheating parties. BA has been used to build *robust* systems since long. Its solutions have been lending their power in systems ranging from flight control, to databases, to peer-to-peer; Microsoft uses BA in Farsite; many structured peer-to-peer systems use BA. Both broadcast and BA also serve as important building block of MPC. Lastly and importantly, BA has reappeared in a new avatar in the form of *Block-chain* technology.

The core focus of my research can thus be broadly classified into two areas as follows: (a) Theory and Practice of MPC; (b) Fault-tolerant Distributed Computing. The main goal and the publications under each category is given below.

Theory and Practice of MPC: The foundational questions for MPC and its building blocks such as circuit garbling, oblivious transfer (OT), commitment schemes, zero-knowledge protocols, verifiable secret sharing (VSS), public key encryptions (PKE), are concerned with the feasibility of realizing these tasks, finding inherent lower bounds on the resources needed for solving these tasks and finding resource-efficient constructions. The resource required by a cryptographic protocol is determined by its computation, round and communication complexity. My works in this regime have appeared (or will appear) in FOCS 2020, TCC 2020, ASIACRYPT 2020, ASIACRYPT 2019, IEEE Transactions on Information Theory 2018, CRYPTO 2018, IEEE Transactions on Information Theory 2017, Journal of Cryptology 2017, CRYPTO 2017, SCN 2016, Journal of Cryptology 2015, ASIACRYPT 2013, DISC 2013, SCN 2014, ASIACRYPT 2012, PODC 2012, ASIACRYPT 2011, AFRICACRYPT 2010, CRYPTO 2009.

Building practically-efficient constructs for MPC, their proof-of-concept implementations, performance analysis on specific tasks (such as training a ML model for breast cancer/retinopathy/skin cancer securely, performing secure prediction, e-voting) is the primary concern here. My works in this regime have appeared in USENIX Security 2021, NDSS 2020, PoPETs 2020, ACM CCS 2019, ACM CCSW 2019, PPML 2019, ACM CCS 2018, NDSS 2017 and are under submission in leading venues.

Fault-tolerant Distributed Computing: Apart from BA and broadcast, I also work on the problem of reliable message transfer (RMT) over untrusted network in this domain. My focus involves foundational feasibility, efficiency and optimality questions, in terms of resources such as round (running time), communication and computation, as in the MPC domain. My works in this regime have appeared (or will appear) in Journal of ACM 2020, Distributed Computing 2020, PODC 2018, DISC 2017, PODC 2016, Distributed Computing 2014, Journal of ACM 2012, Journal of Parallel and Distributed Computing 2011, OPODIS 2011, PODC 2010. ICDCN 2010, PODC 2009, PODC 2008, DISC 2007.

Scientific Publications

Thesis

1. **Arpita Patra**. Studies on Verifiable Secret Sharing, Byzantine Agreement and Multiparty Computation. *PhD Thesis, 2010*. Under supervision of Prof. C. Pandu Rangan.
2. **Arpita Patra**. Efficient Methods for Face Recognition and Multimodal Biometry. *Master Thesis, 2006*. Under supervision of Prof. Sukhendu Das.

Edited Volumes

1. Keren Censor-Hillel and **Arpita Patra**. *Proceedings of the 21st International Conference on Distributed Computing and Networking, ICDCN 2020, Kolkata, India, January 4th-7th, 2020.* ACM 2020.
2. **Arpita Patra** and Nigel P. Smart. *Progress in Cryptology - INDOCRYPT 2017 - 18th International Conference on Cryptology in India, Chennai, India, December 10-13, 2017, Proceedings.* Lecture Notes in Computer Science 10698, Springer 2017. DOI: 10.1007/978-3-319-71667-1

Journals

1. **Arpita Patra** and Divya Ravi. On the Exact Round Complexity of Three-party Computation. *Accepted to Journal of Cryptology*.
2. Chaya Ganesh and **Arpita Patra**. Broadcast Extensions with Optimal Communication and Round Complexity. *Distributed Computing, vol. 34, no. 1, pp. 59–77, 2021.*
3. Laasya Bangalore, Ashish Choudhury, **Arpita Patra**. The Power of Shunning: Efficient Asynchronous Byzantine Agreement Revisited. *Journal of ACM, vol. 67, no. 3, pp. 14:1–14:59, 2020.*
4. Megha Byali, Harsh Chaudhari, **Arpita Patra**, Ajith Suresh. FLASH : Fast and Robust Framework for Privacy-preserving Machine Learning. 20^{th} *Privacy Enhancing Technologies Symposium (PETS/PoPETS), volume 2020, no 2, pp. 459–480, 2020*.
5. **Arpita Patra**, Divya Ravi. On the power of Hybrid Networks in Secure Multi-party Computation. *IEEE Transactions on Information Theory, vol. 64, no. 6, pp. 4207-4227, 2018*.
6. Carmit Hazay, **Arpita Patra**. Efficient One-Sided Adaptively Secure Computation. *Journal of Cryptology, vol. 30, no. 1, pp. 321–371, 2017*.
7. Ashish Choudhury, **Arpita Patra**. An Efficient Framework for Unconditionally Secure Multiparty Computation. *IEEE Transactions on Information Theory, vol. 63, no. 1, pp. 428–468, 2017*.
8. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Efficient Asynchronous Verifiable Secret Sharing and Multiparty Computation. *Journal of Cryptology, vol. 28, no. 1, pp. 49–109, 2015*.

9. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Efficient Asynchronous Byzantine Agreement with Optimal Resilience. *Distributed Computing Journal, vol. 27, no. 2, pp. 111- 146, 2014*.
10. Ashwinkumar B. V, **Arpita Patra**, Ashish Choudhury, Kannan Srinathan and C. Pandu Rangan. On the Tradeoff Between Network Connectivity, Round Complexity and Communication Complexity of Reliable Message Transmission. *Journal of ACM, vol. 59, no. 5, pp. 22, 2012*.
11. Ashish Choudhury, **Arpita Patra**, Ashwinkumar B. V, Kannan Srinathan and C. Pandu Rangan. Secure Message Transmission in Asynchronous Networks. *Journal of Parallel and Distributed Computing, vol. 71, no. 8, pp. 1067-1074, 2011*.
12. **Arpita Patra**, Ashish Choudhury, C. Pandu Rangan and K. Srinathan. Unconditionally Reliable and Secure Message Transmission in Undirected Synchronous Networks: Possibility, Feasibility and Optimality. *International Journal of Applied Cryptography (IJACT), vol 2, Issue 2, pp. 159-197, 2010*.
13. **Arpita Patra**, Ashish Choudhury, C. Pandu Rangan and K. Srinathan. Perfectly Reliable and Secure Message Transmission Tolerating Mobile Adversary. *International Journal of Applied Cryptography (IJACT), vol. 1, Issue 3, pp. 200-224, 2009*.
14. **Arpita Patra** and Sukhendu Das. Enhancing Decision Combination of Face and Fingerprint by Exploitation of Individual Classifier Space: An approach to Multimodal Biometry. *Pattern Recognition (PR), vol. 41, Issue 7, pp. 2298-2308, 2008*.
15. Lalit Gupta, Vinod Pathangay, **Arpita Patra**, A. Dyana and Sukhendu Das. Indoor versus Outdoor Scene Classification using Probabilistic Neural Network. *EURASIP Journal on Advances in Signal Processing, vol. 2007 (2007), Article ID94298, 10 pages*.

Conferences

1. **Arpita Patra** and Akshayaram Srinivasan. Three-Round Secure Multiparty Computation from Black-Box Two-Round Oblivious Transfer. 41^{th} *Annual International Cryptology Conference (CRYPTO 2021)*
2. Nishat Koti, **Arpita Patra**, Ajith Suresh. MPCLeague: Robust and Efficient Mixed-protocol Framework for 4-party Computation. *Poster session of 42nd IEEE Symposium on Security and Privacy (IEEE S&P 2021)* and *ICLR Workshop on Distributed and Private Machine Learning 2021*.
3. Nishat Koti, Mahak Pancholi, **Arpita Patra**, Ajith Suresh. SWIFT: Super-fast and Robust Privacy Preserving Machine Learning. 30^{th} *USENIX Security Symposium (USENIX-Security) 2021.* Brief Announcement in NeurIPS PRIML and PPML Workshop 2020.
4. **Arpita Patra**, Thomas Schneider, Ajith Suresh, Hossein Yalame. ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation. 30^{th} *USENIX Security Symposium (USENIX-Security) 2021.*
5. Benny Applebaum, Eliran Kachlon and **Arpita Patra**. The Round Complexity of Perfect MPC with Active Security and Optimal Resiliency. 61^{th} *Annual IEEE Symposium on Foundations of Computer Science (FOCS), IEEE, pp. 1277-1284, 2020.*
6. Benny Applebaum, Eliran Kachlon and **Arpita Patra**. The Resiliency of MPC with Low Interaction: The Benefit of Making Errors. *The* 18^{th} *Theory of Cryptography Conference (TCC), LNCS 12551, pp. 562–594 2020.*
7. **Arpita Patra**, Divya Ravi and Swati Singla. On the Exact Round Complexity of Best-of-both-Worlds Multi-party Computation. 26^{th} *Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), LNCS 12493, pp. 60–91 2020.*
8. **Arpita Patra** and Ajith Suresh. BLAZE: Blazing fast Privacy-Preserving Machine Learning. 27^{th} *Network and Distributed System Security Symposium (NDSS), The Internet Society, 2020.*
9. **Arpita Patra** and Divya Ravi. Beyond Honest Majority: The round complexity of Fair and Robust Multi-party Computation. 25^{th} *Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), LNCS 11921, pp. 456–487, 2019.*
10. Harsh Chaudhari, Ashish Choudhury, **Arpita Patra** and Ajith Suresh. ASTRA: High Throughput 3PC over Rings with Application to Secure Prediction. *The ACM Cloud Computing Security Workshop (ACM CCSW), ACM Press, pp. 81–92, 2019* (full version) and *Privacy Preserving Machine Learning (PPML) 2019*.
11. Megha Byali, Carmit Hazay, **Arpita Patra** and Swati Singla. Fast Actively Secure Five-Party Computation with Security Beyond Abort. *26th ACM Conference on Computer and Communications Security (CCS 2019), ACM Press, pp. 1573–1590, 2019*.
12. **Arpita Patra** and Divya Ravi. On the Exact Round Complexity of Three-party Computation. 38^{th} *Annual International Cryptology Conference (CRYPTO 2018), LNCS 10992, pp. 425–458, 2018*.
13. Laasya Bangalore, Ashish Choudhury, **Arpita Patra**. Almost-Surely Terminating Asynchronous Byzantine Agreement Revisited. 37^{th} *Annual ACM Symposium on Principles of Distributed Computing (PODC 2018), ACM Press, pp. 295–304, 2018*.
14. Megha Byali, Arun Joseph, **Arpita Patra** and Divya Ravi. Fast Secure Computation for Small Population over the Internet. 25^{th} *ACM Conference on Computer and Communications Security (CCS 2018), ACM Press, pp. 677–694, 2018*.
15. Chaya Ganesh, Yashvanth Kondi, **Arpita Patra**, Pratik Sarkar. Efficient Adaptively Secure Zero-Knowledge from Garbled Circuits. *21st International Conference on Practice and Theory of Public-Key Cryptography (PKC 2018), LNCS 10770, pp. 499-529, 2018*.
16. Ashish Choudhury, Gayathri Garimella, **Arpita Patra**, Divya Ravi and Pratik Sarkar. Brief Announcement: Crash-tolerant Consensus in Directed Graph Revisited. Full version in *25th International Colloquium on Structural Information and Communication Complexity (SIROCCO), 2018*; brief announcement in *31st International Symposium on Distributed Computing (DISC 2017), LIPIcs 91, pp. 46:1–46:4, 2017*.
17. Yashvanth Kondi and **Arpita Patra**. Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic. 37^{th} *Annual International Cryptology Conference (CRYPTO 2017), LNCS 10401, pp. 188–222, 2017*.
18. **Arpita Patra**, Pratik Sarkar and Ajith S. Fast Actively Secure OT Extension for Short Secrets. 24^{th} *Annual Network and Distributed System Security Symposium (NDSS 2017), Internet Society, 2017*.
19. Ashish Choudhury and **Arpita Patra** and Divya Ravi. Round and Communication Efficient Unconditionally-Secure MPC with t < n / 3 in Partially Synchronous Network. *10th International Conference on Information Theoretic Security (ICITS 2017), LNCS 10681, pp. 83–109,2017*.
20. Chaya Ganesh and **Arpita Patra**. Broadcast Extensions with Optimal Communication and Round Complexity. 35^{th} *Annual ACM Symposium on Principles of Distributed Computing (PODC 2016), pp. 371–380, ACM Press, 2016*
21. Ashish Choudhury, Emmanuela Orsini, **Arpita Patra**, Nigel Smart. Linear Overhead Robust MPC with Honest Majority Using Prepro-

cessing. 11^{th} *Conference on Security and Cryptography in Networks (SCN 2016), LNCS 9841, pp 147–168, Springer, 2016*

22. Carmit Hazay and **Arpita Patra** and Bogdan Warinschi. Selective Opening Security Revisited. 21^{st} *Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2015), LNCS 9452, pp. 443–469, 2015.*
23. Carmit Hazay, Yehuda Lindell and **Arpita Patra**. Adaptively Secure Computation with Partial Erasures. 34^{th} *Annual ACM Symposium on Principles of Distributed Computing (PODC 2015), pp. 291–300, ACM Press, 2015*
24. Ashish Choudhury and **Arpita Patra**. Optimally Resilient Asynchronous MPC with Linear Communication Complexity. 16^{th} *International Conference on Distributed Computing and Networking (ICDCN 2015), ACM, 2015.*
25. Carmit Hazay and **Arpita Patra**. One-Sided Adaptively Secure Two-Party Computation. 11^{th} *Theory of Cryptography Conference (TCC 2014), LNCS 8349, pp. 368-393, 2014*
26. Joel Alwen, Martin Hirt, Ueli Maurer, **Arpita Patra** and Pavel Raykov. Key-Indistinguishable Message Authentication Codes. 9^{th} *Conference on Security and Cryptography in Networks (SCN 2014), LNCS 8642, pp 476–493, Springer, 2014*
27. Ashish Choudhury, **Arpita Patra** and Nigel P. Smart. Reducing the Overhead of MPC over a Large Population. 9^{th} *Conference on Security and Cryptography in Networks (SCN 2014), LNCS 8642, pp 197–217, Springer, 2014*
28. Ashish Choudhury, Jake Loftus, Emmanuela Orsini **Arpita Patra** and Nigel P. Smart. Between a Rock and a Hard Place: Interpolating Between MPC and FHE. 19^{th} *Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2013), LNCS 8270, pp. 221-240, 2013*
29. Ashish Choudhury and Martin Hirt and **Arpita Patra**. Unconditionally Secure Asynchronous Multiparty Computation with Linear Communication Complexity. 27^{th} *International Symposium on Distributed Computing (DISC 2013), LNCS 8205, pp. 406–421, 2013*.
30. Ashish Choudhury and **Arpita Patra**. Brief Announcement: Efficient Optimally Resilient Statistical AVSS and Its Applications. 31^{st} *Annual ACM Symposium on Principles of Distributed Computing (PODC 2012), pp. 103-104, ACM Press, 2012*.
31. Michael Backes, Aniket Kate and **Arpita Patra**. Computational Verifiable Secret Sharing Revisited. 17^{th} *Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2011), LNCS 7073, pp. 590-609, 2011*
32. **Arpita Patra**. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity. 15^{th} *International Conference on Principles of Distributed Systems (OPODIS 2011), LNCS 7109, pp. 34-49, 2011*.
33. Ashish Choudhury, Kaoru Kurosawa, **Arpita Patra**. Simple and Efficient Single Round Almost Perfectly Secure Message Transmission Tolerating Generalized Adversary. 9^{th} *International Conference on Applied Cryptography and Network Security (ACNS 2011), LNCS 6715, pp. 292-308, 2011*.
34. Ashish Choudhury, Kaoru Kurosawa, **Arpita Patra**. The Round Complexity of General VSS. 5^{th} *International Conference on Information Theoretic Security (ICITS 2011), LNCS 6673, pp. 143–162, 2011*.
35. **Arpita Patra** and C. Pandu Rangan. Communication Optimal Multi-Valued Asynchronous Byzantine Agreement with Optimal Resilience. 5^{th} *International Conference on Information Theoretic Security (ICITS 2011), LNCS 6673, pp. 206–226, 2011*.
36. Ranjit Kumaresan, **Arpita Patra** and C. Pandu Rangan. The Round Complexity of Verifiable Secret Sharing: The Statistical Case. 16^{th} *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2010), LNCS 6477, pp. 431-447, 2010.*
37. **Arpita Patra** and C. Pandu Rangan. Brief Announcement: Communication Efficient Asynchronous Byzantine Agreement. 29^{th} *Annual ACM Symposium on Principles of Distributed Computing (PODC 2010), pp 243-244, ACM Press, 2010*.
38. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. On The Communication Complexity of Perfectly Secure Message Transmission in Directed Networks. 11^{th} *International Conference on Distributed Computing and Networking (ICDCN 2010), LNCS 5935, pp. 42–53, 2010*.
39. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Communication Efficient Perfectly Secure VSS and MPC in Asynchronous Networks with Optimal Resilience. 3^{rd} *International Conference on Cryptology in Africa (AFRICACRYPT 2010), LNCS 6055, pp. 184–202, 2010*.
40. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Simple and Efficient Asynchronous Byzantine Agreement with Optimal Resilience. 28^{th} *Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2009), pp. 92–101, ACM Press, 2009*
41. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. The Round Complexity of Verifiable Secret Sharing Revisited. 29^{th} *Annual International Cryptology Conference (CRYPTO 2009), LNCS 5677, pp. 487–504, 2009*.
42. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Information Theoretically Secure Multi Party Set Intersection Re-Visited. 16^{th} *Annual International Workshop on Selected Areas in Cryptography (SAC 2009), LNCS 5867, pp. 71–91, 2009.*
43. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Perfectly Secure Message Transmission in Directed Networks Revisited. 28^{th} *Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2009), pp. 278–279, ACM Press, 2009.*
44. Ashwinkumar B.V, **Arpita Patra**, Ashish Choudhury, Kannan Srinathan and C. Pandu Rangan. On Minimal Connectivity Requirement for Secure Message Transmission in Asynchronous Networks. 10^{th} *International on Conference Distributed Computing and Networking (ICDCN 2009), LNCS 5408, pp. 148–162, 2009.*
45. **Arpita Patra**, Ashish Choudhury, and C. Pandu Rangan. Efficient Statistical Asynchronous Verifiable Secret Sharing with Optimal Resilience. 4^{th} *International Conference on Information Theoretic Security (ICITS 2009), LNCS 5973, pp. 74-92, 2009*.
46. Kannan Srinathan, Ashish Choudhury, **Arpita Patra** and C. Pandu Rangan. (Im)Possibility of Unconditionally Secure Message Transmission in Arbitrary Directed Synchronous Networks Tolerating Generalized Adversary. *ACM Symposium on Information, Computer and Communications Security (ASIACCS 2009), pages 171–182, ACM Press, 2009*.
47. Ashwinkumar B.V, **Arpita Patra**, Ashish Choudhury, Kannan Srinathan and C. Pandu Rangan. On Tradeoff Between Network Connectivity, Phase Complexity and Communication Complexity of Reliable Communication Tolerating Mixed Adversary. 27^{th} *Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2008), pp. 115–124, ACM Press, 2008.*
48. **Arpita Patra**, Ashish Choudhury, Kannan Srinathan and C. Pandu Rangan. Brief Announcement: Efficient Single Phase Unconditionally Secure Message Transmission with Optimum Communication Complexity. *PODC 2008,* pp. 457, ACM Press, 2008.
49. **Arpita Patra**, Ashish Choudhury, Madhu Gayatri and C. Pandu Rangan. Efficient Perfectly Reliable and Secure Communication Tol-

erating Mobile Adversary. 13^{th} *Australasian Conference on Information Security and Privacy (ACISP 2008), LNCS 5107, pp. 170–186, 2008.*

50. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Unconditionally Reliable and Secure Message Transmission in Directed Networks Revisited. 6^{th} *International Conference Security and Cryptography for Networks (SCN 2008), LNCS 5229, pp. 309–326, 2008.*
51. Ashish Choudhury, **Arpita Patra**, AshwinKumar B.V, Kannan Srinathan and C. Pandu Rangan. Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary. 3^{rd} *International Conference on Information Theoretic Security (ICITS 2008), LNCS 5155, pp. 137–155, 2008.*
52. **Arpita Patra**, Ashish Choudhury and C. Pandu Rangan. Constant Phase Efficient Protocols for Perfectly Secure Message Transmission in Directed Networks. 26^{th} *Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2007), pp. 322-323, ACM Press, 2007.*
53. **Arpita Patra**, Ashish Choudhury, Kannan Srinathan and C. Pandu Rangan. Perfectly Secure Message Transmission in Directed Networks Tolerating Mixed Adversary. 21^{st} *International Symposium on Distributed Computing (DISC 2007), LNCS 4731, pp. 496–498, 2007.*

Preprints & Manuscripts (J: journal, C: conference, M: Manuscript)

1. (C) Benny Applebaum, Eliran Kachlon, **Arpita Patra**. Round-optimal Honest-majority MPC in Minicrypt and with Everlasting Security. *Under submission*
2. (C) Aditya Hegde, Shravani Patil, **Arpita Patra** and Protik Paul. QuadSquad: Efficient Secure Computation with Friends and Foes. *Under submission*
3. (C) **Arpita Patra**, Thomas Schneider, Ajith Suresh and Hossein Yalame. SynCirc: Efficient Synthesis of Depth-Optimized Circuits for Secure Computation. *Under submission*
4. (C) Pankaj Dayama, Arpita Patra, Protik Paul, Nitin Singh, Dhinakaran Vinayagamurthy. How to prove a statement jointly? Distributed-prover Zero-Knowledge Protocols. *Under Submission*
5. (J) Anirudh C, Ashish Choudhury, **Arpita Patra**. A survey on Perfectly-Secure Verifiable Secret-Sharing. *Under submission*
6. (J) Ashish, Choudhury, **Arpita Patra**. On the Communication Efficiency of Statistically-Secure Asynchronous MPC. *Communicated to Journal of ACM*
7. (J) **Arpita Patra** and Divya Ravi. Beyond Honest Majority: The round complexity of Fair and Robust Multi-party Computation. *Communicated to Journal of Cryptology and Revised with positive review*.

Projects & Grants

Theory and Practice of Secure Computation — *IISc Alumni Endowment*

Arpita Patra — *2021– 2024*

- Amount: ₹4,00,000.

Token-aided Secure Multi-party Computation — *DST, India*

Arpita Patra — *2021– 2026*

- This is a part of bigger initiative of 'Technology Innovation Hub (TIH)' under the National Mission on 'Cyber Security and Cyber Security for Physical Infrastructure', set up at IIT Kanpur with IISc, IIT Kharagpur, IIIT Allahabad and AKTU Lucknow as initial national academic partners, and University of California, San Diego, New York University, New York and Abu-Dhabi Campus, Tel Aviv University and Ben Gurion University in Israel as initial international academic partners. At IISc, I share this grant with Vinod Ganapathi.)
- Amount: ₹5.20 Crores

Privacy-preserving Machine Learning for Social Good [FA/GOGL-20-0001] — *Google*

Arpita Patra — *28 July 2020– 27th July 2023*

- Google India AI/ML Research Award 2020
- Amount: $ 20,000. In addition, $ 12,000 Cloud Platform (GCP) credits

Cryptography with Minimal Communication [SA/DSTO-19-0218] — *SERB, India*

Arpita Patra — *19th March 2020–18 March 2023*

- SERB MATRICS (Mathematical Research Impact Centric Support) 2020
- Amount: ₹ 6,60,000

Secure Multi-party Computation: Feasibility and Efficiency [SP/DSTO-16-1706] — *SERB, India*

Arpita Patra — *22nd March 2017 –21st March 2020*

- Women Excellence Award 2017
- Amount: ₹ 18,00,00

Efficient Secure Multi-party Computation [SA/DSTO-15-1467] — *DST, India*

Arpita Patra — *26th October 2015– 25th October 2020*

- Inspire Faculty Award 2015
- Amount: ₹ 35,00,00

Zero-knowledge Protocols and Applications of MPC — *IBM IRL*

Arpita Patra — *2019*

- *Open Short-term Collaborative Programme (OSCP)* 2019
- Student and PI can collaborate with IBM IRL researchers. Student can travel to present research work in a conference where the joint work gets published.

Multi-party Computation — *Engineering and Physical Sciences Research Council (EPSRC), UK*

PI: Nigel P. Smart, co-PI: Arpita Patra, Ashish Choudhury — *July 2015– July 2017*

- Amount: 70,471 GBP

Secure Multiparty Computation- startup grant — *IISc*

Arpita Patra — *July 2014– July 2016*

- Startup Grant by IISc
- Amount: ₹25,00,000

Honors & Awards

2021	Featured in 'Women's Day Special: Meet India's leading AI researchers' by INDIAai, a MEITY, NEGD & NASSCOM Initiative, 2021.
2020	Fast-track promotion to Associate Professor at IISc, 2020.
2020	Google India AI/ML Research Award 2020.
2018	The National Academy of Sciences, India (NASI)-Young Scientist Platinum Jubilee Award 2018.
2018	Google Travel grant for attending CRYPTO 2018.
2017	Council Member of Indian Association for Research in Computing Science (IARCS) (2017-2021).
2017	TWAS (The World Academy of Sciences) Young Afiliateship (2017-2021).
2017	The Indian National Academy of Engineering (INAE) Young Engineer Award 2017.
2017	The Indian National Academy of Engineering (INAE) Young Associateship (2017-2028).
2017	The Science and Engineering Research Board (SERB) Women Excellence Award 2017.
2015	The Indian Academy of Sciences (IAS) Associateship (2015-2018).
2015	Department of Science & Technology (DST) INSPIRE Faculty Fellowship (2015-2020).
2008	Google India Women in Engineering Award 2008.
2008	Microsoft Research PHD Fellowship (2006-2010).

Public or Media Coverage

The Round Complexity of Perfect MPC with Active Security and Optimal Resiliency — *IISc Court/Annual Report*

Research Highlights — *2020-2021*

Beyond Honest Majority: The round complexity of Fair and Robust Multiparty Computation & BLAZE: Blazing Fast Privacy-Preserving Machine Learning — *IISc Court/Annual Report*

Research Highlights — *2019-2020*

Cryptography's in big demand, but you must know math — *Times of India*

Hear the PROF — *18th Nov 2020*

Data Privacy in Collaborative Projects — *Kernel, IISc Press (IISc's annual magazine)*

Research Highlights — *2019*

What is Cryptography and Why do we Need it? — *CONNECT, IISc Press (IISc's quarterly magazine)*

Research at IISc — *March 2019*

Women in Science — *IISc Website*

Women Scientists in IISc– Dr. Arpita Patra — *2019*

Almost-Surely Terminating Asynchronous Byzantine Agreement Revisited — *IISc Court/Annual Report*

Research Highlights — *2018-2019*

Consensus Protocols for Realistic Distributed Systems — *IISc Website*

Featured Research — *June 2018*

Academic Visits

Bar Ilan University — *Tel Aviv, Israel*

Hosted by Cyber Security Center (Prof. Benny Pinkas and Prof. Carmit Hazay) — *1st June 2019 - 22nd June 2019*

Technion – Israel Institute of Technology — *Haifa, Israel*

Hosted by Prof. Yuval Ishai — *27 April 2019– 31st May 2019*

Schloss Dagstuhl — *Dagstuhl, Germany*

Seminar on 'Practical Yet Composably Secure Cryptographic Protocols', organized by Profs. Jan Camenisch, Ralf Küsters, Anna Lysyanskaya, Alessandra Scafuro — *20 January 2019– 25 January 2019*

Technische Universität Darmstadt — *Darmstadt, Germany*

Hosted by Prof. Thomas Schneider — *17 January 2019– 19 January 2019*

Cornel Tech. — *New York, USA*

Hosted by Prof. Muthuramakrishnan Venkitasubramaniam — *24 August 2018– 1 September 2018*

UC Berkeley — *Berkeley, USA*

Hosted by Prof. Sanjam Garg — *12 August 2018– 16 August 2018*

Aarhus University — *Aarhus, Denmark*

Hosted by Prof. Ivan Damgård — *May 2018–July 2018*

Bristol University — *Bristol, UK*

Hosted by Prof. Nigel Smart — *May 2015–July 2015*

Indian Statistical Institute (ISI) Kolkata — *Kolkata, India*

Hosted by Prof. Bimal Roy — *January 2014–May 2014*

Bar-Ilan University — *Tel-Aviv, Israel*

Hosted by Prof. Yehuda Lindell — *January 2013–March 2013*

Talks & Presentations

1. The Resiliency of MPC with Low Interaction: The Benefit of Making Errors.
   (a) 19th November, 2020. *TCC 2020.*
2. Secure Multi-party Computation.
   (a) 25th November 2020. *Colloquium talk at the Computer Science Department, Ashoka University, Sonipat, Haryana, India*
   (b) 19th October 2020. Indian Dutch Cyber Security School (IDCSS) 2020
   (c) 6th May 2020. Online Webinar. *Samgacchadhwam Series, Conducted by Center of Excellence in Cyber Security, An initiative by Government of Karnataka.*
   (d) 2nd December, 2019. *CSE, IIT Ropar, India.*
   (e) 23rd December 2019. *Department of Mathematics, NISER Bhubaneswar.*
   (f) 7th September 2018. *Invited Talk at National Workshop on Cryptology 2018, CR Rao Advanced Institute of Mathematics, Statistics and Computer science, Hyderabad, India.*
3. Fast Actively-Secure 5-Party Computation with Security Beyond Abort.

(a) 13th November, 2019. ***ACM CCS 2019 at London, UK.***

4. The Round Complexity Landscape of Secure Computation.
   (a) 6th September, 2019. ***Talk at IIT Kharagpur.***
   (b) 20th June 2019. ***Invited talk at 'Theory and Practice of Secure Multi-party Computation (TPMPC) 2019' at Bar-Ilan University, Israel.***
   (c) (upcoming) 19th January 2020. ***Talk at 'Secure Multi-party Computation: Theory and Practice 2020 at Indian Institute of Science, India.***
5. How to Choose a Research Topic. 6-7th July 2019. ***Invited talk at ACM India Grad Cohort 2019 at IIT Delhi, India.***
6. Fast Secure Computation for Small Population over the Internet.
   (a) 10th January 2019. ***Invited talk at "Fairness and Privacy" joint workshop by IISc-UPen-MSR Workshop, Bangalore***
   (b) 17th January, 2019. ***Invited talk at CROSSING Research Seminar at Technische Universitat Darmstadt, Germany.***
7. Cryptography and Machine Learning: Past, Present and Future.
   (a) 26th June 2019. ***Invited talk at ACM India summer school on Algorithmic and Theoretical aspects of Machine learning, IIIT Bangalore.***
   (b) 12th October 2018. ***Invited talk at Faculty Colloquium, CSA IISc.***
   (c) 27th October 2018. ***Invited talk at International Society of Automation, Bangalore, India.***
   (d) 26th November 2018. ***Invited talk at LNM Institute of Information Technology, Jaipur, respectively.***
8. Privacy-Free Garbled Circuits for Formulas: Size Zero and Information-Theoretic. 6th July 2018. ***Talk at Crypto Summer Day, 2018***, Aarhus, Denmark.
9. On the Exact Round Complexity of Three-party Computation. 29th May 2018. ***Contributed talk at Theory and Practice of Multi-party Computation (TPMPC), 2018***, Aarhus, Denmark.
10. Multi-party Computation. 16th March 2018. ***Invited Speech at IEEE CONECCT 2018***, Bangalore, India.
11. Impossibility Results for Information-theoretic Multi-party Computation. 8th January 2018. ***Invited Speech at IISC-IACR School on Cryptology 2018***, Bangalore, India.
12. Information-theoretic Multi-party Computation with Honest Majority. 7th January 2018. ***Invited Speech at IISC-IACR School on Cryptology 2018***, Bangalore, India.
13. OT Extensions. May and June 2017. ISEA Workshop on Cryptography, IISc, India.
14. Garbled Circuit and Yao Two Party Computation. May and June 2017. ISEA Workshop on Cryptography, IISc, India.
15. Computing on Private Data aka Multi-Party Computation. May and June 2017. ISEA Workshop on Cryptography, IISc, India.
16. Fast Actively Secure OT Extension for Short Secrets. March and April 2017. ***Invited Talk at MPC School and Workshop***, IIT Bombay, India and *Theory and Practice of Multi-Party Computation Workshop*, Bristol, UK.
17. Garbled Circuit and Yao's Two-party Computation. March 2017. ***Invited Talk at MPC School and Workshop***, IIT Bombay, India.
18. Oblivious Transfer and Extensions. March 2017. *MPC School and Workshop*, IIT Bombay, India.
19. A Tribute to Diffie and Hellman: The Winners of Turing Award 2015. March 2016. *Dept. of Computer Science & Automation*, IISc, India.
20. Introduction to Cryptography. February 2015. *Workshop on Introduction to Cryptography*, IISc, India.
21. Perfect Security. February 2015. *Workshop on Introduction to Cryptography*, IISc, India.
22. PRF and CPA-Security of SKE. February 2015. *Workshop on Introduction to Cryptography*, IISc, India.
23. Introduction to Secure Computation. February 2015. *Workshop on Topics in Cryptography*, IISc, India.
24. Secret Sharing and Information-Theoretic Secure Computation. February 2015. *Workshop on Topics in Cryptography*, IISc, India.
25. Multiparty Computation. November 2015. *Annual Meeting of Indian Academy of Sciences*, IISER Pune, India.
26. Linear Overhead Multiparty Computation with Honest Majority.
   (a) September 2015. *National Workshop on Cryptology 2015*, KIT, Bhubaneswar, India.
   (b) August 2015. *IIIT Delhi*, India.
27. Verifiable Secret Sharing. December 2014. *Recent Advances in Cryptography Workshop*, IIT Delhi, India.
28. Between a Rock and a Hard Place: Interpolating Between MPC and FHE. December 2013. *ASIACRYPT 2013*, Bengaluru, India.
29. A simple and Efficient Framework for Secure Multiparty Computation.
   (a) 1st November 2013. *IISc Bangalore*, Bengaluru, India.
   (b) October 2014. *Indo-Russian Workshop on Discrete Mathematics, Algebra, Number Theory and their Applications*, Moscow State University, Russia.
30. Asynchronous Multiparty Computation with Linear Communication Complexity. October 2013. *DISC 2013*, Jerusalem, Israel.
31. Anonymous Authentication with Shared Secrets. January 2013. *Bar-Ilan University*, Ramat Gan, Israel.
32. December 2012. Anonymous Authentication with Shared Secrets. *ISI Kolkata*, Kolkata, India.
33. Computational Verifiable Secret Sharing Revisited. *ASIACRYPT 2011*, Seoul, South Korea.
34. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity.
   (a) August 2011. *ISI Kolkata*, Kolkata, India.
   (b) December 2011. *OPODIS 2011*, Toulouse, France.
35. Communication Optimal Multi-valued Asynchronous Byzantine Agreement with Optimal Resilience. May 2011. *ICITS 2011*, Amsterdam, The Netherlands.
36. Verifiable Secret Sharing. May 2010. *National Level Instructional Workshop on Cryptology 2010*, Imphal, Manipur, India.
37. On Communication Complexity of Secure Message Transmission in Directed Networks. January 2010. *ICDCN 2010*, Kolkata, India.
38. Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience. December 2009. *INDOCRYPT 2009*, New Delhi, India.
39. Efficient Statistical Asynchronous Verifiable Secret Sharing with Optimal Resilience. December 2009. *ICITS 2009*, Japan.
40. Secure Distributed Computation and Communication. September 2009. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.

41. Information Checking Protocols. September 2009. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
42. Reliable and Secure Message Transmission. September 2009. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
43. The Round Complexity of Verifiable Secret Sharing Revisited. August 2009. *CRYPTO 2009*, Santa Barbara, USA.
44. Simple and Efficient Asynchronous Byzantine Agreement with Optimal Resilience. August 2009. *PODC 2009*, Calgary, Canada.
45. Information Theoretically Secure Multi Party Set Intersection Re-Visited. August 2009. *SAC 2009*, Calgary, Canada.
46. Secret Sharing Protocols. June 2009. *CRSI-IMSc Joint Workshop on Teaching Cryptology 2009*, ISI, India.
47. Round Efficient Unconditionally Secure Multiparty Computation Protocol. December 2008. *INDOCRYPT 2008*, IITKgp, India.
48. On Tradeoff Between Network Connectivity, Phase Complexity and Communication Complexity of Reliable Communication Tolerating Mixed Adversary.
    (a) August 2008. *China Theory Week (CTW) 2008*, Tsinghua University, Beijing, China.
    (b) August 2008. *PODC 2008*, Toronto, Canada.
49. Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary. August 2008. *ICITS 2008*, Calgary, Canada.
50. Probabilistic Perfectly Reliable and Secure Message Transmission - Possibility, Feasibility and Optimality. December 2007. *INDOCRYPT 2007*, Chennai, India.
51. Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary. December 2007. *CANS 2007*, Singapore.
52. Constant Phase Bit Optimal Protocols for Perfectly Reliable Message Transmission. December 2006. *INDOCRYPT 2006*, Kolkata, India.

Professional Activities

Associate Editor

Sadhana (Computer and Data Sciences), Springer (2018-2021).

Programme Committee (PC) Chair

– ICDCN 2020 (21st International Conference on Distributed Computing and Networking) along with Prof. Keren Censor-Hillel, Technion, Israel.

– INDOCRYPT 2017 (18th International Conference on Cryptology in India) along with Prof. Nigel Smart, University of Bristol, UK.

Programme Committee (PC) Member

2021	ACM CCS'21, PODC'21, ASIACRYPT'21, ITC'21, CFAIL'21, ARCS'21 (ACM-India Inter-Research-Institute Student Seminar in Computer Science) (**Declined**– OPODIS'21, FSTTCS'21, CSCML'21, ACM CODASPY'21, ICDCN'21, ASIACCS'21, ICISS'21)
2020	ASIACRYPT'20, INDOCRYPT'20, ICDCN'20, (**Declined**– ICDCS'20, DISC'20, CSCML'20, PKC'20)
2019	ASIACRYPT'19 (**Declined**– PKC'19, ICDCS'19, FSTTCS'19, INDOCRYPT'19)
2018	ASIACRYPT'18, EUROCRYPT'18, PKC'18, ICISS'18
2017	ASIACRYPT'17, PKC'17, ICITS'17, INDOCRYPT'17
2016-12	INDOCRYPT'16,'15,'12

Major Organization of events

19-22 Jan, 2020	Workshop on Multi-party Computation Theory & Practice	*IISc, India*
30-31 Jan 2020	Security Track in ACM-MSR Annual Academic Research Summit	*BITS Pilani, Goa, India*

Reviewer

Journal of Cryptology 2020, CRYPTO'16, STOC 2016, CRYPTO'15, ISIT'15, PKC'15, ASIACRYPT'14, ACM CCS'13, ASIACRYPT'13, PKC'13, CRYPTO'12, TCC'12, CRYPTO'11, Journal of Cryptology, TCC'11, INDOCRYPT'10, ASIACRYPT'10, PKC'10, ICITS'09, ICALP'09, ACISP'08, ICITS'08, ASIACRYPT'08.

Other Chairships

2019	**Tutorial co-Chair for** ICDCN

Thesis/Synopsis/Proposal Reviewer

2019	**PhD Thesis of Sikhar Patranabis from** IIT Kharagpur
2020/2019	**PhD Thesis and Synopsis of Varsha Bhat from** IIT Ropar
2020	**Research proposal on the Personal Research Grant from** The Israel Science Foundation (ISF)

Session Chair

2013	**Asiacrypt** Bangalore
2020	**Asiacrypt** Virtual

Service to the Institute

1. Comprehensive Committee Member of:
   (a) 2020: Shesadri K. R., CDS, IISc
   (b) 2019: Kripa Shanker, CSA, IISc
   (c) 2017: Shuti Sekar, PhD, Maths and CSA, IISc
   (d) 2015: S B Balaji, ECE, IISc
2. Faculty Coordinator for:
   (a) Narendra Summer Internship 2019
   (b) Perspectives Seminar 2018
   (c) CSA Web Coordinator between August 2017 - February 2019
   (d) CSA Student Welfare Committee member starting from March 2018
   (e) DIGITs Active Directory Creation 2017
   (f) Divisional of Electrical Sciences (EECS) Student Symposium 2017 and 2018
   (g) CSA Open Day 2016
3. Interview Committee Member: Member of Interview committee for CSA research admission in June 2014, 2015, 2016 and 2017, 2020. Member of Interview committee for selecting UG students via KVPY for the year of 2014 and 2015.
4. Institute Representative for GATE and KVPY: Served as IR for GATE 2017, 2018, 2019 and KVPY 2017.
5. Public Talks:
   (a) How to Choose a research topic? ***Orientation Programme for Batch of 2019***, CSA IISc, India.
   (b) Cryptography and Machine Learning: Past, Present and Future, ***Invited talk at Faculty Colloquium***, CSA IISc, India.
   (c) A Tribute to Diffie and Hellman: The Winners of Turing Award 2015. ***Dept. of Computer Science & Automation, IISc, India. March 2016.***
   (d) The Joy of Cryptography. ***CSA Summer School 2017, IISc and Swagatham 2016, CSA, IISc.***
   (e) Computing on Private Data. ***IISc-IBM Day 2017, CSA, IISc.***
   (f) Young Faculty Speaker at EECS Symposium 2016.
   (g) Speaker at CSA Orientation Program 2014, 2015, 2016 and 2019.

Courses

1. QIP short-term course on "Foundations of Cryptography" offered from 30th August - 3rd September, through Centre for Continuing Education (QIP Programme - Sponsored by AICTE), Indian Institute of Science.
2. CSA E0 305: Blockchain and Its Applications. Credit: 3:1. January-April 2019.
3. CSA E0 221: Discrete Structures . Credit: 3:1. August-December 2014.
4. CSA E0 235: Cryptography . Credit: 3:1. January-April 2015, 2016, 2017, 2018, 2019.
5. CSA E0 312: Foundations of Secure Computation. Credit: 3:1. August-December 2015, 2017, 2018, 2019.

In all the above courses that are offered, I have received ratings *close to 5 on 5*. The average student strengths of the foundational courses on 'Discrete Structures' and 'Cryptography' are approximately *35*. The course on cryptography is quite popular among the UG students. The first offering of my advanced course on 'Foundations of Secure Computation' had 8 students and one of projects initiated in the course led to a publication in a top cryptography venue (NDSS 2017).

Students and Post-doctoral Supervision

Post-doctoral Rsearcher

1. Varsha Bhat Kukkala (August 2020–): Working on Secure Allegation Escrows.

PhD

1. Divya Ravi (August 2016 – July 2020):
   (a) Thesis Title: The Round Complexity Landscape of Secure Multiparty Computation.
   (b) Thesis based on: *ASIACRYPT 2020, ASIACRYPT 2019*, *IEEE Transactions on Information Theory 2018*, *CRYPTO 2018*, *ACM CCS 2018*.
   (c) Publications: *ASIACRYPT 2020, ASIACRYPT 2019*, *IEEE Transactions on Information Theory 2018*, *CRYPTO 2018*, *ACM CCS 2018*, *SIROCCO 2018*, *DISC 2017* and ICITS 2017.
   (d) Selected to attend Women in Theory workshop 2020. Received 2nd Prize at 10th IDRBT Doctoral Colloquium 2020. Student Best Paper Award at EECS Research Students' Symposium - 2020.
   (e) Current Employment: Post-doctoral Researcher at Aarhus University, Denmark with Prof. Ivan Damgaard.
2. Ajith S (August 2017 – ongoing):
   (a) Received ***Google PhD fellowship 2019. Selected to participate in Heidelberg Laureate Forum 2020.***
   (b) Publications in *USENIX'21 (two papers), NDSS'20 (two papers), PoPETs 2020, ACM CCSW 2019, PPML 2019*.
   (c) One of the NDSS'20 publications is a student paper (along with another student).
3. Nishat Koti (August 2017 – ongoing):
   (a) Received ***Cisco PhD fellowship 2019.***

(b) Publications in *USENIX'21*.

4. Protik Paul (August 2018 – ongoing): Joint works under submission.
5. Shravani Patil (August 2019 – ongoing): Joint works under submission.
6. Moumita Dutta (August 2020 – ongoing):

M. Tech (Research)

1. Ajith S (August 2014 – August 2017):
   (a) Thesis Title: Fast Actively Secure OT Extension for Short Secrets
   (b) Thesis based on: *NDSS 2017*
   (c) Continuing PhD under my supervision from August 2017.
2. Pratik Sarkar (August 2015 – August 2018):
   (a) Thesis Title: Adaptively Secure Primitives in the Random Oracle Model
   (b) Thesis based on: *PKC 2018* .
   (c) Publication during the programme: *NDSS 2017*, *PKC 2018*, *SIROCCO 2018*.
   (d) Recipient of M. Tech funding from *Robert Bosch Center for Cyber Physical Systems for the project titled "Computing on private data in high-latency networks"* .
   (e) Joined Prof. Ran Canetti for PhD at Boston University from September 2018.
3. Megha Byali (August 2016 – July 2019): Thesis based on: *ACM CCS 2019.*
   (a) Thesis Title: Practically Efficient Secure Small Party Computation over the Internet
   (b) Thesis based on: *ACM CCS 2019.*
   (c) Publication during the programme: *PoPETS 2020, ACM CCS 2019, ACM CCS 2018.*
   (d) Awarded ***Swamy medal for the best M.Tech. Research thesis in the Dept. of Computer Science & Automation, IISc in 2020.***
   (e) Current employment: Citrix
4. Swati Singla (August 2016 – July 2019):
   (a) Thesis Title: Honest Majority and Beyond: Efficient Secure Computation over Small Population
   (b) Thesis based on part of *ACM CCS 2019*
   (c) Publication during the programme: *ASIACRYPT 2020, ACM CCS 2019*.
   (d) Current employment: Google
5. Harsh Choudhary (August 2017 – December 2019):
   (a) Thesis Title: Privacy Preserving Machine Learning via Multi-party Computation
   (b) Thesis based on: *PoPETs 2020.*
   (c) Publication during the programme: *PoPETs 2020, ACM CCSW 2019, PPML 2019*.
   (d) Current employment: Myntra

M. Tech

1. Mahak Pancholi (January 2019 – July 2020):
   (a) Thesis Title: A Robust PPML framework for Three Servers
   (b) Received ***CISCO scholarship 2019***.
2. Arun Joseph (January 2017 - July 2018):
   (a) Thesis title: A Framework for Efficient Secure Three-Party Computation
3. Divya Ravi (January 2015 - July 2016):
   (a) Thesis title: On Verifiable Secret Sharing With Honest Majority
4. Dheeraj Ram (January 2015 - July 2016):
   (a) Thesis title: On Scalable Secure Computation
5. Aakar Deora (January 2014 - July 2014):
   (a) Thesis title: On Verifiable Secret Sharing With Honest Majority

General Information

1. I love photography and I am happy to share with you my *photo-steam*. My photography skills have been acknowledged. *This* photograph was selected as the BIG PICTURE of the week by 'The Telegraph, UK'. *This* photograph had got honorable mention in the photo contest organized by 'PhotoContests.com' in the 'Reflection' category.
2. As and when the fancy of writing strikes me, I put down my thoughts in this space `http://arpitapatra.blogspot.com/`.
3. My hobbies also include: Traveling, Yoga, Swimming, Hiking, Cycling, Reading classical literature in Bengali and English.
4. I am a Yoga Enthusiast. Recently, I completed 108 Surya Namaskara Challenge on the eve of Ratha Saptami.
5. I am a Yellow Belt in Hapkido - A Self Defence Based Korean Martial Arts.
6. I am a passionate marathon runner and can run upto 10 km. I have come first in 5KM marathon (women category) in IIIT Bangalore's annual sport event Spandan 2015 and have come 2nd in 10 KM marathon (women category) in IISc's annual sport event Spectrum 2018.
7. Languages known: English, Hindi and Bengali (Mother Tongue).

8. I am an Indian citizen.