Arpita **Patra**

Assistant Professor · Cryptographer

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

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

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

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

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

Visiting Scientist (Hosted by Prof. Bimal Roy) — *January 2014–May 2014*

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*

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

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

Research Interest

My specialisation is on cryptography, a key enabling technology for cybersecurity. In cryptography, my focus is on the standard-bearer problem, called multi-party computation (MPC) that allows a set of distrusting parties to jointly perform a collaborative computation on their private inputs in a way that no coalition of cheating parties can learn more information than their intended outputs. MPC finds application in any scenario that involve computations on sensitive data from two or more entities. E-election, e-auction, privacy-preserving bioinformatics, biometrics, machine-learning, outsourcing and data analytics, preventing satellites from collision are few of the many applications of MPC. I also work in the area of fault-tolerant distributed computing that includes classic problems such as broadcast and Byzantine Agreement (BA) that allow a set of distrusting parties to jointly reach agreement on their private inputs even in the face of a coalition of cheating parties. The core focus of my research can be broadly classified into three areas as follows and as elaborated below: (a) Foundations of MPC; (b) Applied MPC; (c) Fault-tolerant Distributed Computing.

Foundations 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 in IEEE Transactions on Information Theory 2018, IEEE Transactions on Information Theory 2017, Journal of Cryptology 2017, CRYPTO 2017, Journal of Cryptology 2015, SCN 2016, ASIACRYPT 2013, DISC 2013, SCN 2014, ASIACRYPT 2012, PODC 2012, ASIACRYPT 2011, AFRICACRYPT 2010, CRYPTO 2009.

Fault-tolerant Distributed Computing: This area includes classic problems such as Byzantine Agreement and message communication over untrusted network and involves foundational feasibility, efficiency and optimality questions as in the MPC domain. My works in this regime have appeared in Distributed Computing Journal 2014, DISC 2017, PODC 2016, Journal of ACM 2012, Journal of Parallel and Distributed Computing 2011, OPODIS 2011, PODC 2010. ICDCN 2010, PODC 2009, PODC 2008, DISC 2007.

Applied MPC: Building practically efficient constructions for MPC and its building blocks is the primary concern here. My works in this regime have appeared in NDSS 2017 and are under submission in a few venues.

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. **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**, Divya Ravi. On the power of Hybrid Networks in Secure Multi-party Computation. *Accepted to IEEE Transactions on Information Theory, 2018*
2. Carmit Hazay, **Arpita Patra**. Efficient One-Sided Adaptively Secure Computation. *Journal of Cryptology, vol. 30, no. 1, pp. 321–371, 2017*.
3. 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*.
4. **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*.
5. **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Efficient Asynchronous Byzantine Agreement with Optimal Resilience. *Distributed Computing Journal, vol. 27, no. 2, pp. 111- 146, 2014*.
6. 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*.
7. 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*.
8. **Arpita Patra**, Ashish Choudhary, 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*.
9. **Arpita Patra**, Ashish Choudhary, 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*.
10. **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*.
11. 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. 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*.
2. 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*.
3. **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 2016), Internet Society, 2017*.

4. 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*.
5. Ashish Choudhury, Gayathri Garimella, **Arpita Patra**, Divya Ravi and Pratik Sarkar. Crash-tolerant Consensus in Directed Graph Revisited. *31st International Symposium on Distributed Computing (DISC 2017), LIPIcs 91, pp. 46:1–46:4, 2017*.
6. 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*
7. Ashish Choudhury, Emmanuela Orsini, **Arpita Patra**, Nigel Smart. Linear Overhead Robust MPC with Honest Majority Using Preprocessing. 11^{th} *Conference on Security and Cryptography in Networks (SCN 2016), LNCS 9841, pp 147–168, Springer, 2016*
8. 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.*
9. 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*
10. 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.*
11. 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*
12. 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*
13. 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*
14. 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*
15. 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*.
16. 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*.
17. 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*
18. **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*.
19. 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*.
20. 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*.
21. **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*.
22. 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.*
23. **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*.
24. **Arpita Patra**, Ashish Choudhary 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*.
25. **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*.
26. **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*
27. **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*.
28. **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.*
29. **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.*
30. 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.*
31. **Arpita Patra**, Ashish Choudhary, 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*.

32. Kannan Srinathan, Ashish Choudhary, **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*.
33. 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.*
34. **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.
35. **Arpita Patra**, Ashish Choudhury, Madhu Gayatri and C. Pandu Rangan. Efficient Perfectly Reliable and Secure Communication Tolerating Mobile Adversary. 13^{th} *Australasian Conference on Information Security and Privacy (ACISP 2008), LNCS 5107, pp. 170–186, 2008.*
36. **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.*
37. Ashish Choudhary, **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*.
38. **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.*
39. **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 & Under Submission

1. Chaya Ganesh and **Arpita Patra**. Broadcast Extensions with Optimal Communication and Round Complexity. *Communicated to Distributed Computing Journal*.
2. Carmit Hazay and Yehuda Lindell and **Arpita Patra**. Adaptively Secure Computation with Partial Erasures. *Communicated to Information and Computation.*
3. **Arpita Patra** and Divya Ravi. On the Exact Round Complexity of Three-party Computation. *Under Submission*.
4. Laasya Bangalore, Ashish Choudhury, **Arpita Patra**. Almost-Surely Terminating Asynchronous Byzantine Agreement Revisited. *Under Submission*.
5. Megha Byali, Arun Joseph, **Arpita Patra** and Divya Ravi. Fast Secure Computation for Small Population. *Under Submission*.
6. Megha Byali, **Arpita Patra**, Divya Ravi and Pratik Sarkar. Fast, Universally-Composable Oblivious Transfer and Commitment Scheme with Adaptive Security. *Under Submission*.

Projects & Grants

1. Secure Multi-party Computation: Feasibility and Efficiency: PI; *Funded by Science and Engineering Research Board (SERB), India* for a period of three years starting from 2017; Grant Value: ₹15,00,000.
2. Efficient Secure Multi-party Computation: *Funded by INSPIRE DST for a period of five years starting from 2015*. Grant Value: ₹35,00,000.
3. Multi-party Computation. *Funded by Engineering and Physical Sciences Research Council (EPSRC) of United Kingdom for a period of two years starting from July 2015*. Jointly with Prof. Nigel P. Smart and Dr. Ashish Choudhury. Grant Value: 70,471 GBP.
4. Information Security Research and Development. *Funded by Department of Electronics & Information Technology (DeitY) for a period of five years starting from 2015*. Jointly with Prof. N Balakrishnan, Prof C E Veni Madhavan, Dr Bhavana Kanukurthi, Dr. Sanjit Chaterjee.
5. Secure Multiparty Computation- startup grant. *Funded by IISc for a period of two years starting from 2014*. Grant Value: ₹25,00,000.

Honors & Awards

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).

Talks & Presentations

1. 16th March 2018. Multi-party Computation, *Invited Speech at IEEE CONECCT 2018*, Bangalore, India.

2. 8th January 2018. Impossibility Results for Information-theoretic Multi-party Computation, ***Invited Speech at IISC-IACR School on Cryptology 2018***, Bangalore, India.
3. 7th January 2018. Information-theoretic Multi-party Computation with Honest Majority, ***Invited Speech at IISC-IACR School on Cryptology 2018***, Bangalore, India.
4. May and June 2017. OT Extensions, ISEA Workshop on Cryptography, IISc, India.
5. May and June 2017. Garbled Circuit and Yao Two Party Computation, ISEA Workshop on Cryptography, IISc, India.
6. May and June 2017. Computing on Private Data aka Multi-Party Computation, ISEA Workshop on Cryptography, IISc, India.
7. March and April 2017. Fast Actively Secure OT Extension for Short Secrets. *MPC School and Workshop*, IIT Bombay, India and *Theory and Practice of Multi-Party Computation Workshop*, Bristol, UK.
8. March 2017. Garbled Circuit and Yao's Two-party Computation. *MPC School and Workshop*, IIT Bombay, India.
9. March 2017. Oblivious Transfer and Extensions. *MPC School and Workshop*, IIT Bombay, India.
10. March 2016. A Tribute to Diffie and Hellman: The Winners of Turing Award 2015. *Dept. of Computer Science & Automation*, IISc, India.
11. February 2015. Introduction to Cryptography. *Workshop on Introduction to Cryptography*, IISc, India.
12. February 2015. Perfect Security. *Workshop on Introduction to Cryptography*, IISc, India.
13. February 2015. PRF and CPA-Security of SKE. *Workshop on Introduction to Cryptography*, IISc, India.
14. February 2015. Introduction to Secure Computation. *Workshop on Topics in Cryptography*, IISc, India.
15. February 2015. Secret Sharing and Information-Theoretic Secure Computation. *Workshop on Topics in Cryptography*, IISc, India.
16. November 2015. Multiparty Computation *Annual Meeting of Indian Academy of Sciences*, IISER Pune, India.
17. September 2015. Linear Overhead Multiparty Computation *National Workshop on Cryptology 2015*, KIT, Bhubaneswar, India.
18. August 2015. Linear Overhead Multiparty Computation with Honest Majority. *IIIT Delhi*, India.
19. December 2014. Verifiable Secret Sharing. *Recent Advances in Cryptography Workshop*, IIT Delhi, India.
20. October 2014. A simple and Efficient Framework for Secure Multiparty Computation. *Indo-Russian Workshop on Discrete Mathematics, Algebra, Number Theory and their Applications*, Moscow State University, Russia.
21. December 2013. Between a Rock and a Hard Place: Interpolating Between MPC and FHE. *ASIACRYPT 2013*, Bengaluru, India.
22. November 2013. A simple and Efficient Framework for Secure Multiparty Computation. *IISc Bangalore*, Bengaluru, India.
23. October 2013. Asynchronous Multiparty Computation with Linear Communication Complexity. *DISC 2013*, Jerusalem, Israel.
24. January 2013. Anonymous Authentication with Shared Secrets. *Bar-Ilan University*, Ramat Gan, Israel.
25. December 2012. Anonymous Authentication with Shared Secrets. *ISI Kolkata*, Kolkata, India.
26. December 2011. Computational Verifiable Secret Sharing Revisited. *ASIACRYPT 2011*, Seoul, South Korea.
27. December 2011. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity. *OPODIS 2011*, Toulouse, France.
28. August 2011. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity. *ISI Kolkata*, Kolkata, India.
29. May 2011. Communication Optimal Multi-valued Asynchronous Byzantine Agreement with Optimal Resilience. *ICITS 2011*, Amsterdam, The Netherlands.
30. May 2010. Verifiable Secret Sharing. *National Level Instructional Workshop on Cryptology 2010*, Imphal, Manipur, India.
31. January 2010. On Communication Complexity of Secure Message Transmission in Directed Networks. *ICDCN 2010*, Kolkata, India.
32. December 2009. Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience. *INDOCRYPT 2009*, New Delhi, India.
33. December 2009. Efficient Statistical Asynchronous Verifiable Secret Sharing with Optimal Resilience. *ICITS 2009*, Japan.
34. September 2009. Secure Distributed Computation and Communication. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
35. September 2009. Information Checking Protocols. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
36. September 2009. Reliable and Secure Message Transmission. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
37. August 2009. The Round Complexity of Verifiable Secret Sharing Revisited. *CRYPTO 2009*, Santa Barbara, USA.
38. August 2009. Simple and Efficient Asynchronous Byzantine Agreement with Optimal Resilience, *PODC 2009*, Calgary, Canada.
39. August 2009. Information Theoretically Secure Multi Party Set Intersection Re-Visited. *SAC 2009*, Calgary, Canada.
40. June 2009. Secret Sharing Protocols. *CRSI-IMSc Joint Workshop on Teaching Cryptology 2009*, ISI, India.
41. December 2008. Round Efficient Unconditionally Secure Multiparty Computation Protocol. *INDOCRYPT 2008*, IITKgp, India.
42. September 2008. On Tradeoff Between Network Connectivity, Phase Complexity and Communication Complexity of Reliable Communication Tolerating Mixed Adversary. *China Theory Week (CTW) 2008*, Tsinghua University, Beijing, China.
43. August 2008. On Tradeoff Between Network Connectivity, Phase Complexity and Communication Complexity of Reliable Communication Tolerating Mixed Adversary. *PODC 2008*, Toronto, Canada.
44. August 2008. Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary. *ICITS 2008*, Calgary, Canada.
45. December 2007. Probabilistic Perfectly Reliable and Secure Message Transmission - Possibility, Feasibility and Optimality. *INDOCRYPT 2007*, Chennai, India.
46. December 2007. Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary. *CANS 2007*, Singapore.
47. December 2006. Constant Phase Bit Optimal Protocols for Perfectly Reliable Message Transmission. *INDOCRYPT 2006*, Kolkata, India.

Professional Activities

Programme Committee (PC Chair)

INDOCRYPT'17 (18th International Conference on Cryptology in India) along with Prof. Nigel Smart, University of Bristol, UK.

Programme Committee (PC) Member

2018	ASIACRYPT'18, EUROCRYPT'18, PKC'18, ICISS'18
2017	ASIACRYPT'17, PKC'17, ICITS'17
2016-12	INDOCRYPT'16,'15,'12

External Reviewer

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

Courses

1. QIP short-term course on "Foundations of Cryptography" to be offered from 23rd - 27th July, 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. To be offered in 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.
5. CSA E0 312: Foundations of Secure Computation. Credit: 3:1. August-December 2015, 2017.

In all the above courses that are offerred, 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 Supervision

PhD

1. Divya Ravi (August 2016 – ongoing): Joint projects accepted to *IEEE Transactions on Information Theory*, *31st International Symposium on Distributed Computing (DISC 2017)* and *10th International Conference on Information Theoretic Security (ICITS 2017)*. Joint projects submitted to *CRYPTO 2018* and *IEEE S&P 2018*
2. Ajith S (August 2017 – ongoing)
3. Nishat Koti (August 2017 – ongoing)

M. Tech (Research)

1. Ajith S (August 2014 – August 2017); thesis is based on a paper published in *24th Annual Network and Distributed System Security Symposium (NDSS 2017)*
2. Pratik Sarkar (August 2015 – ongoing); Joint projects published in *24th Annual Network and Distributed System Security Symposium (NDSS 2017)* and *21st International Conference on Practice and Theory of Public-Key Cryptography (PKC 2018)*. Joint project submitted to *11th Conference on Security and Cryptography for Networks (SCN 2018)*; Joining Prof. Ran Canetti for PhD at Boston University from September 2018.
3. Megha Byali (August 2016 – ongoing); Joint projects submitted to *IEEE S&P 2018* and *11th Conference on Security and Cryptography for Networks (SCN 2018)*
4. Swati Singla (August 2016 – ongoing)
5. Harsh Choudhary (August 2017 – ongoing)

M. Tech

I have guided four M. Tech students so far.

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. Blogging caught my fancy very recently. As and when the fancy strikes me, I put down my thoughts in this space `http://arpitapatra.blogspot.co.uk`.
3. My hobbies also include: Traveling, Hiking, Reading classical literature in Bengali and English, Reciting poems, listening music, Badminton, Yoga, Hapkido, Swimming.
4. I am a Yellow Belt in Hapkido - A Self Defense Based Korean Martial Arts.

5. 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 Spentrum 2018.
6. Languages known: English, Hindi and Bengali (Mother Tongue).
7. I am an Indian citizen.