ARPITA PATRA

Dept. of Computer Science & Automation,
Indian Institute of Science, Bangalore
Bengaluru, 560012
India
http://drona.csa.iisc.ernet.in/~arpita/
arpita@csa.iisc.ernet.in
arpitapatra10@gmail.com

Apartment No.101,
KT-39, Leela Niwas,
4th Main, 15th Cross, Malleshwaram,
Bangalore 560003,
India

Current Position

Assistant Professor at Dept. of Computer Science & Automation, Indian Institute of Science (IISc) Bangalore. May 2014–Present

Education

◇ **Ph.D. in Computer Science and Engineering** India
Indian Institute of Technology (IIT) Madras August 2006–May 2010
CGPA: 9.50/10
Dissertation Area: Cryptography
Dissertation Title: Studies on Verifiable Secret Sharing, Byzantine Agreement and Multi-party Computation
Supervisor: Prof. C. Pandu Rangan

◇ **Master of Science (by research) in Computer Science and Engineering** India
Indian Institute of Technology (IIT) Madras August 2004–July 2006
CGPA: 9.60/10
Dissertation Area: Image Processing
Dissertation Title: Efficient Methods for Face Recognition and Multimodal Biometry
Supervisor: Prof. Sukhendu Das

◇ **Bachelor of Technology in Computer Science and Engineering** India
Haldia Institute of Technology August 2000–July 2004
CGPA: 9.61/10
Project Area: Formal methods of verification
Project Title: Development of Timing Analysis Tool for Asynchronous Systems
Under the guidance of Prof. Supratik Chakraborty, IIT Bombay

Work History and Academic Visits

◇ **Visiting Scientist** January 2014–May 2014.
Indian Statistical Institute (ISI) Kolkata
Hosted by Prof. Bimal Roy.

◇ **Post-doctoral Researcher** September 2012–December 2013.
University of Bristol, United Kingdom
Hosted by Prof. Nigel P. Smart.

◇ **Postdoctoral Researcher** September 2011–August 2012.
ETH Zurich, Switzerland,
Hosted by Prof. Ueli Maurer.

◇ **Postdoctoral Researcher** September 2010–August 2011.
Aarhus University, Denmark,
Hosted by Prof. Ivan Damgård.

◇ **Visitor** January 2013–March 2013.
Bar-Ilan University, Israel,
Hosted by Prof. Yehuda Lindell.

Research Interests

The focus of my research is the theoretical foundations of *cryptography* that are concerned with the *feasibility* of securely realizing cryptographic tasks, finding inherent *lower bounds* on the computational resources that are needed for solving cryptographic tasks and finding *resource efficient* secure constructions. The resources most often considered are computational complexity (i.e., measuring the time required to compute some cryptographic function like encryption or secure computation of a functionality), round and communication complexity (i.e., the number of rounds and bandwidth required for a secure interactive protocol). The topics of cryptography I have been interested in so far include: Secure Communication, Secure Multiparty Computation, Verifiable Secret Sharing, Adaptive Security, Public Key Encryption, Oblivious Transfer, Zero Knowledge Proofs, Byzantine Agreement and Broadcast.

Research Topics

◇ **Secure Communication**
Published at Journal of ACM (JACM)'12, Journal of Parallel and Distributed Computing (JPDC)'11, ICDCN'10, PODC'09, ICDCN'09, PODC'08, DISC'07 etc.

◇ **Verifiable Secret Sharing.**
Published at Journal of Cryptology. Published at ASIACRYPT'12, PODC'12, ASIACRYPT'11, CRYPTO'09 etc. Further works under submission.

◇ **Byzantine Agreement and Broadcast.**
Published at Distributed Computing Journal, OPODIS'11, PODC'10. PODC'09 etc. Further works under submission.

◇ **Multiparty Computation.**
Published at Journal of Cryptology, ASIACRYPT'13, DISC'13, SCN'14, AFRICACRYPT'10 etc. Further works under submission.

◇ **Adaptive Security.**
Published at TCC'14, PODC15. Further works under submission and under progress.

◇ **Anonymous Authentication.**
Published at SCN'14, Latincrypt'14.

◇ **Selective Opening Attack Secure Public Key Encryptions.**
Published at ASIACRYPT'15.

Refereed Publications

Following the standard in Theoretical Computer Science, the authors in the publications (except my PhD publications) are listed in alphabetical order. The papers marked with $*$ appeared in top publication fora.

REFEREED JOURNALS

1 $*$ **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*.

2 $*$ **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*.

3 ∗ 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*.

4 ∗ 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*.

5 **Arpita Patra**, Ashish Choudhary, C. Pandu Rangan and Kannan 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*.

6 **Arpita Patra**, Ashish Choudhary, C. Pandu Rangan, Kannan Srinathan and Prasad Raghavendra. Perfectly Reliable and Secure Message Transmission Tolerating Mobile Adversary. *International Journal of Applied Cryptography (IJACT), vol. 1, Issue 3, pp. 200-224, 2009*.

7 ∗ **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*.

8 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*.

REFEREED CONFERENCES

9 ∗ Carmit Hazay and **Arpita Patra** and Bogdan Warinschi. Selective Opening Security Revisited. *ASIACRYPT 2015*.

10 ∗ Carmit Hazay and 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.*.

11 ∗ 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.

12 ∗ Ashish Choudhury and **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*.

13 Joel Alwen, Martin Hirt, Ueli Maurer, **Arpita Patra** and Pavel Raykov. Anonymous Authentication with Shared Secrets. Cryptology ePrint Archive, Report 2014/073. 3^{rd} *International Conference on Cryptology and Information Security in Latin America (LatinCrypt 2014), LNCS 8895, pp. 219–236, 2014*.

14 ∗ 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*.

15 ∗ Carmit Hazay and **Arpita Patra**. Constant Round One-Sided Adaptively Secure Two-Party Computation. 11^{th} *Theory of Cryptography Conference (TCC 2014), LNCS 8349, pp. 368-393, 2014*.

16 ∗ 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.

17 ∗ Ashish Choudhury, 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.*

18 ∗ 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.*

19 ∗ 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.*

20 ∗ **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.*

21 ∗ 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.*

22 Ashish Choudhury and **Arpita Patra**. On the Communication Complexity of Reliable and Secure Message Transmission in Asynchronous Networks. 14^{th} *Information Security and Cryptology Conference (ICISC 2011), LNCS 7259, pp. 450-466, 2011.*

23 ∗ 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.*

24 ∗ **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.*

25 Ashish Choudhury, **Arpita Patra**. Statistical Asynchronous Weak Commitment Scheme: A New Primitive to Design Statistical Asynchronous Verifiable Secret Sharing Scheme. 7^{th} *International Workshop on Coding and Cryptography (WCC 2011), 2011.*

26 ∗ 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.*

27 ∗ **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.*

28 ∗ **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.*

29 ∗ **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.*

30 **Arpita Patra** and C. Pandu Rangan. Communication Optimal Multi-Valued Asynchronous Broadcast Protocol. 1^{st} *International Conference on Cryptology and Information Security in Latin America (LATINCRYPT 2010), LNCS 6212, pp. 162-177, 2010*.

31 $*$ **Arpita Patra**, Ashish Choudhary, Tal Rabin 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*.

32 $*$ **Arpita Patra**, Ashish Choudhary 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*.

33 $*$ **Arpita Patra**, Ashish Choudhary 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*.

34 $*$ **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Brief Announcement: 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*.

35 $*$ Ashish Choudhary, **Arpita Patra**, Ashwinkumar B.V, 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*.

36 $*$ **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*.

37 **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Communication Efficient Statistical Asynchronous Multiparty Computation with Optimal Resilience. 5^{th} *International Conferences on Information Security and Cryptology (INSCRYPT 2009), LNCS 6151, pp. 179-197, 2009*.

38 **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience. 10^{th} *International Conference on Cryptology in India (INDOCRYPT 2009), LNCS 5922, pp. 398-417, 2009*.

39 Sathya Narayanan G, Aishwarya T, Anugrah Agrawal, **Arpita Patra**, Ashish Choudhary, C. Pandu Rangan. Multi Party Distributed Private Matching, Set Disjointness and Cardinality Set Intersection with Information Theoretic Security. 8^{th} *International Conference on Cryptology and Network Security (CANS 2009), LNCS 5888, pp. 21-40, 2009*.

40 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*.

41 $*$ AshwinKumar B. V, **Arpita Patra**, Ashish Choudhary, 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*.

42 ∗ Kannan Srinathan, Ashish Choudhary, **Arpita Patra** and C. Pandu Rangan. Brief Announcement: Efficient Single Phase Unconditionally Secure Message Transmission with Optimum Communication Complexity. 27^{th} *Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2008), pp. 457, ACM Press, 2008*.

43 ∗ **Arpita Patra**, Ashish Choudhary, 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*.

44 ∗ **Arpita Patra**, Ashish Choudhary 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*.

45 **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Round Efficient Unconditionally Secure Multiparty Computation Protocol. 9^{th} *International Conference on Cryptology in India (INDOCRYPT 2008), LNCS 5365, pp. 185 - 199, 2008*.

46 ∗ 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*.

47 Kannan Srinathan, **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Unconditionally Reliable Message Transmission in Directed Hypergraphs. 7^{th} *International Conference on Cryptology and Network Security (CANS 2008), LNCS 5339, pp. 285–303, LNCS 5339, 2008*.

48 ∗ **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Brief Announcement: 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*.

49 ∗ **Arpita Patra**, Ashish Choudhary, K. Srinathan and C. Pandu Rangan. Brief Announcement: 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*.

50 **Arpita Patra**, Bhavani Shankar, Ashish Choudhary, Kannan Srinathan and C. Pandu Rangan. Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary. 6^{th} *International Conference on Cryptology and Network Security (CANS 2007), LNCS 4856, pp. 80–101, 2007*.

51 Kannan Srinathan, **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Probabilistic Perfectly Reliable and Secure Message Transmission - Possibility, Feasibility and Optimality. 8^{th} *International Conference on Cryptology in India (INDOCRYPT 2007), LNCS 4859, pp. 101–122, 2007*.

52 **Arpita Patra**, Ashish Choudhary, Kannan Srinathan and C. Pandu Rangan. Constant Phase Bit Optimal Protocols for Perfectly Reliable Message Transmission. 7^{th} *International Conference on Cryptology in India (INDOCRYPT 2006), LNCS 4329, pp. 221–235, 2006*.

53 **Arpita Patra** and Sukhendu Das. Dual Space based Face Recognition using Feature Fusion. *International Conference on Visual Information Engineering (IEE-VIE 2006), pp. 18–23, 2006*.

Preprints and Submissions

- Chaya Ganesh and **Arpita Patra**. Multi-valued Broadcast Revisited. *In Preparation*.
- Ashish Choudhury, Emmanuela Orsini **Arpita Patra** and Nigel Smart. Linear Overhead Robust MPC with Honest Majority Using Preprocessing. *In Submission*.
- Ashish Choudhury and **Arpita Patra**. An Efficient Framework for Unconditionally-secure Multiparty Computation. *Communicated to IEEE Transactions on Information Theory.*.
- Carmit Hazay and Yehuda Lindell and **Arpita Patra**. Adaptively Secure Computation with Partial Erasures. *Communicated to Journal of Cryptology.*.
- Carmit Hazay and **Arpita Patra**. One-Sided Adaptively Secure Two-Party Computation. *Communicated to Journal of Cryptology*.
- **Arpita Patra**, Ashish Choudhary and C. Pandu Rangan. Efficient Statistical Asynchronous Verifiable Secret Sharing and Multiparty Computation with Optimal Resilience. *Communicated to Information and Computation Journal*.
- **Arpita Patra**, Ashish Choudhury, and C. Pandu Rangan. Statistically Reliable and Secure Message Transmission in Directed Networks. *Communicated to Information and Computation Journal*.

Awards, Scholarships and Achievements

- **Associate of Indian Academy of Sciences**.
- **DST INSPIRE Faculty Fellowship** 2015.
- **Google India Women in Engineering Award** 2008.
- **Microsoft Research India Fellowship** during PhD.
- **First prize in Techvista 2007** - the annual flagship event of Microsoft Research India, (jointly with my co-researcher Mr. Ashish Choudhary). Around 27 posters were called for presentation from all over India at TechVista 2007.
- **Second prize in Techvista 2006** - the annual flagship event of Microsoft Research India, (jointly with my co-researcher Mr. Ashish Choudhary). Around 25 posters were called for presentation from all over India at TechVista 2006.
- **First prize at IRISS (Inter Research Institute Student Seminar) 2007** held at IIIT Hyderabad.
- Recipient of **Indian Institute of Technology (GATE) Scholarship for doing Masters** in the Department of Computer Science and Engineering, Indian Institute of Technology, Madras.
- Recipient of **Gold Medal for securing First Rank** in the University (Vidyasagar University) during B. Tech (in Computer Science) 2004.
- Secured fourth position in all India M. Sc entrance examination conducted by **Chennai Mathematical Institute (CMI), Chennai for admission to M. Sc programme** in Computer Science at CMI.
- School First Rank holder in West Bengal Board X Std. Examination, 1998.

Talks and Presentations

- August 2015. Linear Overhead Multiparty Computation with Honest Majority. *IIIT Delhi*, India.
- December 2014. Verifiable Secret Sharing. *Recent Advances in Cryptography Workshop*, IIT Delhi, India.

- ◇ 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.
- ◇ December 2013. Between a Rock and a Hard Place: Interpolating Between MPC and FHE. *ASIACRYPT 2013*, Bengaluru, India.
- ◇ November 2013. A simple and Efficient Framework for Secure Multiparty Computation. *IISc Bangalore*, Bengaluru, India.
- ◇ October 2013. Asynchronous Multiparty Computation with Linear Communication Complexity. *DISC 2013*, Jerusalem, Israel.
- ◇ January 2013. Anonymous Authentication with Shared Secrets. *Bar-Ilan University*, Ramat Gan, Israel.
- ◇ December 2012. Anonymous Authentication with Shared Secrets. *ISI Kolkata*, Kolkata, India.
- ◇ December 2011. Computational Verifiable Secret Sharing Revisited. *ASIACRYPT 2011*, Seoul, South Korea.
- ◇ December 2011. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity. *OPODIS 2011*, Toulouse, France.
- ◇ August 2011. Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity. *ISI Kolkata*, Kolkata, India.
- ◇ May 2011. Communication Optimal Multi-valued Asynchronous Byzantine Agreement with Optimal Resilience. *ICITS 2011*, Amsterdam, The Netherlands.
- ◇ May 2010. Verifiable Secret Sharing. *National Level Instructional Workshop on Cryptology 2010*, Imphal, Manipur, India.
- ◇ January 2010. On Communication Complexity of Secure Message Transmission in Directed Networks. *ICDCN 2010*, Kolkata, India.
- ◇ December 2009. Round Efficient Unconditionally Secure MPC and Multiparty Set Intersection with Optimal Resilience. *INDOCRYPT 2009*, New Delhi, India.
- ◇ December 2009. Efficient Statistical Asynchronous Verifiable Secret Sharing with Optimal Resilience. *ICITS 2009*, Japan.
- ◇ September 2009. Secure Distributed Computation and Communication. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
- ◇ September 2009. Information Checking Protocols. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
- ◇ September 2009. Reliable and Secure Message Transmission. *Grace Hopper Celebration of Women in Computing (GHC) 2009*, Tucson, Arizona, USA.
- ◇ August 2009. The Round Complexity of Verifiable Secret Sharing Revisited. *CRYPTO 2009*, Santa Barbara, USA.
- ◇ August 2009. Simple and Efficient Asynchronous Byzantine Agreement with Optimal Resilience, *PODC 2009*, Calgary, Canada.
- ◇ August 2009. Information Theoretically Secure Multi Party Set Intersection Re-Visited. *SAC 2009*, Calgary, Canada.
- ◇ June 2009. Secret Sharing Protocols. *CRSI-IMSc Joint Workshop on Teaching Cryptology 2009*, ISI, India.

- ◇ December 2008. Round Efficient Unconditionally Secure Multiparty Computation Protocol. *INDOCRYPT 2008*, IITKgp, India.
- ◇ 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.
- ◇ August 2008. On Tradeoff Between Network Connectivity, Phase Complexity and Communication Complexity of Reliable Communication Tolerating Mixed Adversary. *PODC 2008*, Toronto, Canada.
- ◇ August 2008. Perfectly Reliable and Secure Communication Tolerating Static and Mobile Mixed Adversary. *ICITS 2008*, Calgary, Canada.
- ◇ December 2007. Probabilistic Perfectly Reliable and Secure Message Transmission - Possibility, Feasibility and Optimality. *INDOCRYPT 2007*, Chennai, India.
- ◇ December 2007. Perfectly Secure Message Transmission in Directed Networks Tolerating Threshold and Non Threshold Adversary. *CANS 2007*, Singapore.
- ◇ December 2006. Constant Phase Bit Optimal Protocols for Perfectly Reliable Message Transmission. *INDOCRYPT 2006*, Kolkata, India.

Professional Activities

- ◇ External Thesis Reviewer:
  Reviewed six Dual-degree Theses of Dept. of CSE, IITKgp.
- ◇ PC Member:
  SPACE 2013, INDOCRYPT 2012, SPACE 2012, INDOCRYPT 2015.
- ◇ Reviewer:
  CRYPTO 2015, ISIT 2015, PKC 2014, ASIACRYPT 2014, ACM CCS 2013, ASIACRYPT 2013, PKC 2013, CRYPTO 2012, TCC 2012, Crypto 2011, Journal of Cryptology, TCC 2011, INDOCRYPT 2010, ASIACRYPT 2010, PKC 2010, IEEE Transactions on Dependable and Secure Computing, Design, Codes and Cryptography, ICITS 2009, ICALP 2009, ACISP 2008, ICITS 2008, ASIACRYPT 2008, CANS 2008.

Teaching Experience

- ◇ Course Instructor, IISc — Aug-Dec 2015
  Secure Computation.
- ◇ Course Instructor, IISc — Jan-April 2015
  Cryptography.
- ◇ Course Instructor, IISc — Aug-Dec 2014
  Discrete Structures.
- ◇ Teaching Assistant, ETH Zurich — Spring 2012
  Cryptographic Protocols.
- ◇ Teaching Assistant, ETH Zurich — Fall 2011
  Discrete Mathematics.
- ◇ Teaching Assistant, IIT Madras — 2006–2010
  Data Structures and Algorithms (DSA)
  Advanced Data Structures and Algorithms (ADSA)
  Recent Developments in Theoretical Computer Science (RDTCS)
  Topics in Design and Analysis of Algorithms (TDAA)

General Information

- ◇ I love photography and I am happy to share with you my photo stream: `http://www.flickr.com/photos/arpitapatra/`. My photography skills have been acknowledged.
  - · One of the photographs taken by me was selected as the BIG PICTURE of the week by 'The Telegraph, UK'. See `http://www.telegraph.co.uk/travel/picturegalleries/9836246/The-Big-Picture-photography-competition-round-240.html` for the details.
  - · Another photograph had got honorable mention in the photo contest organized by 'PhotoContests.com' in the 'Reflection' category. See `https://www.facebook.com/photo.php?fbid=441320579295153&set=a.441317199295491.1073741830.284972521596627&type=1&permPage=1` for the details.
- ◇ 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`.
- ◇ My hobbies also include: Traveling, Hiking, Reading classical literature in Bengali and English, Reciting poems, listening music, Badminton, Yoga, Hapkido, Swimming.
- ◇ I am a Yellow Belt in Hapkido - A Self Defense Based Korean Martial Arts.
- ◇ I am familiar with the Macintosh, Linux and Windows platforms and have programming experience in C,C++, and Java.
- ◇ I had served as a volunteer during 45th Annual Convocation of IIT Madras.
- ◇ I was part of the team that co-ordinated the hosting of IRISS'06 at IIT Madras.
- ◇ Languages known: English, Hindi and Bengali (Mother Tongue).
- ◇ I am an Indian citizen.

Arpita Patra
August 2015