

Curriculum Vitae

Dr. Sourav Mukhopadhyay

Professor

Department of Mathematics

Indian Institute of Technology Kharagpur

West Bengal, India-721302

Email: sourav@maths.iitkgp.ac.in

<http://www.facweb.iitkgp.ernet.in/~sourav/>

1 Date of Birth: 21st January 1975

2 Academic Qualifications

Degree	Institution/University	Year	Subject	Class/Division	% marks	Rank
PhD*	Indian Statistical Institute, India	2007	Computer Science (Cryptography)	–	–	
M.Tech.	Indian Statistical Institute, India	2001	Computer Science	First Class, Distinction	81	5 th
M.Stat.	Indian Statistical Institute, India	1999	Statistics	First Class	73	4 th
B.Sc.	Ramakrishna Mission Vidamandira, Calcutta University	1997	Mathematics (Hons.)	First Class	70	5 th

*Title of Thesis: A Study on Time/Memory Trade-Off Cryptanalysis

*Supervisor: Prof. Palash Sarkar (Indian Statistical Institute, India)

3 Position and Employment (Starting with the most recent employment)

Sl No.	Institution Place	Position	From (Date)	To (date)
-1	Indian Institute of Technology Kharagpur	Professor	Feb 2020	Till Date
0	Indian Institute of Technology Kharagpur	Associate Professor	Oct 2014	Feb 2020
1	Indian Institute of Technology Kharagpur	Assistant Professor	Dec 2009	Oct 2014
2	School of Electronic Engineering, Dublin City University, Ireland.	Postdoctoral Research Fellow	Feb 2008	Dec 2009
3	School of Electronic Engineering, Dublin City University, Ireland.	Lecturer	Feb 2009	June 2009
4	School of Computer Engineering, Nanyang Technological University	Postdoctoral Research Fellow	Sep 2007	Feb 2008

5	School of Computing, Department of Computer Science, National University of Singapore, Singapore.	Research Assistant	Sep 2006	Sep 2007
6	INRIA Rocquencourt, project CODES, INRIA, France.	Visiting Scientist	April 2006	June 2006
7	Applied Statistics Unit, Indian Statistical Institute, Kolkata.	Project Linked Researcher	Feb 2003	March 2006
8	School of Computing, Department of Computer Science, National University of Singapore, Singapore	Research Assistant	Feb 2002	Dec 2002
9	Machine Intelligent Unit, Indian Statistical Institute, Kolkata	Junior Research Fellow	July 2001	Jan 2002

4 Teaching Experience (Subject/s Taught/Teaching)

Indian Institute of Technology, Kharagpur:

- MA21005/MA21007: DESIGN & ANALYSIS OF ALGORITHMS for *B.Tech./M.Sc(5Y)*. (no. of students: 310), JULY - DEC, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020.
- MA60031/MA51115: CRYPTOGRAPHY AND NETWORK SECURITY for *B.Tech./M.Sc.(5Y)/ M.Sc.(2Y)/M.Tech.* (no. of students: 172), JULY - DEC, 2011, 2012, 2013, 2015, 2016, 2017, 2018.
- MA30006/ MA61002: SWITCHING & FINITE AUTOMATA THEORY for *B.Tech./M.Sc.(5Y)/M.Tech.* (no. of students: 120), JAN - APRIL, 2012, 2013, 2019.
- MA20106: PROBABILITY & STOCHASTIC PROCESSES for *B.Tech.* (no. of students: 160), JAN - APRIL, 2012, 2013, 2014*, 2015*, 2016* (*SUBJECT CO-ORDINATOR).
- MA20104: PROBABILITY AND STATISTICS for *B.Tech.* (no. of students: 160), JAN - APRIL, 2010, 2011.
- MA32006: REGRESSION ANALYSIS for *B.Tech./M.Sc.(5Y)*, JAN - APRIL, 2010, 2011.
- MA41017/MA60067: STOCHASTIC PROCESSES for *B.Tech./M.Sc.(5Y)*, (no. of students: 80) JAN - APRIL, 2017.
- MA31020: REGRESSION AND TIME SERIES MODEL for *B.Tech./M.Sc.(5Y)*, JULY - DEC, 2011.
- MA41009: PROBABILITY AND STATISTICS for *M.Sc.(2Y)*, JULY - DEC, 2010, 2011, 2012.
- MA60002: DATA STRUCTURE AND ALGORITHM for *B.Tech./M.Tech.* (no. of students: 126), JAN - APRIL, 2015, 2016, 2017, 2018, 2019.
- MA41021/MA60001: PROGRAMMING LANGUAGES for *M.Tech.*, JULY - DEC, 2010.

12. MA31009: COMPUTER ORGANISATION & ARCHITECTURE for *M.Sc.(5Y)/M.tech.* (no. of students: 60), JULY - DEC, 2014.
13. MA29005: DESIGN & ANALYSIS OF ALGORITHMS LAB, JULY - DEC, 2011, 2012, 2013, 2018, 2019.
14. MA49010/MA53027: STATISTICAL SOFTWARE LABORATORY, JULY - DEC, 2010, 2014.
15. MA69004: DATA STRUCTURE AND ALGORITHM LABORATORY, JAN - APRIL, 2014, 2018.

NPTEL online certified course (MOOC):

16. Cryptography and Network Security (no. of students: 15048), JAN-APRIL, 2018, 2019, 2020.
17. Introduction to Automata. Language and Computation (no. of students: 11220), JAN-APRIL, 2019.
18. Introduction to Abstract and Linear Algebra (no. of students: 4817), August - December 2018, 2019.
19. Introduction to Algorithms and Analysis (no. of students: 8500), 2017, 2020.
20. Internetwork Security (no. of students: 7476), JAN-APRIL, 2017.
21. Fundamental Algorithms: Design and Analysis (no. of students: 5200), SEP, 2016.

Dublin City University, Ireland:

22. EE548: Internetwork Security (7.5 credit full course with no. of students is 118), FEB - JUN, 2009.

5 AWARD(S) / HONOUR(S) / FELLOWSHIP DETAILS

1. Offered Assistant Professorship, from the following places:
 - a) CR Rao Advanced Institute of Mathematics, Statistics and Computer Science, 2009.
 - b) Department of Computer Science, Indian Institute of Technology Punjab, 2009
2. Offered Scientist C post from Defence Research & Development Organization (DRDO), New Delhi, India, 2008.
3. Postdoctoral Research Fellow, School of Electronic Engineering, Dublin City University, Dublin 9, Ireland, February 2008- December 2009.
4. Postdoctoral Research Fellow, School of Computer Engineering, Nanyang Technological University, Singapore, September 2007- February 2008.
5. Offered postdoctoral Research position from the following places:
 - a) Center for Information Security Technologies (CIST), Korea University, Seoul, Korea, 2007.
 - b) Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka, Japan, 2006.
6. Offered Scientist C post from National Technical Research Organization (NTRO), Govt. of India, New Delhi, 2007.
7. Visiting Scientist Position, INRIA-Rocquencourt, project CODES, France, April 2006- June 2006.
8. Project Linked Research Assistant, Cryptology Research Group, Applied Statistics Unit, Indian Statistical Institute, February 2003- March 2006.
9. Research Assistant, School of Computing, National University of Singapore, February 2002- December 2002 and September 2006- September 2007.

10. ISI-INSEAD fellowship, France INSEAD and Indian Statistical Institute joint fellowship, 2001.
11. Junior Research Fellowship, Indian Statistical Institute, July 2001- January 2002.
12. Offered the position of Member of Technical Staff, Sun Microsystems (India), 2001.
13. Offered Design Engineer position, Texas Instruments (India), 2001.

6 Research Interests

- a) Time/Memory Trade-off Cryptanalysis
- b) Algebraic Cryptanalysis on Symmetric Cipher.
- c) Digital Rights Managements
- d) Key pre-distribution for Wireless Sensor Networks
- e) Functional Encryption
- f) Quantum Cryptography
- g) Cloud Computing
- h) Block chain, bit-coin and Crypto-currency
- i) A5/3 Decrypter

11 Students Advised

Doctoral Guidance:

Completed (Single guidance):

1. **Sarbari Mitra (Completed in 2014)**. Currently Associate Professor at Fort Hays State University, USA.

Dissertation: A Study on Key Pre-distribution in Wireless Sensor Networks.

2. **Dibyendu Roy (Completed in 2016)**. Currently Assistant Professor at IIIT Vadodara, India.

Dissertation: A study on selective stream ciphers and construction of T-function.

3. **Pratish Datta (Completed in 2017)**. Currently Research Scientist @ CIS Laboratories, NTT Research, Inc., East Palo Alto, California, U.S.A..

Dissertation: Design and Analysis of Expressive and Secure Functional Encryption, Signcryption and Constrained Pseudorandom Function.

4. **Jangirala Srinivas (Completed in 2017)**. Currently Associate professor at O.P. Jindal Global (Institution of Eminence Deemed To Be University), Haryana, INDIA.

Dissertation: Design and Analysis of User Authentication and Key Agreement Schemes for Wireless Sensor Networks

5. **Meenakshi Kansal (Completed in 2020)**. Currently Assistant Professor at SITAICS, RRU Gandhinagar, India.

Dissertation: Design and Analysis of Lattice-based Group Signature, Nominative Signature and Multisignature

6. **Sarbani Roy (Completed in 2020)**. Currently working at Germany.

Dissertation: A study on quantum cryptographic protocols in the device-independent paradigm

7. **Ravi Anand (Completed in 2021)**. Currently Assistant Professor at IIT Delhi, India.

Dissertation: A study on quantum cryptographic protocols in the device-independent paradigm

8. **Dr. Amit Kumar Singh (Completed in 2023)**. Currently Assistant Professor at the Center for Data Science, Department of CSE, SOA (Deemed to be) University, Bhubaneswar, India.

Dissertation: Construction of Broadcast Encryption and Multi-signature Scheme

9. **Subhranil Dutta (Completed in 2024)**. Currently a Post-doctoral fellow at University of St.Gallen (HSG), Switzerland.

Dissertation: Selected Constructive Approaches towards Linear Functional Encryption with Advanced Features for Cloud Computing

10. **Anushree Belel (Completed in 2024)**. Currently Research Associate at ISI Kolkata.

Dissertation: A Study of Provably Secure Advanced Encryption Techniques Using Pairing-Based Cryptography

11. **Ramprasad Sarkar (Completed in 2024)**. Currently a Post-doctoral fellow at ISI Kolkata.

Dissertation: Design and Analysis of Secure and Efficient Broadcast Encryption Protocols with Anonymity, Traceability and Post-Quantum Security

Significant Advisory Role:

1. Dheerendra Mishra (PhD 2014), Advisor: Pawan Kumar
Dissertation: A Study on Privacy and Portability Schemes in Multi-Distributor DRM System.

Ongoing: 4

Master's and Bachelor's Thesis Guidance:

Completed: **120** students

Ongoing: 10 students

Post-Doctoral Guidance:

1. Dr. Vandana: NBHM postdoc (PhD from IIT Kharagpur), 2016-2017
2. Dr. Ankita Chaturvedi: NBHM postdoc (PhD from IIT Roorkee), 2013-2016

Certificate of Excellence in Research:

Dr. Debasish Roy (IPS, DG, WB Police): 2018 - till today

8 Current Sponsored Projects

Sl. No.	Responsibility	Title of the Project	Sponsoring Agency	Amount	Duration
1.	Co-Principal Investigator	Development of QVPN	The Indian ARMY	Rs. 150L	2023-2024
2.	Principal Investigator (Consultancy)	Cryptographic hash algorithm based on quantum paradigm	ARQANUM TECHNOLOGIES PRIVATE LIMITED	Rs. 53L	2022-2023
3.	Principal Investigator	Developing obfuscation based cryptographic primitives and	NBHM, DAE, GOVT. of	Rs. 15L	2021-2024

		investigating their efficient realization	India		
4.	Principal Investigator (Consultancy)	CRYPTOGRAPHY AND CRYPTANALYSIS	Stratign FZE, Dubai, UAE	Rs. 72L	2018 - 2021
5.	Principal Investigator	DEVELOPMENT OF MULTI-PARTY COMPUTATION PROTOCOLS AS AN AID TO CLOUD COMPUTING	SERB, DST, Govt. of India	Rs. 18L	2018 - 2021
6.	Co-Principal Investigator	EARLY DETECTION OF ORAL CANCER USING DIGITAL INFRARED	SERB, DST, Govt. of India	Rs. 38L	2018 - 2021
7.	Co-Principal Investigator	Development of prototype of digital infrared thermal and optical imaging based system for early detection of oral cancer	MHRD, DEPARTMENT OF HIGHER EDUCATION, NEW Delhi	Rs 79L	2014-2017
8.	Principal Investigator	Cryptographic support for digital rights management	CSIR, Govt. of India	Rs 26L	2012-2015
9.	Principal Investigator	Construction of Boolean Functions to Design Cryptographically Secure Stream Cipher	SRIC, IIT KGP	Rs. 5L	2011 - 2014
10.	Co-Principal Investigator	DESIGN AND ANALYSIS OF CRYPTOGRAPHIC PRIMITIVE USING MULTILINEAR MAPS	NBHM	Rs 3.3L	2016-2019

9 Professional Activities

- a) Program Co-Chair: Indocrypt 2024 (Silver Jubilee!!!), the 25th International Conference on Cryptology in India, which will be held at IMSC Chennai, India, December 18-21, 2024.
- b) Organized (principal coordinator and subject expert) online Training course on "Cyber Security and Modern Cryptography" for TEQIP-III faculty members (55 participants) funded by NPIU, MHRD, Govt of India during 9 - 13 November 2020 with a budget of INR 6L.
- c) Organized (principal coordinator and subject expert) a short term trainee course on Cyber Security for **Nigerian Citizens** (serving Nigerian Police officers) during 27 January to 7 February 2020 at IIT-Kharagpur, funded by Stratign FZE, Dubai (UAE) with a budget of USD 30000 (INR 20L).
- d) Organized (principal coordinator) a short term trainee course on Cryptography and Cryptanalysis for **Egyptian military officers** during 25 March to 4 April 2019 at IIT-Kharagpur, funded by the Stratign FZE, Dubai (UAE) with a budget of USD 32000.
- e) Delivered lectures on Cryptography to the officers of CID Crime Branch, Kolkata in April 2019.
- f) Receive top teaching feedback from the students at ERP

- g) Organizing one-day symposium on computational data science and its applications on 17th February 2020 at Dept. of Mathematics, IIT-Kharagpur, funded by Stratign FZE, Dubai (UAE).
- h) Organizing (Subject expert) TEQIP sponsored short term course entitled "Advanced Topics in Cryptography", 10-14 February, 2020 at the department of Mathematics, IIT kharagpur.
- i) Organizing (principal coordinator) TEQIP sponsored short term course entitled "Cyber Security", 13-17 April, 2020 at the department of Mathematics, IIT kharagpur.
- j) Organized (principal coordinator) a short term course entitled "Fundamental Algorithms: Design and Analysis", February, 2017 at the department of Mathematics, IIT kharagpur.
- k) Organized (principal coordinator) a short term course entitled "A Short Term Course on Cryptography" from 18-24 May, 2014 at the department of Mathematics, IIT kharagpur.
- l) Subject expert for the MOOC on Algorithm course, NPTEL, IIT Madras.
- m) Faculty Adviser of Mathematics and Computing (MA-5Y), since 2011.
- n) Departmental time table and ERP co-in-charge, 2010-2014.
- o) Prof-in charge, Mathematics Colloquium, IIT kharagpur, 2012 - 2015.
- p) Departmental Examination Co in-charge, since 2014
- q) Member of Departmental Academic Committee (PG & R)
- r) Assistant Wardenship: LBS and MMM Hall of residence.
- s) Reviewed papers for ACISP, Asiacrypt, Crypto, Eurocrypt, FSE, Indocrypt, IEEE Transaction on Information Theory, ISC, SAC and many other conferences.
- t) Attended the induction course entitled "Training and Support for New Lecturer", Learning Innovation Unit, Dublin City University, Ireland.

10 Short Academic Visits

- a) Stratign FZE, Dubai, 18-23 November 2018.
- b) Stratign FZE, Dubai, 13-16 October 2018.
- c) Stratign FZE, Dubai, 12-14 September 2018.
- d) Engineering and Information Sciences, University of Wollongong, 7-9 July 2014.
- e) Department of Computer Science, University of York, UK, Oct 18-20, 2009.
- f) Electrical Engineering Department, Katholieke Universiteit Leuven, Leuven, Belgium, November 25, 2008.
- g) University College Cork, Ireland, May 19-20, 2008.
- h) Cryptography & Security Department, Institute for Infocomm Research, Singapore, July 14 to August 8, 2006.
- i) Laboratory of Algorithms, Security and Cryptology (LACS), University of Luxembourg, Luxembourg, May 9-11, 2006.
- j) Attended conferences: Acisp 2014, ACNS 2007, IEEE AMS 2007, IEEE WCNC 2007, SAC 2005, WISA 2005, Asiacrypt 2005, FSE 2004, Indocrypt 2004, Indocrypt 2000.

11 Publications (Journal/Conference/Book Chapter)

1. Jayaprakash Kar, Sourav Mukhopadhyay, Kshirasagar Naik, "SL-PPCP: Secure and Low-Cost Privacy-Preserving Communication Protocol for Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, doi: 10.1109/TVT.2024.3362152.
2. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Key-homomorphic and Revocable Ciphertext-Policy Attribute Based Key Encapsulation Mechanism for Multimedia Applications, Multimedia Tools and Applications, Springer, 2024.
3. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Hierarchical Identity-Based Inner Product Functional Encryption for Unbounded Hierarchical Depth. In the Proceeding of the 25th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2023), LNCS, Springer-Verlag, 2-4 October 2023, New Jersey, USA.

4. Amit Kumar Singh, Kamalesh Acharya, and Sourav Mukhopadhyay, Constructions of Broadcast Encryption with Personalized Messages from Bilinear Map, *Computer Communications*, 2023.
5. Amit Kumar Singh, Kamalesh Acharya, and Sourav Mukhopadhyay, Post-quantum Secure Recipient Revocable Broadcast Encryption Supporting Anonymity, *Multimedia Tools and Applications*, Springer 2023
6. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Short attribute-based signatures for arbitrary Turing machines from standard assumptions, *Designs, Codes and Cryptography*, Springer 2023.
7. Ramprasad Sarkar, Mriganka Mandal and Sourav Mukhopadhyay. "Quantum-Safe Identity-based Broadcast Encryption with Provable Security from Multivariate Cryptography", *Advances in Mathematics of Communications (AMC)*, Doi-<http://dx.doi.org/10.3934/amc.2022026>, American Institute of Mathematical Sciences, 2022.
8. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Communication-friendly Threshold Trapdoor Function from Weaker Assumption for Distributed Cryptography. *Annals of Telecommunications*, Springer 2022 (Accepted)
9. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Key Encapsulation Mechanism in Ciphertext-Policy Attribute Based Setting Featuring Revocation and Key-homomorphic Property. In the Proceeding of the 19th International Conference on Security and Cryptography (SECRYPT 2022), July 11-13, 2022 (Accepted).
10. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Hierarchical Identity Based Inner Product Functional Encryption for Privacy Preserving Statistical Analysis without q-type assumption, in the proceeding of the Third International Conference on Emerging Information Security and Applications (EISA 2022), Wuhan, China, Springer, October 29-30, 2022.
11. Subhranil Dutta, Ratna Dutta and Sourav Mukhopadhyay: Constructing Pairing Free Unbounded Inner Product Functional Encryption Schemes with Unbounded Inner Product Policy. In the Proceeding of the 15th International Conference on Security for Information Technology and Communications (SECITC 2022), LNCS, Springer-Verlag, 8-9 December, 2022 (Accepted).
12. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Trapdoor Function from Weaker Assumption in the Standard Model for Decentralized Network, in the proceeding of the 8th International Cryptology and Information Security Conference 2022 (CRYPTOLOGY2022), Port Dickson, Malaysia, July 26-28, 2022.
13. Ravi Anand, Arpita Mitra, Subhamoy Mitra, Chandra Sekhar Mukherjee, Sourav Mukhopadhyay. "Quantum Resource estimation for fsr based estimation symmetric ciphers & related grover's attacks", In the Proceeding of 22nd International Conference on Cryptology in India (Indocrypt 2021), LNCS, Springer-Verlag (to appear).
14. S. Rana, D. Mishra, S. Mukhopadhyay: "Blockchain-based multimedia content distribution with the assured system update mechanism", *Multimedia Tools and Applications* (Springer). (Accepted) (Impact Factor: 2.313)
15. M. Kansal, R. Dutta and S. Mukhopadhyay: 'Lattice based Nominative Signature using Pseudorandom Function' *IET Information Security*, (Accepted, 2021) (Impact Factor: .89).
16. Sarbani Roy and Sourav Mukhopadhyay: "(t, n) Threshold d-level QSS based on QFT". *Quantum Inf. Comput.* 20(11&12): 957-968 (2020) (Impact Factor: 1.563).
17. Ravi Anand, Arpita Maitra, Sourav Mukhopadhyay: "Grover on SIMON". *Quantum Inf. Process.* 19(9): 340 (2020) (Impact Factor: 2.433).
18. M. Kansal, R. Dutta, S. Mukhopadhyay: Group signature from lattices preserving forward security in dynamic setting. *Adv. Math. Commun.* 14(4): 535-553 (2020) (Impact Factor: 0.92)

19. S. Rana, M. S. Obaidat, D. Mishra, S. Mukhopadhyay and B. Sadoun, "Computational Efficient Authenticated Digital Content Distribution Frameworks for DRM Systems: Review and Outlook," in *IEEE Systems Journal*, 1-8, 2020, doi: 10.1109/JSYST.2020.2992650. Impact Factor: 3.987)
20. Sarbani Roy and Sourav Mukhopadhyay. "Device-independent quantum secret sharing in arbitrary even dimensions", *Phys. Rev. A, American Physical Society*, 100, 012319 (2019)
21. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Constrained Pseudorandom Functions for Turing Machines Revisited: How to Achieve Verifiability and Key Delegation". *Algorithmica* 81(9): 3245-3390 (2019)
22. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay. "Group Signature from Lattices preserving Forward Security in Dynamic setting", *Advances in Mathematics of Communications (AMC), American Institute of Mathematical Sciences*, (accepted) 2019
23. Jangirala Srinivas, Dheerendra Mishra, Sourav Mukhopadhyay, Saru Kumari, Vandana Guleria. "An Authentication Framework for Roaming Service in Global Mobility Networks". *ITC* 48(1): 129-145 (2019)
24. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Succinct Predicate and Online-Offline Multi-Input Inner Product Encryptions under Standard Static Assumptions". *Journal of Information Security and Applications*, ELSEVIER, Volume 48, 2019.
25. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay. " Construction for a Nominative Signature Scheme from Lattice with Enhanced Security". In the Proceeding of 3th International Conference on Codes, Cryptology And Information Security (C2SI), 2019, LNCS, Springer-Verlag.
26. Ravi Anand, Akhilesh Siddhanti, Subhamoy Maitra and Sourav Mukhopadhyay. "Differential Fault Attack on SIMON with very few Faults". In the Proceeding of 19th International Conference on Cryptology in India (Indocrypt 2018), LNCS, Springer-Verlag.
27. Sarbani Roy, Arpita Maitra, and Sourav Mukhopadhyay. "Measurement-device-independent quantum private query with qutrits", *International Journal of Quantum Information*, Vol. 16, No. 4 (2018) 1850045 (16 pages), World Scientific Publishing Company.
28. Jangirala Srinivas, Dheerendra Mishra, Sourav Mukhopadhyay, Saru Kumari. "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks". *J. Ambient Intelligence and Humanized Computing* 9(4): 875-895 (2018).
29. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Functional Signcryption". *Journal of Information Security and Applications*, ELSEVIER, Volume 42, October 2018, Pages 118-134..
30. Ankita Chaturvedi, Dheerendra Mishra, Jangirala Srinivas and Sourav Mukhopadhyay. " A privacy preserving biometric-based three-factor remote user authenticated key agreement scheme", in *Journal of Information Security and Applications (Elsevier)*, Accepted, 2017.
31. Jangirala Srinivas, Sourav Mukhopadhyay, and Ashok Kumar Das. "A Multi-Server Environment with Secure and Efficient Remote User Authentication Scheme based on Dynamic ID using Smart Cards," in *Wireless Personal Communications (Springer)*, 2017, Accepted. (2015 SCI Impact Factor: 0.701)

32. Jangirala Srinivas, Sourav Mukhopadhyay, Dheerendra Mishra. "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," in *Journal of Ad Hoc Networks* 54: 147-169 (2017) (Citation Index: SCIE, Impact Factor: 1.456).
33. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Constrained Pseudorandom Functions for Unconstrained Inputs Revisited: Achieving Verifiability and Key Delegation". In the Proceeding of 20th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2017), LNCS, Springer-Verlag.
34. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Strongly Full-Hiding Inner Product Encryption". Theoretical Computer Science (TCS) Journal, ELSEVIER, 2017.
35. Dheerendra Mishra, Ashok Kumar Das, Sourav Mukhopadhyay, and Mohammad Wazid. "A Secure and Robust Smartcard-Based Authentication Scheme for Session Initiation Protocol Using Elliptic Curve Cryptography," in *Wireless Personal Communications* (Springer), Vol. 91, No. 3, pp.1361-1391, 2016, DOI: 10.1007/s11277-016-3533-0. (2015 SCI Impact Factor: 0.701)
36. Ankita Chaturvedi, Ashok Kumar Das, Dheerendra Mishra, and Sourav Mukhopadhyay. "Design of a secure smartcard-based multi-server authentication scheme," in *Journal of Information Security and Applications* (Elsevier), Vol. 30, pp. 64-80, 2016. [Indexed in Emerging Sources Citation Index (ESCI), Thomson Reuters]
37. Dheerendra Mishra, Ashok Kumar Das, and Sourav Mukhopadhyay. "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card," in *Peer-to-Peer Networking and Applications* (Springer), Vol. 9, No. 1, pp.171-192, 2016. (2015 SCI Impact Factor: 1.000)
38. Ashok Kumar Das, Dheerendra Mishra, and Sourav Mukhopadhyay. "An anonymous and secure biometric-based enterprise digital rights management system for mobile environment," in *Security and Communication Networks* (Wiley), Vol. 8, No. 18, pp. 3383-3404, 2015, DOI: 10.1002/sec.1266. (2015 SCI Impact Factor: 0.806)
39. Srinivas Jangirala, Dheerendra Mishra, Sourav Mukhopadhyay. "Secure Lightweight User Authentication and Key Agreement Scheme for Wireless Sensor Networks Tailored for the Internet of Things Environment". *ICISS 2016*: 45-65
40. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Adaptively Secure Unrestricted Attribute-Based Encryption with Subset Difference Revocation in Bilinear Groups of Prime Order", In the Proceeding of 8th International Conference on Cryptology, AFRICACRYPT 2016, LNCS, Springer-Verlag
41. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Functional Encryption for Inner Product with Full Function Privacy", In the Proceeding of 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016), LNCS, Springer-Verlag.
42. Dheerendra Mishra, Ashok Kumar Das, Ankita Chaturvedi, and Sourav Mukhopadhyay. "A secure password-based authentication and key agreement scheme using smart cards," in *Journal of*

- Information Security and Applications (Elsevier), Vol. 23, pp. 28-43, August 2015, DOI: 10.1016/j.jisa.2015.06.003. [Indexed in Emerging Sources Citation Index (ESCI), Thomson Reuters]
43. Dheerendra Mishra, Ankita Chaturvedi, and Sourav Mukhopadhyay, "An Improved Biometric-based Remote User Authentication Scheme for Connected Health Care", in *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, **Inderscience**, 18(1/2): 75-84, 2015.
 44. Dheerendra Mishra, Ankita Chaturvedi, and Sourav Mukhopadhyay, "Design of a Lightweight Two-factor Authentication Scheme with Smart Card Revocation," in *Journal of Information Security and Applications (Elsevier)*, Vol. 23, pp. 44-51, August 2015, DOI: 10.1016/j.jisa.2015.06.003. [Indexed in Emerging Sources Citation Index (ESCI), Thomson Reuters]
 45. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "General Circuit Realizing Compact Attribute-Based Encryption and Signcryption from Multilinear Maps", In the Proceeding of 16th International Conference on Cryptology (Indocrypt 2015), **LNCS**, Springer-Verlag.
 46. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Functional Signcryption: Notion, Construction, and Applications", In the Proceeding of Seventh International Conference on Provable Security (ProvSec 2015) **LNCS**, Springer-Verlag.
 47. Dibyendu Roy, Ankita Chaturvedi and Sourav Mukhopadhyay. "New Constructions of T-function", In the Proceeding of the 11th Information Security Practice and Experience Conference (ISPEC 2015), **LNCS**, Springer-Verlag, 2015.
 48. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps", In the Proceeding of the 18th Information Security Conference (ISC 2015), **LNCS**, Springer-Verlag, 2015.
 49. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Fully Secure Online/Offline Predicate and Attribute-Based Encryption", In the Proceeding of the 11th Information Security Practice and Experience Conference (ISPEC 2015), **LNCS**, Springer-Verlag, 2015.
 50. Ankita Chaturvedi, Dheerendra Mishra, and Sourav Mukhopadhyay, "An Enhanced Dynamic ID-Based Authentication Scheme for Telecare Medical Information Systems", in *Journal of King Saud University - Computer and Information Sciences*, **ELSEVIER**, 2014 (Accepted).
 51. Dibyendu Roy, Pratish Datta, and Sourav Mukhopadhyay, "Algebraic Cryptanalysis of Stream Ciphers Using Decomposition of Boolean Function", in *Journal of Applied Mathematics and Computing*, **Springer**, 2014.
 52. Dheerendra Mishra, Jangirala Srinivas, and Sourav Mukhopadhyay, "A Secure and Efficient Chaotic Map-based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems", in *Journal of Medical Systems*, **Springer**. (Citation Index: SCIE, Impact Factor: 1.783).
 53. Dheerendra Mishra, Ashok Kumar Das, and Sourav Mukhopadhyay, "A Secure User Anonymity-Preserving Biometric-Based Multi-Server Authenticated Key Agreement Scheme using Smart Cards", in *International Journal of Expert Systems with Applications*, **ELSEVIER**. (Citation Index: SCIE, Impact Factor: 1.854)

54. Dheerendra Mishra, and Sourav Mukhopadhyay, "A Privacy Enabling Content Distribution Framework for Digital Rights Management", in *International Journal of trust management in computing and communications* (Accepted).
55. Dheerendra Mishra, Sourav Mukhopadhyay, Saru Kumari, Muhammad Khurram Khan, and Ankita Chaturvedi, "Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce", in *Journal of Medical Systems*, 38 (5) pp. 1-11, 2014. doi: <http://dx.doi.org/10.1007/s10916-014-0041-1>. (Citation Index: SCIE, Impact Factor: 1.783).
56. Dheerendra Mishra, Ankita Chaturvedi, Sourav Mukhopadhyay, Saru Kumari, and Muhammad Khurram Khan, "Cryptanalysis and Improvement of Yan et al.'s Biometric-based Authentication Scheme for Telecare Medicine Information Systems", in *Journal of Medical Systems* (Accepted). (Citation Index: SCIE, Impact Factor: 1.783).
57. Sarbari Mitra, Sourav Mukhopadhyay, and Ratna Dutta, "Key Pre-Distribution in a Non-Uniform Rectangular Grid for Wireless Sensor Networks". in *Journal of Applied Mathematics and Computing*, Springer, 2014.
58. Pratish Datta, Dibyendu Roy and Sourav Mukhopadhyay. "A Probabilistic Algebraic Attack on the Grain Family of Stream Ciphers". In the Proceeding of the 7th International Conference on Network and System Security (NSS 2014), LNCS, Springer-Verlag, 2014.
59. Dheerendra Mishra and Sourav Mukhopadhyay. "Cryptanalysis of Two Authentication Scheme for DRM System". In the Proceeding of the 2nd International Conference on Security in Computer Networks and Distributed Systems (SNDS-2014), Springer (CCIS), ISSN: 1865:0929, 2014.
60. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Fully Secure Self-Updatable Encryption in Prime Order Bilinear Groups", In the Proceeding of Information Security, the Seventeenth International Conference (ISC 2014), LNCS, Springer-Verlag, 2014.
61. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay. "Universally Composable Efficient Priced Oblivious Transfer from a Flexible Membership Encryption", In the Proceeding of 19th Australasian Conference on Information Security and Privacy (ACISP 2014), LNCS, Springer-Verlag, 2014.
62. Dheerendra Mishra and Sourav Mukhopadhyay. "Cryptanalysis of Yang et al.'s Digital Rights Management Authentication Scheme Based on Smart Card". In the Proceeding of the 2nd International Conference on Security in Computer Networks and Distributed Systems (SNDS-2014), Springer (CCIS), ISSN: 1865:0929, 2014.
63. Dibyendu Roy, Pratish Datta and Sourav Mukhopadhyay. "A New Variant of Algebraic Attack". In the Proceeding of the 2nd International Conference on Security in Computer Networks and Distributed Systems (SNDS-2014), Springer (CCIS), ISSN: 1865:0929, 2014.
64. Sarbari Mitra, Sourav Mukhopadhyay, and Ratna Dutta, "A Deterministic Key Pre-distribution Scheme for WSN Using Projective Planes and Their Complements". in *International Journal of Trust Management in Computing and Communications (IJTMCC)*, 2013 (Citation Index: SCI).

65. Sarbari Mitra, Sourav Mukhopadhyay, and Ratna Dutta, "Unconditionally-Secure Key Pre-Distribution for Triangular Grid Based Wireless Sensor Network". in *Journal of Applied Mathematics and Computing*, Springer, 2013.
66. Ankita Chaturvedi, Dheerendra Mishra and Sourav Mukhopadhyay. "Improved Biometric-based Three-factor Remote User Authentication Scheme with Key Agreement using Smart Card", In the Proceeding of the 9th International Conference on Information Systems Security (ICISS 2013), LNCS, Springer-Verlag, 2013.
67. Dheerendra Mishra and Sourav Mukhopadhyay. "Cryptanalysis of Pairing-free Identity-Based Authenticated Key Agreement Protocols", In the Proceeding of the 9th International Conference on Information Systems Security (ICISS 13), LNCS, Springer-Verlag, 2013.
68. Dheerendra Mishra, Vinod Kumar and Sourav Mukhopadhyay. "A Pairing-free Identity Based Authentication Framework for Cloud Computing", In the Proceeding of the 7th International Conference on Network and System Security (NSS 2013), LNCS, Springer-Verlag, 2013.
69. Dheerendra Mishra and Sourav Mukhopadhyay. "Privacy Preserving Mechanism in Multi-Distributor based DRM System", In the Proceeding of the 9th Information Security Practice and Experience Conference (ISPEC 2013), LNCS, Springer-Verlag, 2013.
70. Sarbari Mitra and Sourav Mukhopadhyay." Key Pre-Distribution in a Non-Uniform Network Using Combinatorial Design", In the Proceeding of 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (Qshine 2013), LNICST (Springer Lecture Notes of ICST). 2013.
71. Dheerendra Mishra and Sourav Mukhopadhyay."A Certificateless Authenticated Key Agreement Protocol for Digital Rights Management System", In the Proceeding of 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (Qshine 2013), LNICST (Springer Lecture Notes of ICST). 2013.
72. Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta."Unconditionally Secure Fully Connected Key Establishment using Deployment Knowledge", In the Proceeding of AsiaARES 2013, LNCS, Springer-Verlag, 2013.
73. Sarbari Mitra, Sourav Mukhopadhyay, and Ratna Dutta. "A Group-Based Deterministic Key Predistribution Scheme for Wireless Sensor Network", in *International Journal of Wireless and Mobile Computing (IJWMC)*, Special Issue on u- and e-Service, Science and Technology, 2012 (Citation Index: SCI).
74. Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta. "Flexible Deterministic Approach to Key Pre-Distribution in Grid Based WSN", In Proceeding of ADHOCNETS 2012, LNICST (Springer Lecture Notes of ICST). 2012.
75. Dheerendra Mishra and Sourav Mukhopadhyay. "Towards a Secure, Transparent and Privacy-Preserving DRM System", In Proceeding of the International Conference on Security in Computer Networks and Distributed Systems (SNDS-2012), Springer. 2012.

76. Dheerendra Mishra and Sourav Mukhopadhyay. "Privacy Rights Management in Multiparty Multilevel DRM System", In Proceeding of the International Conference on Advances in Computing, Communications and Informatics (ICACCI-2012), ACM digital library. 2012.
77. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Adaptive Routing Strategy for Large Scale Rearrangeable Symmetric Networks", *Evolving Developments in Grid and Cloud Computing: Advancing Research*. Book Chapter, P. 212-222, Chapter15, ISBN13: 9781466600560, 2012. IGI Global
78. Sarbari Mitra, Ratna Dutta and Sourav Mukhopadhyay. "A Hierarchical Deterministic Key Predistribution for WSN Using Projective Planes", In Proceeding of ADHOCNETS 2011, LNICST (Springer Lecture Notes of ICST). 2011.
79. Ratna Dutta, Sourav Mukhopadhyay and Dheerendra Mishra. "Access Policy Based Key Management in Multi-Level Multi-Distributor DRM Architecture", In Proceeding of InfoSecHiComNet 2011, LNCS, Springer-Verlag, 2011.
80. Sarbari Mitra, Ratna Dutta and Sourav Mukhopadhyay. "Towards a Deterministic Hierarchical Key Predistribution for WSN Using Complementary Fano Plane", In Proceeding of SecureComm 2011, LNICST (Springer Lecture Notes of ICST). 2011.
81. Ratna Dutta, Dheerendra Mishra and Sourav Mukhopadhyay. "Vector Space Access Structure and ID based Distributed DRM Key Management", In proceedings of ID2011, LNCS, Springer-Verlag, 2011.
82. Ratna Dutta, Sourav Mukhopadhyay, and Martin Collier. "Computationally secure self-healing key distribution with revocation in wireless ad hoc networks", in *Journal of Ad Hoc Networks* 8(6): 597-613 (Citation Index: SCIE, Impact Factor: 1.456).
83. Amitabha Chakrabarty, Martin Collier, and Sourav Mukhopadhyay. "Adaptive Routing Strategy for Large Scale Rearrangeable Symmetric Networks". in *International Journal of Grid and High Performance Computing (IJGHPC)*, 2(2): 53-63.
84. Sourav Mukhopadhyay and Palash Sarkar. "Hardware Architecture and Cost/time/data Trade-off for Generic Inversion of One-way Function". in *Journal of Computacion y Sistemas*, ISSN 1405-5546, Special Issue on Applied Cryptography & Data Security, pp 331-355, Volume 12, No. 3, 2009.
85. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Symmetric Rearrangeable Networks: Algorithms and Rearrangement Limits", In Proceedings of the 7th International Conference on Information Technology - New Generations (ITNG), April 12-14, 2010, Las Vegas, Nevada, USA.
86. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Matrix Based Nonblocking Routing Algorithm for Bene's Networks". Proceeding of the International Conference on Future Computational Technologies and Applications (FUTURE COMPUTING 2009). IEEE Computer Society Press. Athens, Greece, November 15-20, 2009.
87. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Dynamic Path Selection Algorithm for Bene's Network". Proceeding of the IEEE International conference on Computational Intelligence, Communication Systems and Networks (CICSyN2009). IEEE Computer Society Press, 2009.

88. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Generalized Self-Healing Key Distribution in Wireless Ad hoc Networks with Trade-Offs in User's Pre-Arranged Life Cycle and Collusion Resistance". Proceeding of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2009). ACM Press. Canary Islands, Spain, 26-30 October, 2009.
89. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Enhanced Access Polynomial Based Self-Healing Key Distribution". Proceeding of the ICST International Workshop on Security in Emerging Wireless Communication and Networking Systems (SEWCN09). LNICST (Springer Lecture Notes of ICST). Athens, Greece, September 14, 2009.
90. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Key Management in Multi-Distributor based DRM System with Mobile Clients using IBE". Proceeding of the IEEE International conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009). IEEE Computer Society Press. London, UK, August 4-6, 2009.
91. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Trade-Off between Collusion Resistance and User Life Cycle in Self-Healing Key Distributions with t-Revocation". Proceeding of the IEEE International conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009). IEEE Computer Society Press. London, UK, August 4-6, 2009.
92. Ratna Dutta, Sourav Mukhopadhyay and Sabu Emmanuel. "Low Bandwidth Self-Healing Key Distribution in Wireless Ad Hoc Network". Proceeding of the IEEE Asia International Conference on Modelling and Simulation (AMS 2008), IEEE Computer Society Press, Kuala Lumpur, Malaysia 13-15 May, 2008.
93. Ratna Dutta, Sourav Mukhopadhyay, Amitabha Das and Sabu Emmanuel. "Generalized Self-Healing Key Distribution using Vector Space Access Structure". Proceedings of IFIP Networking 2008, LNCS 4982, pp. 612-623, Springer-Verlag, 2008.
94. Ratna Dutta and Sourav Mukhopadhyay. "Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network". Proceeding of the IEEE Wireless Communications and Networking Conference (WCNC 2007), Hong Kong, 2007.
95. Ratna Dutta, Sourav Mukhopadhyay and Yong Dong Wu. "Constant Storage Self-Healing Key Distribution with Revocation in Wireless Sensor Network". Proceeding of the IEEE International Conference on Communications (ICC 2007), Glasgow, 2007.
96. Ratna Dutta, Chang Ee-Chien and Sourav Mukhopadhyay. "Efficient Self-Healing Key Distributions with Revocation for Wireless Network using One Way Key Chains". Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS 2007), LNCS 4521, pp. 385-400, Springer-Verlag, 2007.
97. Ratna Dutta and Sourav Mukhopadhyay. "Designing Scalable Self-Healing Key Distribution Schemes with Revocation Capability". Proceedings of the 5th International Symposium on Parallel and Distributed Processing and Applications (ISPA-07), LNCS 4742, pp. 419-430, Springer-Verlag, 2007.

98. Sourav Mukhopadhyay and Palash Sarkar. "Hardware Architecture and Trade-offs for Generic Inversion of One-way Functions". IEEE International Symposium on Circuits and Systems (ISCAS 2006), Greece, 2006.
99. Sourav Mukhopadhyay and Palash Sarkar. "Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms". Proceedings of Applied Cryptography and Information Security 2006 (ACIS 2006) in conjunction with ICCSA 2006, LNCS 3982, pp. 426-435, Springer Verlag, 2006.
100. Sourav Mukhopadhyay and Palash Sarkar. "On the Effectiveness of TMTO and Exhaustive Search Attacks". Proceedings of the 1st International Workshop on Security (IWSEC2006), LNCS 4266, pp. 337-352, Springer Verlag, 2006.
101. Alex Biryukov, Sourav Mukhopadhyay and Palash Sarkar. "Improved Time-Memory Trade-offs with Multiple Data". Proceedings of Selected Areas in Cryptography (SAC 2005), LNCS 3897, pp. 110-127, Springer Verlag, 2005.
102. Sourav Mukhopadhyay and Palash Sarkar. "Application of LFSRs in Time/Memory Trade-Off Cryptanalysis". Proceedings of Workshop on Information Security Applications (WISA 2005), LNCS 3786, pp. 25-37, Springer Verlag, 2005.
103. Bimal Roy and Sourav Mukhopadhyay. "Statistical Cryptanalysis on Block Cipher". in *Journal of the Indian Society for Probability and Statistics*, Vol. 7, 2003.
104. Sourav Mukhopadhyay. "Time/Memory Trade-Off: A Survey". in *Journal of the Indian Statistical Association (JISA)*, Special Issue on Statistics in Cryptology, Volume 42, No. 2, ISSN 0537-2585, 2004.