Dr. Sourav Mukhopadhyay

Present Address:

Department of Mathematics
Indian Institute of Technology
Kharagpur- 721 302, INDIA
Tel: +91 3222 282858 (O), +91-3222-283645 (R)
Email: sourav@maths.iitkgp.ernet.in, msourav@gmail.com

Present Position:

Associate Professor
Department of Mathematics
Indian Institute of Technology, Kharagpur- 721302, India.

Date of Birth : 21/01/1975

Sex (M/F): M

Education (Post-Graduation onwards & Professional Career)

Sl No.	Institution Place	Degree Awarded	Year	Field of Study
1	Indian Statistical Institute, Kolkata	Doctoral	2007	Cryptanalysis on Symmetric Cipher
2	Indian Statistical Institute, Kolkata	M.Tech	2001	Computer Science
3	Indian Statistical Institute, Delhi and Kolkata.	M.Stat	1999	Statistics
4	Ramakrishna Mission Vidymandira, University of Calcutta.	B.Sc	1997	Mathematics

A. Position and Honors

<u>Position and Employment</u> (Starting with the most recent employment)

Sl No.	Institution Place	Position	From (Date)	To (date)
1	Indian Institute of Technology, Kharagpur	Associate Professor	Oct 2014	Till Date
2	Indian Institute of Technology, Kharagpur	Assistant Professor	01/12/09	01/09/14
3	School of Electronic Engineering, Dublin CityUniversity, Ireland.	Lecturer	Feb 2009	June 2009
4	School of Electronic Engineering, Dublin CityUniversity, Ireland.	Postdoctoral Research Fellow	01/02/08	01/12/09

5	School of Computer Engineering, Nanyang Technological University, Singapore	Postdoctoral Research Fellow	01/09/07	01/02/08
6	School of Computing, Department of Computer Science, National University of Singapore,Singapore.	Research Assistant	Sep 2006	Sep 2007
7	Institute for Infocomm Research (I2R), Singapore	Visiting Scientist	01/06/06	01/08/06
8	INRIA Rocquencourt, project CODES, INRIA, France.	Visiting Scientist	01/04/06	June 2006
9	Applied Statistics Unit, Indian Statistical Institute, Kolkata.	Project Linked Researcher	Feb 2003	01/03/06
10	School of Computing, Department of Computer Science, National University of Singapore, Singapore	Research Assistant	Feb 2002	Dec 2002
11	Machine Intelligent Unit, Indian Statistical Institute, Kolkata	Junior Research Fellow	July 2001	Jan 2002

Honors/Awards

1. Assistant Professorship, Department of Mathematics, Indian Institute of Technology, Kharagpur, India, December 2009 -September 2014.
2. Offered professorship at Institute of Informatics, Istanbul Technical University for the Cybersecurity Engineering and Cryptography program, Turkey, 2014.
3. Offered Assistant Professorship, from the following places:
   -- CR Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS), India, 2009.
   -- Department of Computer Science at the Indian Institute of Technology, Ropar (Punjab), India, 2009
4. Offered Scientist C post from Defence Research & Development Organization (DRDO), New Delhi, India, 2008.
5. Postdoctoral Research Fellow, School of Electronic Engineering, Dublin City University, Dublin 9, Ireland, February 2008- December 2009.
6. Postdoctoral Research Fellow, School of Computer Engineering, Nanyang Technological University, Singapore, September 2007- February 2008.
7. Offered postdoctoral Research position from the following places:

-- Center for Information Security Technologies (CIST), Korea University, Seoul, Korea, 2007.
-- Department of Computer Science and Communication Engineering, Kyushu University, Fukuoka, Japan, 2006.

8. Offered Scientist C post from National Technical Research Organization (NTRO), Govt. of India, New Delhi, 2007.
9. Visiting Scientist Position, INRIA-Rocquencourt, project CODES, France, April 2006- June 2006.
10. Project Linked Research Assistant, Cryptology Research Group, Applied Statistics Unit, Indian Statistical Institute, February 2003- March 2006.
11. Research Assistant, School of Computing, National University of Singapore, February 2002{December 2002 and September 2006- September 2007.
12. ISI-INSEAD fellowship, France INSEAD and Indian Statistical Institute joint fellowship, 2001.
13. Junior Research Fellowship, Indian Statistical Institute, July 2001- January2002.
14. Offered the position of Member of Technical Staff, Sun Microsystems (India), 2001.
15. Offered Design Engineer position, Texas Instruments (India), 2001.
16. Ranked 5th in M.Tech, Indian Statistical Institute, 2001.
17. Ranked 4th in M.Stat, Indian Statistical Institute, 1999.
18. Ranked 5th in B.Sc., University of Calcutta, 1997.

Research Interests

1. Algebraic Cryptanalysis on Symmetric Cipher.
2. Cloud Computing
3. Digital Rights Managements
4. Key pre-distribution for Wireless Sensor Networks
1. Time/Memory Trade-off Cryptanalysis

Teaching Experience

1. Indian Institute of Technology, Kharagpur:

- MA20106: PROBABILITY & STOCHASTIC PROCESSES, JAN – APRIL, 2012, 2013, 2014, **2015** (SUBJECT CO-ORDINATOR).
- MA21005/MA21007: DESIGN & ANALYSIS OF ALGORITHMS, JULY – DEC, 2013, 2014.
- MA31009: COMPUTER ORGANISATION & ARCHITECTURE, JULY – DEC, 2014**.**
- MA20104: PROBABILITY AND STATISTICS, JAN – APRIL, 2010, 2011.
- MA32006: REGRESSION ANALYSIS, JAN – APRIL, 2010, 2011.
- MA30006/ MA61002: SWITCHING & FINITE AUTOMATA THEORY, JAN – APRIL, 2012, 2013.
- MA31020: REGRESSION AND TIME SERIES MODEL, JULY – DEC, 2011.
- MA41009: PROBABILITY AND STATISTICS, JULY – DEC, 2010, 2011, 2012.
- MA41021/MA60001: PROGRAMMING LANGUAGES, JULY – DEC, 2010.

- MA60031/MA51115: CRYPTOGRAPHY AND NETWORK SECURITY, JULY –DEC, 2011, 2012, 2013.
- MA29005: DESIGN & ANALYSIS OF ALGORITHMS LAB, JULY – DEC, 2011, 2012, 2013.
- MA49010/MA53027: STATISTICAL SOFTWARE LABORATORY, JULY – DEC, 2010, 2014.
- MA69004: DATA STRUCTURE AND ALGORITHM LABORATORY, JAN – APRIL, 2014, **2015**.
- MA10001: MATH-I (Summer quarter 2014)
- MA10002: MATH – II (Summer quarter 2014)

2. Dublin City University, Ireland:

- EE548: Internetwork Security, FEB – JUN, 2009.

Doctoral Guidance:

Completed: 1

Ongoing: 3 Research scholars, 1 Project scholars.

Master's and Bachelor's Thesis Guidance:

Completed: 4 M.Tech. Students, 32 M.Sc Student

Ongoing: 6 M.Sc. Student, 4 M.Tech. Students

Post-Doctoral Guidance:

Ongoing: 1

Reviewed Papers Published/ Accepted:

Journal: 21; Conference: 45.

Sponsored Projects/ Consultancies:

Completed: 1; In Progress: 3.

Professional Activities:

1. Significant advisory role in supervising 1 PhD thesis at Indian Institute of Technology, Kharagpur, 2014.
2. Taught a 7.5 credit full Cryptology course (EE548: Internetwork Security) at Master's (5th) level with strength 118 at Dublin City University, Feb – June, 2009.
3. Reviewed papers for ACISP, Asiacrypt, Crypto, Eurocrypt, FSE, Indocrypt, IEEE Transaction on Information Theory, ISC, SAC and many other conferences.
4. Attended the induction course entitled \Training and Support for New Lecturer", Learning Innovation Unit, Dublin City University, Ireland.
5. Supervised thesis of 3 Masters' students at Dublin City University in 2008.
6. Supervised thesis of 1 MCA student and 1 B.Tech student at Indian Statistical Institute in 2005.

B. List of Publications:

Book Chapter:

1. 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

Journal:

1 Dheerendra Mishra, Ashok Kumar Das, and Sourav Mukhopadhyay , “An anonymous and secure biometric-based enterprise digital rights management system for mobile environment”, *Security and Communication Networks*, Wiley (Accepted), 2015.

2 Dheerendra Mishra, Ashok Kumar Das, and Sourav Mukhopadhyay. "A secure password-based authentication and key agreement scheme using smart cards," in *Journal of Information Security and Applications*, **Elsevier**, 2015, In Press.

3 Dheerendra Mishra, Ankita Chaturvedi, and Sourav Mukhopadhyay, "Design of a Lightweight Two-factor Authentication Scheme with Smart Card Revocation", *Journal of Information Security and Applications*, **ELSEVIER** (Accepted), 2015.

4 Dheerendra Mishra, Ankita Chaturvedi, Sourav Mukhopadhyay, “An improved biometric-based remote user authentication scheme for connected healthcare”. *International **Journal** of Ad Hoc and Ubiquitous Computing*, 18(1/2): 75-84, Inderscience, 2015.

5 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).

6 Dheerendra Mishra, Ashok Kumar Das, and Sourav Mukhopadhyay , “A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card”. *Peer-to-Peer Networking and Applications*, Springer, **In Press,** 2014
DOI 10.1007/s12083-014-0321-z

7 Dibyendu Roy, Pratish Datta and Sourav Mukhopadhyay, “Algebraic Cryptanalysis of Stream Ciphers Using Decomposition of Boolean Function”, ***Journal** of Applied Mathematics and Computing, Springer*, (Accepted), 2014.

8 Dheerendra Mishra, Jangirala Srinivas and Sourav Mukhopadhyay, “A Secure and Efficient Chaotic Map-based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems", ***Journal** of Medical Systems* 38(10)*: 120, Springer, 2014. Springer*.
(Citation Index: SCIE, Impact Factor: 1.783)

9 Dheerendra Mishra, Ashok Kumar Das and Sourav Mukhopadhyay, “A Secure User Anonymity-Preserving Biometric-Based Multi-Server Authenticated Key Agreement Scheme using Smart Cards", *International **Journal** of Expert Systems with Applications*, 41(18)*: 8129-8143, Elsevier, 2014.*
(Citation Index: SCIE, Impact Factor: 1.854)

10 Dheerendra Mishra and Sourav Mukhopadhyay, “A Privacy Enabling Content Distribution Framework for Digital Rights Management", *International **Journal** of Trust Management in Computing and Communications*, 2(1):22-39, Inderscience, 2014.
11 Dheerendra Mishra, Sourav Mukhopadhyay, Ankita Chaturvedi, Saru Kumari and Muhammad Khurram Khan. "Security Enhancement of a Biometric based Authentication Scheme for Telecare Medicine Information Systems with Nonce”, ***Journal** of Medical Systems*, 38 (5):1-11, Springer, 2014.
DOI: http://dx.doi.org/10.1007/s10916-014-0041-1.
(Citation Index: SCIE, Impact Factor: 1.783)
12 Dheerendra Mishra, Sourav Mukhopadhyay, Ankita Chaturvedi, Saru Kumari and Muhammad Khurram Khan. "Cryptanalysis and Improvement of Yan et al.'s Biometric-based Authentication Scheme for Telecare Medicine Information Systems”, ***Journal** of Medical Systems*, 38(6): 24, Springer, 2014.
(Citation Index: SCIE, Impact Factor: 1.783)
13 Sarbari Mitra, Sourav Mukhopadhyay, Ratna Dutta, A Deterministic Key Pre-distribution Scheme for WSN Using Projective Planes and Their Complements. In the *International **Journal** of Trust Management in Computing and Communications*, 2(2):150-184, Inderscience, 2014.
14 Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta, “Key Pre-Distribution in a Non-Uniform Rectangular Grid for Wireless Sensor Networks”. ***Journal** of Applied Mathematics and Computing*, 45(1-2): 63-85, *Springer*, 2014.
15 Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta, “Unconditionally-Secure Key Pre-Distribution for Triangular Grid Based Wireless Sensor Network”. ***Journal** of Applied Mathematics and Computing*, 44(1-2):229–249, Springer, 2014.
16 Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta. “A Group-Based Deterministic Key Predistribution Scheme for Wireless Sensor Network”, *In the International **Journal** of Wireless and Mobile Computing (IJWMC),* Special Issue on u- and e-Service, 7(5): 435-447, Inderscience, 2014.
17 Ratna Dutta, Sourav Mukhopadhyay and Martin Collier. “Computationally secure self-healing key distribution with revocation in wireless ad hoc networks”, ***Journal** of Ad Hoc Networks* 8(6): 597-613, *Elsevier,* 2010.
18 Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. “Adaptive Routing Strategy for Large Scale Rearrangeable Symmetric Networks”. *International **Journal** of Grid and High Performance Computing (IJGHPC),* 2(2): 53-63, 2010.
19 Sourav Mukhopadhyay and Palash Sarkar. "Hardware Architecture and Cost/time/data Trade-off for Generic Inversion of One-way Function". ***Journal** of Computacion y Sistemas*, ISSN 1405-5546, Special Issue on Applied Cryptography & Data Security, 12(3): 331-355, 2009.
20 Bimal Roy and Sourav Mukhopadhyay. "Statistical Cryptanalysis on Block Cipher". in *Journal of the Indian Society for Probability and Statistics*, Vol. 7, 2003.

21 Sourav Mukhopadhyay. "Time/Memory Trade-Off: A Survey". ***Journal*** *of the Indian Statistical Association (JISA)*, Special Issue on Statistics in Cryptology, 42(2), ISSN 0537-2585, 2004.

Conference:

1. 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** 9646, pp. 325-345, Springer-Verlag, Morocco, 2016.
2. 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** 9614, pp. 164-195, Springer-Verlag, Taipei, Taiwan, 2016.
3. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Compact Attribute-Based Encryption and Signcryption for General Circuits from Multilinear Maps. In the Proceeding of 16th International Conference on Cryptology (Indocrypt 2015), **LNCS** 9462, pp. 3-24, Springer-Verlag, Bengaluru, India, 2015.
4. 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** 9451, pp. 268-288, Springer-Verlag, Kanazawa, Japan, 2015.
5. 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 , *September 9-11, 2015*.
6. 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** 9065, Springer-Verlag, Beijing, China, May 5-8, 2015.
7. Dibyendu Roy and Sourav Mukhopadhyay. "Fault Analysis on the Stream Ciphers LILI-128 and Achterbahn". In the Proceeding of the 11th Information Security Practice and Experience Conference (ISPEC 2015), **LNCS** 9065, Springer-Verlag, Beijing, China, May 5-8, 2015.
8. 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** 8792, pp. 558-565, Springer-Verlag, 2014.
9. 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** 8783, pp 1-18, Springer-Verlag, 2014.
10. 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** 8544, pp 98-114, Springer-Verlag, 2014.

11. 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), CCIS 420, pp 184-191, Springer-Verlag, ISSN: 1865:0929, 2014.
12. 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), CCIS 420, pp 288-297, Springer-Verlag, ISSN: 1865:0929, 2014.
13. 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), CCIS 420, pp 211-222, Springer-Verlag, ISSN: 1865:0929, 2014.
14. 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** 8303, pp 63-77 Springer-Verlag, 2013.
15. 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 2013), **LNCS** 8303, pp 247-254, Springer-Verlag, 2013.
16. 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** 7873, pp 721-727, Springer-Verlag, 2013.
17. 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** 7863, pp 321-335 Springer-Verlag, 2013.
18. 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) 115, pp 155-170, 2013.
19. 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) 115, pp 568-577, 2013.
20. Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta.“Unconditionally Secure Fully Connected Key Establishment using Deployment Knowledge”. In the Proceeding of ICT-EurAsia 2013 , **LNCS** 7804, pp 496-501, Springer-Verlag, 2013.
21. 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), 111, pp 164-179 2013.
22. 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), CCIS 335, 2012, pp 304-313, Springer-Verlag, 2012.
23. 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), pp. 625-631, ACM digital library, 2012.
24. 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), 89, pp 16-31 2012.
25. 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** 7011, pp 57-71 Springer-Verlag, 2011.
26. 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), 96, pp 373-388 2012.
27. Ratna Dutta, Dheerendra Mishra and Sourav Mukhopadhyay**.** “Vector Space Access Structure and ID based Distributed DRM Key Management”. In proceedings of ACC 2011, **LNCS** 193, pp 223-232 Springer-Verlag, 2011.
28. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. “Symmetric Rearrangeable Networks: Algorithms and Rearrangement Limits”, ITNG 2010, pp. 1274-1277, IEEE Computer Society Press, 2010.
29. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Matrix Based Nonblocking Routing Algorithm for Bene's Networks". In Proceeding of the International Conference on Future Computational Technologies and Applications (FUTURE COMPUTING 2009), pp. 551-556, IEEE Computer Society Press, Athens, Greece, November 15-20, 2009.
30. Amitabha Chakrabarty, Martin Collier and Sourav Mukhopadhyay. "Dynamic Path Selection Algorithm for Beneˇs Network". In Proceeding of the IEEE International conference on Computational Intelligence, Communication Systems and Networks (CICSyN2009), pp: 23-28, IEEE Computer Society Press, 2009.
31. 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". In Proceeding of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2009), pp. 80-87, ACM Press, , Spain, 26-30 October, 2009.
32. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Enhanced Access Polynomial Based Self-Healing Key Distribution". In Proceeding of the ICST International Workshop on Security in Emerging Wireless Communication and Networking Systems (SEWCN09), LNICST (Springer Lecture Notes of ICST), 42, pp 13-24, Athens, Greece, September 14, 2010.

33. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Key Management in Multi-Distributor based DRM System with Mobile Clients using IBE". In Proceeding of the IEEE International conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009), pp. 597-602, IEEE Computer Society Press, London, UK, August 4-6, 2009.
34. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling. "Trade-Off between Collusion Resistance and User Life Cycle in Self-Healing Key Distributions with t-Revocation". In Proceeding of the IEEE International conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009), pp. 603-607, IEEE Computer Society Press, London, UK, August 4-6, 2009.
35. Ratna Dutta, Sourav Mukhopadhyay and Sabu Emmanuel. "Low Bandwidth Self-Healing Key Distribution in Wireless Ad Hoc Network". In Proceeding of the IEEE Asia International Conference on Modelling and Simulation (AMS 2008), pp. 867-872, IEEE Computer Society Press, Kuala Lumpur, Malaysia 13-15 May, 2008.
36. Ratna Dutta, Sourav Mukhopadhyay, Amitabha Das and Sabu Emmanuel. "Generalized Self-Healing Key Distribution using Vector Space Access Structure". In Proceedings of IFIP Networking 2008, **LNCS** 4982, pp. 612-623, Springer-Verlag, 2008.
37. Ratna Dutta and Sourav Mukhopadhyay. "Improved Self-Healing Key Distribution with Revocation in Wireless Sensor Network". In Proceeding of the IEEE Wireless Communications and Networking Conference (WCNC 2007), pp. 2965-2970, IEEE Computer Society Press, Hong Kong, 2007.
38. Ratna Dutta, Sourav Mukhopadhyay and Yong Dong Wu. "Constant Storage Self-Healing Key Distribution with Revocation in Wireless Sensor Network". In Proceeding of the IEEE International Conference on Communications (ICC 2007), pp. 1323-1328, IEEE Computer Society Press, Glasgow, 2007.
39. Ratna Dutta, Chang Ee-Chien and Sourav Mukhopadhyay. "Efficient Self-Healing Key Distributions with Revocation for Wireless Network using One Way Key Chains". In Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS 2007), **LNCS** 4521, pp. 385-400, Springer-Verlag, 2007.
40. Ratna Dutta and Sourav Mukhopadhyay. "Designing Scalable Self-Healing Key Distribution Schemes with Revocation Capability". In Proceedings of the 5th International Symposium on Parallel and Distributed Processing and Applications (ISPA-07), **LNCS** 4742, pp. 419-430, Springer-Verlag, 2007.
41. Sourav Mukhopadhyay and Palash Sarkar. "Hardware Architecture and Trade-offs for Generic Inversion of One-way Functions". In IEEE International Symposium on Circuits and Systems (ISCAS 2006), pp. 4847-4850, IEEE, Greece, 2006.
42. Sourav Mukhopadhyay and Palash Sarkar. "Application of LFSRs for Parallel Sequence Generation in Cryptologic Algorithms". In Proceedings of Applied Cryptography and Information Security 2006 (ACIS'06) in conjunction with ICCSA 2006, **LNCS** 3982, pp. 426-435, Springer-Verlag, 2006.
43. Sourav Mukhopadhyay and Palash Sarkar. "On the Effectiveness of TMTO and Exhaustive Search Attacks". In Proceedings of the 1st International Workshop on Security (IWSEC2006), **LNCS** 4266 , pp. 337-352, Springer-Verlag, 2006.

44. Alex Biryukov, Sourav Mukhopadhyay and Palash Sarkar. "Improved Time-Memory Trade-offs with Multiple Data". In Proceedings of Selected Areas in Cryptography (SAC'05), **LNCS** 3897, pp. 110-127, Springer-Verlag, 2005.
45. Sourav Mukhopadhyay and Palash Sarkar. "Application of LFSRs in Time/Memory Trade-Off Cryptanalysis". In Proceedings of Workshop on Information Security Applications (WISA'05), **LNCS** 3786, pp. 25-37, Springer-Verlag, 2005.

Technical Report:

1. Sourav Mukhopadhyay and Palash Sarkar. "A New Cryptanalytic Time/Memory/Data Trade-off Algorithm". IACR Technical Report, No. 2006/127, 2006. Available at http://eprint.iacr.org/2005/090.
2. Sourav Mukhopadhyay and Palash Sarkar. "Nearly Orthogonal Rainbow Tables". Indian Statistical Institute Technical Report, No. ASD/2004/9, November 2004.
3. Sourav Mukhopadhyay and Palash Sarkar. "Unified Analysis of Time/Memory/Data Trade-off Attacks". Indian Statistical Institute Technical Report, No. ASD/2005/2, February 2005.
4. Sourav Mukhopadhyay and Palash Sarkar. "TMTO with multiple Data: Analysis and new single table trade-offs". Indian Statistical Institute Technical Report, No. ASD/2005/7, 24 June 2005.
5. Sourav Mukhopadhyay and Palash Sarkar. "New Hardware Architecture for Generic Inversion of One-Way Function". Indian Statistical Institute Technical Report, No. ASD/2006/2, 24 March 2006.

c. Current Sponsored Projects:

Sl. No.	Responsibility	Title of the Project	Sponsoring Agency	Amount	Year	Status
1	Co-Investigator	Design and Analysis of Cryptographic Primitives using Multilinear Maps	NBHM	Rs. 3 Lakhs	2016	In Progress
2	Principal Investigator	Construction of Boolean Functions to Design Cryptographically Secure Stream Cipher	ISIRD, SRIC, IIT KGP	Rs. 5 Lakhs	2011	Complete
3	Principal Investigator	Cryptographic support for digital rights management	CSIR, Govt. of India	Rs 30 Lakhs	2012	Complete
4	Co-Investigator	Development of prototype of digital infrared thermal and optical imaging based system for early	MHRD,DEPARTMENT OF HIGHER EDUCATI	Rs 79 Lakhs	2014	In Progress

		detection of oral cancer	ON, NEW Delhi			

E. Talks:

- PKC
- ISM-Dhanbad
- "Fully Secure Self-Updatable Encryption in Prime Order Bilinear Groups", University of Hong Kong, Hong Kong, October 12, 2014.
- "Key managements problems in Digital Rights Managements", University of York, York, UK, October 20, 2009 (Invited).
- "A Study on Time/Memory Trade-Off Cryptanalysis", Ph.D. Defence, Indian Statistical Institute, Kolkata, India, June 22, 2007.
- "Self-Healing Key Distributions with Revocation for Wireless Sensor Network", IIT Kanpur, India, June 20, 2007 (Invited).
- "Efficient Self-Healing Key Distributions with Revocation for Wireless Network using One Way Key Chains", ACNS 2007, Zhuhai, China, June 8, 2007.
- "Introduction to Time/Memory Trade-off Cryptanalysis", IIT Guwahati, India, August 14, 2006 (Invited).
- "Time/Memory Trade-off Cryptanalysis", LACS, University of Luxembourg, Luxembourg, May 10, 2006 (Invited).
- "Time-Memory Tradeoffs with Multiple Data", ICSD Seminar, Institute for Infocomm Research (I2R), Singapore, August 26, 2005 (Invited).
- "Improved Time-Memory Trade-offs with Multiple Data", Selected Areas in Cryptography 2005, Kingston, Canada, August 11, 2005.
- "Application of LFSRs in Time/Memory Trade-Off Cryptanalysis", Information Security Applications 2005, Jeju Island, Korea, August 22, 2005.
- "Edge detection using wavelets based compression", National Brain Research Centre, Gurgaon, India, December 24, 2002 (Invited).

D. Short Academic Visits:

• University of Hong-Kong, October 2014.
• University of Wollongong, Australia, July 2014.
• University of York, York, UK, October 2009.
• Cryptography & Security Department, Institute for Infocomm Research, Singapore, July 14 to August 8, 2006.
• Laboratory of Algorithms, Security and Cryptology (LACS), University of Luxembourg, Luxembourg, May 9 to May 11, 2006.
• INRIA, Rocquencourt, Project CODES, FRANCE, April 3 to June 12, 2006.
• Attended the following conferences: ISC 2014, ACISP 2014, ACNS 2007, IEEE AMS 2007, IEEE WCNC 2007, SAC 2005, WISA 2005, Asiacrypt 2005, FSE 2004, Indocrypt 2004, Indocrypt 2000.

References

Prof. Bimal Roy
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata 700 108, India.
E-mail : bimal@isical.ac.in
Fax : +91 33 2577 3104

Prof. Palash Sarkar
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata 700 108, India.
E-mail : palash@isical.ac.in
Fax : +91 33 2577 3104

Prof. Subhamoy Maitra
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata 700 108, India.
E-mail : subho@isical.ac.in
Fax : +91 33 2577 3104

Prof. Arijit Chaudhuri
Applied Statistics Unit,
Indian Statistical Institute,
Kolkata 700 108, India.
E-mail : achau@isical.ac.in
Fax : +91 33 2577 3104