Dr. Ratna Dutta

Present Address:

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

Present Position:

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

Date of Birth : 11/09/1974

Sex (M/F): F

Academic Qualifications:

1. Ph.D. in Computer Science from Indian Statistical Institute, Kolkata in 2006. Topic: “Studies on Pairing-Based and Constant Round Dynamic Group Key Agreement”.
2. M.Sc. in Applied Mathematics (Specialization in Advanced Computer Science and Cybernetics) from University of Calcutta, Kolkata in 1998. Percentage of marks: 71.1 %.
3. B. Sc. in Mathematics Hons. from University of Calcutta, Calcutta in 1996. (College: Lady Brabourne College, Kolkata).Percentage of marks: 66.25 %.
4. Passed Higher Secondary (10+2) in 1993 from West Bengal Council for Higher Secondary Education. Subjects: Science (School: Barasat Girls’ High School, Barasat). Percentage of marks: 83.1 %
5. Passed Madhyamik Examinations in 1991from West Bengal Board of Secondary Education (School: Barasat Girls’ High School, Barasat) with 72.1 % marks.

Research/ Industry Experience:

1. Joined in Department of Mathematics, IIT Kharagpur, as Associate Professor during April 2016.
2. Worked as Assistant Professor, Department of Mathematics, IIT Kharagpur during December 2009-March 2016.
3. Worked as Post-doctoral Research Fellow, Claude Shannon Institute, NUIM, Maynooth, Co. Kildare, IRELAND during Feb 2008 - Dec 2009.
   Field of Work: Digital Rights Management, Self-Healing Key Distribution, Attribute-Based Encryption, Key Management Problem in Clustering-Based Wireless Mobile Ad Hoc Networks, Elliptic Curve Cryptography, Pairing-Based Cryptography.
4. Worked as Research Fellow, Institute for Infocomm Research, 21 Heng Mui Keng Terrace, Singapore 119613 during June 2006 - Feb 2008.
   Field of Work: Wireless Sensor Network, Self-Healing Key Distribution, Privacy-preserving Database and Information Retrieval, Digital Rights Management.
5. Worked as Visiting Scientist, UMA-ENSTA, 32 Boulevard Victor, 75739 Paris cedex 15, France during Apr 2006 - Jun 2006.
   Field of Work: Word Based Public Key Cryptosystems, studying existing protocols, their cryptanalysis in CCA model, analysing Oleshchuk’s Public Key Cryptosystem from both the designing and cryptanalytic aspects.

6. Worked as Senior Research Fellow, Stat-Math Unit, Indian Statistical Institute, Kolkata during Aug 2002 - Aug 2006.
   Field of Work: Pairing-Based Cryptographic Protocol Design, Constructing Efficient Constant Round Group Key Agreement in Dynamic Scenario, Password-Based Group Key Agreement, Security Analysis of the designed protocols in existing security models.
7. Worked as Junior Research Fellow, Stat-Math Unit, Indian Statistical Institute, Kolkata during Aug 2000 - Aug 2002
   Field of Work: Successful completion of two-year course work (2000-2002) with M.Tech in Computer Science, reading courses on Elliptic Curve Cryptography and Probability Theory.
8. Worked as Junior Research Fellow, Department of Applied Mathematics, University of Calcutta, Kolkata during Feb 1999 - Mar 2000
   Field of Work: Project on Seismology entitled Modeling of Seismic Wave Fields in Complex Structure

Teaching Experience:

- Cryptography and Security Issues (Jul-Dec 2011, 2014, 2019)
- Information and Coding Theory (Jan-May 2010-13, 2015, 2016, 2019, **2020**)
- Design & Analysis of Algorithms (Jul-Dec 2011, 2012)
- Data Structure and Algorithms (Jan-May 2011, 2014, 2019)
- Design & Analysis of Algorithms Lab (Jul-Dec 2011)
- Mathematics-II (Jan-May 2010-13)
- Mathematics-I (Jul-Dec 2013-19)
- Switching & Finite Automata (Jan-May 2014-18, **2020**)
- Graph Theory & Algorithms (Jul-Dec 2012, 2013)
- Number Theory (Jul-Dec 2015-18)
- Discrete Mathematics (Jan-May 2017, 2018)

Awards/ Distinctions:

1. Assistant Professorship, Department of Mathematics, Indian Institute of Technology, Kharagpur, India, December 2009 -March 2016.
2. Offered Professorship at Institute of Informatics, Istanbul Technical University for the Cybersecurity Engineering and Cryptography program, Turkey, 2014.
3. Offered Assistant Professorship, Department of Mathematics at the Indian Institute of Technology, Kanpur, India, 2009.
4. Offered Assistant Professorship, Department of Mathematics at the Indian Institute of Technology, Punjab, India, 2009.
5. Offered Assistant Professorship, CR Rao Advanced Institute Of Mathematics, Statistics and Computer Science (AIMSCS), University of Hyderabad Campus, India, 2009.
6. Post-doctoral Research Fellow, Claude Shannon Institute, NUIM, Maynooth, Ireland, 2007.
7. Associate Scientist, Institute for Infocomm Research (I2R), Singapore, 2006
8. Visiting Scientist, UMA-ENSTA, 32 Boulevard Victor, 75739 Paris cedex 15, France , 2006
9. Offered Post-doctoral Fellowship, Information Security Institute at the Queensland University of Technology, Brisbane, Australia, 2006.
10. Offered Scientist C post from Defence Research & Development Organization (DRDO), New Delhi, India, 2008.

11. Offered Scientist C post from National Technical Research Organization (NTRO), Govt. of India, New Delhi, 2007.
12. Offered Senior Lecturership, Department of Mathematics at the Indian Institute of Technology, Guwahati, India, 2007.
13. Offered Assistant Professorship, Department of Mathematics at the Indian Institute of Technology, Kanpur, India, 2007.
14. Senior Research Fellowship, Indian Statistical Institute, 2002
15. Junior Research Fellowship, Indian Statistical Institute, 2000
16. Junior Research Fellowship, Department of Applied Mathematics, University of Calcutta, 1999
17. Awarded UGC-SLET Junior Research Fellowship/Lectureship (Government of India), 2001
18. Awarded CSIR-NET Junior Research Fellowship/Lectureship (Government of India), 2000
19. Awarded GATE Junior Research Fellowship (Government of India), 1998
20. Ranked 2nd in M.Sc., Calcutta University, 1998.
21. Ranked 55th in H.S, West Bengal Council of Higher Secondary Education, 1993.
22. National Scholar for B.Sc Result, Government of India, 1996-98
23. National Scholar for H.S Result, Government of India, 1993-96

Doctoral Guidance:

Completed: 4

Ongoing: 5 Research scholars, 1 Project scholar.

Master’s and Bachelor’s Thesis Guidance:

Completed: 10 M.Tech. Students, 16 M.Sc. Student

Ongoing: 2 M.Sc. Student

Reviewed Papers Published/ Accepted:

Journal: 26; Conference: 66.

Sponsored Projects/ Consultancies:

Completed: 5; In Progress: 3

Industry Collaboration: Sumanta Sarkar, Research Scientist, TCS Innovation Labs, Hyderabad, India

Academic Collaboration: Shweta Agrawal, Associate Professor, Computer Science and Engineering department, Indian Institute of Technology, Madras.

Professional Activities:

1. Delivered series of lecture as invited speaker in a short term course on “Cyber Security” for Nigerian Citizens serving Nigerian Police, sponsored by the R&D company Stratign FZE, Dubai (UAE)) at IIT Kharagpur during 27th January - 7th February, 2020.
2. *Short-Term Course organized as Coordinator:* ***TEQIP-KIT sponsored*** *short term course on "Advanced Topics in Cryptography" during 10-14 February,* Dept. of Mathematics, IIT Kharagpur, 2020.
3. Delivered series of lecture as invited speaker in a short term course on “Cryptography and Cryptanalysis” for Egyptian military officers, sponsored by the

R&D company Stratign FZE, Dubai (UAE)) at IIT Kharagpur during 25th March - 4th April, 2019.

4. *Short-Term Course organized as Coordinator: TEQIP-III sponsored short term course on "Modern Cryptography" during 17-29 September,* Dept. of Mathematics, IIT Kharagpur, 2018.
5. *Short-Term Course organized as Coordinator: TEQIP-II sponsored short term course on "Introduction to Cryptography" during 27-31 January,* Dept. of Mathematics, IIT Kharagpur, 2017.
6. Delivered series of lecture as invited speaker at TEQIP-II sponsored short term course on "Fundamental Algorithms: Design and Analysis", IIT Kharagpur during 9 -13 February, 2017.
7. Significant advisory role: Pratish Datta (Completed PhD in 2017). Advisor: Sourav Mukhopadhyay, Department of Mathematics, Indian Institute of Technology, Kharagpur.
8. Significant advisory role: Sarbari Mitra (Completed PhD in 2014). Advisor: Sourav Mukhopadhyay, Department of Mathematics, Indian Institute of Technology, Kharagpur.
9. Representative of Claude Shannon Institute for European framework 7 E-crypt projects (eCrypt-2 MAYA Working Group)
10. Co-supervised Ph.D. students at Claude Shannon Institute.
11. Reviewer of papers for Theoretical Computer Science, Design, Codes and Cryptography Journal, Adhoc Networks, International Journal of Information Security, IEEE Transactions on Information Forensics & Security, IEEE Transactions on Information Theory, IEEE Transactions on Mobile Computing, IEEE Communications Letters, Journal of Systems and Software, Journal of Network and Computer Applications, EURASIP Journal of Wireless Communications and Networking, The Computer Journal, Journal of Network and Computer Applications, Security and Communication Networks, IEEE Communications Letters
12. Reviewer of papers for conferences Asiacrypt, PKC, ACISP, ACNS, Indocrypt, Inscrypt, ICC, ICISS, and many other international journals and conferences.
13. Following MS theses from the Department of Computer Science and Engineering, IIT-Kharagpur are examined:
    a) “Lightweight Crypto-Primitives on Fpgas” by Mr. Souvik Kolay (11CS72P03)
    b) “Algebraic Cryptanalysis of Stream Ciphers.” by Mr. Proloy Biswas (09CS7009)
    c) “Improvements of Linearization-Based Algebraic Attacks on Block Ciphers.” by Mr. Satrajit Ghosh (09CS7002)

A. List of Publications:
Journal:

1. 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, October 2019
2. 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.
3. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Constrained Pseudorandom Functions for Turing Machines Revisited: How to Achieve Verifiability and Key Delegation. Algorithmica, Springer, (accepted), 2019.
4. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Functional Signcryption. Journal of Information Security and Applications, Vol. 42, pp. 118-134, Elsevier, 2018.

5. Y.Sreenivasa Rao and Ratna Dutta, Computational Friendly Attribute-Based Encryptions with Short Ciphertext. Theoretical Computer Science (TCS), Vol. 668, pp. 1-26, ELSEVIER, 2017.
6. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Strongly Full-Hiding Inner Product Encryption. Theoretical Computer Science (TCS), Vol. 667, pp. 16-50, ELSEVIER, 2017.
7. Y.Sreenivasa Rao and Ratna Dutta.: Bandwidth-Efficient Attribute-Based Key-Insulated Signatures with Message Recovery. Information Sciences-Journal, Vol. 369, pp. 648-673, ELSEVIER, 2016.
8. Y.Sreenivasa Rao and Ratna Dutta, Attribute Based Key-Insulated Signature for Boolean Formula. In International Journal of Computer Mathematics, Vol. 93, No. 6, Taylor & Francis, 2016.
9. Vandana Guleria and Ratna Dutta.: Efficient Oblivious Transfer with Adaptive Queries in UC Framework. Journal of Security and Communication Networks, Vol. 9, No. 15, pp. 2592-2611, Wiley, 2016.
10. Sumit Kumar Debnath and Ratna Dutta**,** Towards Fair Mutual Private Set Intersection with Linear Complexity. In Security and Communication Networks, Vol. 9, No. 11, pp. 1589-1612, Wiley, 2016.
11. Y.Sreenivasa Rao and Ratna Dutta, Efficient Attribute-Based Signature and Signcryption Realizing Expressive Access Structures. International Journal of Information Security, Springer, Vol. , pp. 81-15, No.1109, 2016.
12. Y.Sreenivasa Rao and Ratna Dutta, Fully Secure Bandwidth-Efficient Anonymous Ciphertext-Policy Attribute Based Encryption. In Security and Communication Networks, Vol. 8, No. 18, pp. 4157-4176, Wiley, 2015
13. Y.Sreenivasa Rao and Ratna Dutta.: Fully Secure Anonymous Spatial Encryption Under Affine Space Delegation Functionality Revisited. Journal of Information Security and Applications, Vol. 24-25, pp. 1-12, ELSEVIER, 2015.
14. Vandana Guleria and Ratna Dutta, Universally Composable Issuer-Free Adaptive Oblivious Transfer with Access Policy. In Security and Communication Networks, Vol. 8, N0. 18, pp. 3615-3683, Wiley, 2015
15. 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, Science and Technology, Vol. 2, No. 2, pp. 150-184, 2014.
16. Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta, Key Pre-Distribution in a Non-Uniform Rectangular Grid for Wireless Sensor Networks. In the Journal of Applied Mathematics and Computing, Vol. 45, Issue 1-2, pp. 63-85, Springer, 2014.
17. Sarbari Mitra, Sourav Mukhopadhyay and Ratna Dutta, Unconditionally-Secure Key Pre-Distribution for Triangular Grid Based Wireless Sensor Network. In the Journal of Applied Mathematics and Computing, Vol. 44, Issue 1-2, pp.229–249, Springer, 2014.
18. Ratna Dutta, Anti-Collusive Self-Healing Key Distributions for Wireless Networks. In the International Journal of Wireless and Mobile Computing (IJWMC), Vol. 7, No. 4, pp.362-377, Special Issue on u- and e-Service, Science and Technology, 2014.
19. Sarbari Mitra, Sourav Mukhopadhyay, Ratna Dutta, A Group-Based Deterministic Key Predistribution Scheme for Wireless Sensor Network. In the International Journal of Wireless and Mobile Computing (IJWMC), Vol. 7, No. 5, pp. 435-447, Special Issue on u- and e-Service, Science and Technology, 2014.
20. Ratna Dutta, Sugata Sanyal, Collusion Resistant Self-Healing Key Distribution in Mobile Wireless Networks.In the International Journal of Wireless and Mobile Computing (IJWMC), Vol. 5, No. 3, pp.228-243, 2012.
21. Ratna Dutta and Tom Dowling, Provably Secure Hybrid Key Agreement Protocols in Cluster-Based Wireless Ad Hoc Networks. In Ad Hoc Networks 9(5): 767-787, 2011.

22. Ratna Dutta, Sourav Mukhopadhyay, and Martin Collier, Computationally Secure Self-Healing Key Distribution with Revocation in Wireless Ad Hoc Networks. In Ad Hoc Networks, Vol. 8, No. 6, pp. 597-613, ELSEVIER, 2010.
23. Ratna Dutta and Tom Dowling, Secure and Efficient Group Key Agreements for Cluster Based Networks. In the Transactions on Computational Sciences IV, Special Issue on Security in Computing, LNCS 5430, pp. 87-116, Springer-Verlag, 2009.
24. Ratna Dutta and Rana Barua, Provably Secure Constant Round Contributory Group Key Agreement in Dynamic Setting. In the IEEE Transactions on Information Theory (IEEE-IT), Vol. 54, No. 5, pp. 2007- 2025, May 2008.
25. Ratna Dutta, Converting Group Key Agreement Protocol into Password-Based Setting – Case Study. In the Journal of Computers, ISSN 1796-203X, Vol. 12, No. 2, pp. 26-33, Academy Publisher, October 2007.
26. Ratna Dutta and Rana Barua, Password-Based Encrypted Group Key Agreement. In the International Journal of Network Security (IJNS), Vol.3, No.1, pp. 23-34, July 2006. Available at http://isrc.nchu.edu.tw/ijns.

Conference:

1. Jayashree Dey, Ratna Dutta: Secure Key Encapsulation Mechanism with Compact Ciphertext and Public Key from Generalized Srivastava Code. In the Proceeding of the 22th Annual International Conference on Information Security and Cryptology (ICISC 2019), LNCS, Springer-Verlag, Seoul, Korea, 2019
2. Mriganka Mandal, Ratna Dutta: Efficient Identity-based Outsider Anonymous Public-Key Trace and Revoke with Constant Ciphertext-Size and Fast Decryption. In the Proceeding of the 15th International Conference on Information Security and Cryptology (INSCRYPT 2019), LNCS, Springer-Verlag, Nanjing, China, 2019
3. Tapas Pal, Ratna Dutta.: Offline Witness Encryption from Witness PRF and Randomized Encoding in CRS model, The 24th Australasian Conference on Information Security and Privacy (ACISP), Christchurch, New Zealand (2019)
4. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay.: Construction for a Nominative Signature Scheme from Lattice with Enhanced Security, International Conference on Codes, Cryptology And Information Security (C2SI 2019), Rabat - Morocco (2019)
5. Kamalesh Acharya, Ratna Dutta.: Constructions of Secure Multi-Channel Broadcast Encryption Schemes in Public Key Framework. In the Proceeding of the 17th International Conference on Cryptology And Network Security (CANS 2018), **LNCS**, pp. Springer-Verlag, Naples, Italy, 2018.
6. Mriganka Mandal, Ratna Dutta.: Efficient Adaptively Secure Public-Key Trace and Revoke from Subset Cover Using Deja Q Framework. In the Proceeding of the 14th International Conference on Information Security and Cryptology (Inscrypt 2018), **LNCS** ,pp. 468-489, Springer-Verlag, Fuzhou, China, 2018.
7. Mriganka Mandal, Ratna Dutta.: Cost-effective Private Linear Key Agreement with Adaptive CCA Security from Prime Order Multilinear Maps and Tracing Traitors. ICETE (2) 2018: 522-529, 2018.
8. Kamalesh Acharya, Ratna Dutta.: Recipient Revocable Broadcast Encryption Schemes Without Random Oracles. In the Proceeding of the 20th Annual International Conference on Information Security and Cryptology (ICISC 2017), **LNCS,** pp. Springer-Verlag, Seoul, Korea, 2017.
9. Kamalesh Acharya, Ratna Dutta.: Provable Secure Constructions for Broadcast Encryption with Personalized Messages. In the Proceeding of 11th International Conference on

Provable Security (ProvSec 2017), **LNCS** 10592, pp.329-348, Springer-Verlag , Xi'an, China, 2017.

10. 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** 10175, pp. 463-493, Springer-Verlag, Amsterdam, The Netherlands, 2017.
11. Sumit Kumar Debnath and Ratna Dutta.: New Realizations of Efficient and Secure Private Set Intersection Protocols Preserving Fairness. In the Proceeding of the 19th Annual International Conference on Information Security and Cryptology (ICISC 2016), **LNCS** 10157, pp. 254-284, Springer-Verlag, Seoul, Korea, 2016.
12. Kamalesh Acharya and Ratna Dutta.: Adaptively Secure Broadcast Encryption with Dealership. In the Proceeding of the 19th Annual International Conference on Information Security and Cryptology (ICISC 2016), **LNCS** 10157, pp. 161-177, Springer-Verlag, Seoul, Korea, 2016.
13. Sumit Kumar Debnath and Ratna Dutta.: Provably Secure Fair Mutual Private Set Intersection Cardinality Utilizing Bloom Filter. In the Proceeding of the 12th International Conference on Information Security and Cryptology (Inscrypt 2016), **LNCS** 10143, pp. 505-525, Springer-Verlag, Beijing, China, 2016.
14. Kamalesh Acharya and Ratna Dutta.: Secure and Efficient Construction of Broadcast Encryption with Dealership. In the Proceeding of Tenth International Conference on Provable Security (ProvSec 2016), **LNCS** 10005, pp. 277-295, Springer-Verlag, Nanjing, China, 2016.
15. Sumit Kumar Debnath and Ratna Dutta.: How to Meet Big Data When Private Set Intersection Realizes Constant Communication Complexity. In the Proceeding of the 18th IEEE International Conference on Information and Communications Security (ICICS 2016), **LNCS** 9977, pp. 445-454, Springer-Verlag, Singapore, 2016.
16. 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.
17. 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.
18. 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.
19. Sumit Kumar Debnath and Ratna Dutta, Efficient Private Set Intersection Cardinality in the Presence of Malicious Adversaries. In the Proceeding of Seventh International Conference on Provable Security (ProvSec 2015) **LNCS** 9451, pp. 326-339, Springer-Verlag, Kanazawa, Japan, 2015.
20. 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.
21. Sumit Kumar Debnath and Ratna Dutta, Secure and Efficient Private Set Intersection Cardinality using Bloom Filter. In the Proceeding of the 18th Information Security Conference (ISC 2015), **LNCS** 9290, pp 209-226 Springer-Verlag, Trondheim, Norway, 2015.

22. 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** 9290, pp 336-354, Springer-Verlag, Trondheim, Norway, 2015.
23. 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, pp 331-345, Springer-Verlag, Beijing, China, 2015.
24. Vandana Guleria and Ratna Dutta, Universally Composable Identity Based Adaptive Oblivious Transfer with Access Control. In the Proceeding of the 10th China International Conference on Information Security and Cryptology (Inscrypt 2014), **LNCS** 8957, pp 109-129, Springer-Verlag, Beijing, China, 2014.
25. Vandana Guleria and Ratna Dutta.: Adaptive Oblivious Transfer Realizing Expressive Hidden Access Policy. In the Proceeding of the 11th International Joint Conference, ICETE (Selected Papers) 2014: Volume 554 of the series Communications in Computer and Information Science, pp. 212-233, Springer, 2014.
26. Vandana Guleria and Ratna Dutta, Issuer-Free Adaptive Oblivious Transfer with Access Policy. In the Proceeding of the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014), **LNCS** 8949, pp 402-418, Springer-Verlag, Seoul, Korea, 2014.
27. Sumit Kumar Debnath and Ratna Dutta, A Fair and Efficient Mutual Private Set Intersection Protocol from a Two-way Oblivious Pseudorandom Function. In the Proceeding of the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014), **LNCS** 8949, pp 343-359, Springer-Verlag, Seoul, Korea, 2014.
28. Vandana Guleria and Ratna Dutta, Efficient Adaptive Oblivious Transfer without q-type Assumptions in UC Framework. In the Proceeding of the 16th International Conference on Information and Communications Security (ICICS 2014), **LNCS**, Springer-Verlag, Hong Kong, China, *(accepted)* 2014.
29. Y.Sreenivasa Rao and Ratna Dutta, Attribute Based Key-Insulated Signatures with Message Recovery. In the Proceeding of the 16th International Conference on Information and Communications Security (ICICS 2014), **LNCS**, Springer-Verlag, Hong Kong, China, *(accepted)* 2014.
30. Vandana Guleria and Ratna Dutta, Adaptive Oblivious Transfer with Hidden Access Policy Realizing Disjunction. In the Proceeding of the 11th International Conference on Security and Cryptography (SECRYPT 2014), pp. 43-54, Vienna, Austria, 2014.
31. Vandana Guleria and Ratna Dutta, Lightweight Universally Composable Adaptive Oblivious Transfer. In the Proceeding of the 8th International Conference on Network and System Security (NSS 2014), **LNCS** 8792, pp. 285-298, Springer-Verlag, Xian, China, 2014.
32. 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, Hong Kong, China, 2014.
33. Y.Sreenivasa Rao and Ratna Dutta, Expressive Bandwidth-Efficient Attribute Based Signature and Signcryption. In the Proceeding of 19th Australasian Conference on Information Security and Privacy (ACISP 2014), **LNCS** 8544, pp. 209-225, Springer-Verlag, Wollongong, Australia, 2014.
34. 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, Wollongong, Australia, 2014. Also available at http://eprint.iacr.org/2014/584.

35. Y.Sreenivasa Rao and Ratna Dutta, Expressive Attribute Based Signcryption with Constant-Size Ciphertext. In the Proceeding of 7-th International Conference on the Theory and Applications of Cryptology (Africacrypt 2014)， **LNCS** 8469, pp. 398–419, Springer-Verlag, Marrakesh, Morocco, 2014.
36. Vandana Guleria and Ratna Dutta, Efficient Adaptive Oblivious Transfer in UC Framework. In the Proceeding of the 10-th Information Security Practice and Experience Conference (ISPEC 2014), **LNCS** 8434, pp. 271–286, Springer-Verlag, Fuzhou, China, 2014.
37. Y.Sreenivasa Rao and Ratna Dutta, Dynamic Ciphertext-Policy Attribute-Based Encryption for Expressive Access Policy. In the Proceeding of 10-th International Conference on Distributed Computing and Internet Technology (ICDCIT 2014), **LNCS** 8337, pp. 275-286, Springer-Verlag, Bhubaneswar, India, 2014.
38. Y.Sreenivasa Rao and Ratna Dutta, Computationally Efficient Expressive Key-Policy Attribute Based Encryption Schemes with Constant-Size Ciphertext. In the Proceeding of 15th International Conference on Information and Communications Security (ICICS 2013), **LNCS** 8233, pp. 346-362, Springer-Verlag, 2013.
39. Y.Sreenivasa Rao and Ratna Dutta, Computationally Efficient Dual-Policy Attribute Based Encryption with Short Ciphertext. In the Proceeding of Seventh International Conference on Provable Security (ProvSec 2013), **LNCS** 8209, pp. 288-308 , Springer-Verlag, 2013.
40. Y.Sreenivasa Rao and Ratna Dutta, Recipient Anonymous Ciphertext-Policy Attribute Based Encryption. In the Proceeding of 9th International Conference on Information Systems Security (ICISS 2013), **LNCS**, 8303, 2013, pp. 329-344, Springer-Verlag, 2013.
41. Y.Sreenivasa Rao and Ratna Dutta, Decentralized Ciphertext-Policy Attribute-Based Encryption Scheme with Fast Decryption. In the Proceeding of the 14th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2013), **LNCS** 8099, pp. 66-81, Springer-Verlag, 2013.
42. Y.Sreenivasa Rao and Ratna Dutta, Efficient Attribute Based Access Control Mechanism for Vehicular Ad Hoc Network, In the Proceeding of 7th International Conference on Network and System Security (NSS 2013), **LNCS** 7873, pp. 26-39 Springer-Verlag, 2013.
43. 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.
44. Y.Sreenivasa Rao and Ratna Dutta, Computationally Efficient Secure Access Control for Vehicular Ad Hoc Networks, In the Proceeding of eighth International Conference on Information Systems Security (ICISS 2012), **LNCS** 7671, pp. 294-309 Springer-Verlag, 2012.
45. 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.
46. Ratna Dutta, Access Polynomial Based Self-Healing Key Distribution with Improved Security and Performance. In Proceeding of InfoSecHiComNet 2011, **LNCS** 7011, pp. 72-82, Springer-Verlag, 2011.
47. 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.
48. 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.
49. 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.

50. Ratna Dutta, Dheerendra Mishra and Sourav Mukhopadhyay, Vector Space Access Structure and ID based Distributed DRM Key Management. In proceedings of ACC 2011, Part IV, CCIS 193, pp. 223-232, Springer-Verlag, 2011.
51. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling, Enhanced Access Polynomial Based Self-Healing Key Distribution. In proceedings 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, 2010.
52. Ratna Dutta , Sourav Mukhopadhyay and Tom Dowling, Generalized Self-Healing Key Distribution in Wireless Ad hoc Networks with Trade-Offs in Users Pre-Arranged Life Cycle and Collusion Resistance. In proceedings of the 5th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2009), **ACM** Press, pp. 80-87, 2009.
53. Ratna Dutta,Sourav Mukhopadhyay and Tom Dowling, Key Management in Multi-Distributor based DRM System with Mobile Clients using IBE. Accepted in the International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009), pp. 597-602, **IEEE**, London, 2009.
54. Ratna Dutta, Sourav Mukhopadhyay and Tom Dowling, Trade-Off between Collusion Resistance and User Life Cycle in Self-Healing Key Distributions with t-Revocation. Accepted in the International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2009), pp. 603-607, **IEEE**, London, 2009.
55. 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.
56. 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, 2008.
57. Ratna Dutta, Chang Ee-Chien and Sourav Mukhopadhyay, Efficient Self-Healing Key Distributions with Revocation for Wireless Sensor Network using One Way Key Chains. In proceedings of ACNS’07, **LNCS** 4521, pp. 385-400, Springer-Verlag, 2007.
58. Ratna Dutta and Sourav Mukhopadhyay, Designing Scalable Self-Healing Key Distribution Schemes with Revocation Capability . In proceedings of ISPA’07, **LNCS** 4742, pp. 419-430, Springer-Verlag, 2007.
59. Ratna Dutta and Sourav Mukhopadhyay, Constant Storage Self-Healing Key Distribution with Revocationin Wireless Sensor Network. In proceeding of the **IEEE** International Conference on Communications (ICC 2007), pp. 1323-1328, IEEE Communications Society Press, 2007.
60. 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) - Networking, pp. 2965-2970, **IEEE** Communications Society Press, 2007.
61. Ratna Dutta, Overcome Weakness of a Password-Based Group Key Agreement Protocol. In proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC 2007), pp. 469-474, **IEEE** Computer Society and Communications Society Press, 2007.
62. Ratna Dutta, Multi-Party Key Agreement in Password-Based Setting. In proceeding of the IEEE Asia International Conference on Modelling and Simulation (AMS 2007), pp. 133-138, **IEEE** Computer Society Press, 2007.
63. Ratna Dutta and Rana Barua, Constant Round Dynamic Group Key Agreement. In proceedings of ISC’05, **LNCS** 3650, pp. 74-88, Springer-Verlag, 2005.

64. Ratna Dutta and Rana Barua, Dynamic Group Key Agreement in Tree-Based Setting. In proceedings of ACISP’05, **LNCS** 3574, pp. 101-112, Springer-Verlag, 2005. Also available at http://eprint.iacr.org/2005/131.
65. Ratna Dutta, Rana Barua and Palash Sarkar, Provably Secure Authenticated Tree Based Group Key Agreement. In proceedings of ICICS’04, **LNCS** 3269, pp. 92-104, Springer-Verlag, 2004. Also available at http://eprint.iacr.org/2004/090.\
66. Rana Barua, Ratna Dutta and Palash Sarkar, Extending Joux Protocol to Multi-Party Key Agreement. In proceedings of INDOCRYPT’03, **LNCS** 2904, pp. 205-217, Springer-Verlag, 2003. Also available at http://eprint.iacr.org/2003/062.

Technical Report:

1. Ratna Dutta and Rana Barua, Overview of Key Agreement Protocols. Available at http://eprint.iacr.org/2005/289.
2. Ratna Dutta, Rana Barua and Palash Sarkar, Pairing Based Cryptographic Protocols : A Survey. Available at http://eprint.iacr.org/2004/064/
3. Ratna Dutta and Rana Barua, Group Key Agreement Immune to Dictionary Attacks. In proceedings of National Workshop on Cryptology 2005, Shimoga, India, August 2005.
4. Ratna Dutta, Rana Barua and Palash Sarkar, Authenticated Multi-party Key Agreement : A Provably Secure Tree Based Scheme using Pairing. In proceedings of National Workshop on Cryptology 2004, Kerala, India, October 2004.

B. Current Sponsored Projects:

Sl. No.	**Responsibility**	**Title of the Project**	**Sponsoring Agency**	**Amount**	**Year**	**Status**
1	Principal Investigator	Designing ABE Schemes for Fine-Grained Access Control in DTNs	ISIRD, SRIC, IIT KGP	Rs. 5 Lakhs	2011	Complete
2	Principal Investigator	Elliptic Curves and Pairing Based Cryptography for Wireless Communications	DST First Track Scheme for Young Scientist	Rs. 10.92 Lakhs	2012	Complete
3	Principal Investigator	Secure Key Management in Wireless Adhoc Network	ISRO, IIT Kharagpur CELL Space Technology Cell	Rs. 23.688 Lakhs	2013	Complete
4	Co-Investigator	Cryptographic support for Digital Rights Management	CSIR	Rs. 30 Lakhs	2012	Complete
5	Principal Investigator	Design and Analysis of Cryptographic Primitives using Multilinear Maps	NBHM	Rs. 3.325 Lakhs	2016	Complete
6	Principal Investigator	Constructing New Central Trapdoors	**Mathematical Research**	Rs. 6.60	2021	In progress

		and Multivariate Cryptosystems from Hidden Field Equations	**Impact Centric Support (MATRICS)** to the Science and Engineering Research Board (SERB)	Lakhs		
7	Principal Investigator	Construction of Optimal Trace and Revoke System in Broadcast Encryption	**Core Research Grant** to the Science and Engineering Research Board (SERB)	Rs. 18.92 Lakhs	2021	In progress
8	Principal Investigator	Quantum Resistant Cryptographic Protocols for Cloud computing	ISRO, IIT Kharagpur CELL Space Technology Cell	Rs. 24.768 Lakhs	2022	In progress

C. Conferences Attended

- Invited talk on On Practical Functional Encryption at IIT-Guwahati, India, May 2019
- Invited talk on Homomorphic Encryption and Functional Encryption at NIT-Jamsedpur, India, July 2019
- Invited talk on Code-based cryptography at ISM-Dhanbad, India, September 2018
- Invited talk on Broadcast Encryption and Attribute-Based Encryption at IIIT-Delhi, India, July 2018
- Invited talk on Multivariate Public Key Encryption at Indian Statistical Institute, Delhi, India, July 2018
- Invited talk on Identity-based cryptosystems at ACM summer school, Indian Statistical Institute, Kolkata, India, June 2018

- Invited talk on Functional Encryption at 14th Annual ADMA Conference & Graph Theory Day, Dhirubhai Ambani Institute of Information and Communication Technology, India June 2018

- Presented papers in the 19th Annual International Conference on Information Security and Cryptology (ICISC 2016) held in Seoul, Korea, November 2016

- Presented paper in the 19th Australian Conference on Information Security and Privacy (ACISP'14) held in University of Wollongong, Australia, July 2014

- Presented progress of Fast Track SERB/DST YS project in Group Monitoring Workshop (GMW) on SERB/DST Young Scientists Scheme (YS) in Physical & Mathematical Sciences held in Kodaikanal Solar Observatory, Indian Institute of Astrophysics, Kodaikanal, India, August 2014

- Presented paper in the Claude Shannon Institute Workshop on Coding and Cryptography (CSI WCC’08) held in Dublin, Ireland, November 2008

- Presented paper in the Claude Shannon Institute Workshop on Coding and Cryptography (CSI WCC’08) held in Cork, Ireland, May 2008

- Presented paper in the IEEE Wireless Communications and Networking Conference - Networking (WCNC’07) held in Hong Kong, March 2007

- Presented paper in the 1st IEEE Asia International Conference on Modelling & Simulation (AMS’07) held in Phuket, Thailand, March 2007

- Presented paper in the 10th Australian Conference on Information Security and Privacy (ACISP’05) held in Queensland University of Technology, Brisbane, Australia, July 2005

- Presented paper in the 6th International Conference on Information and Communications Security (ICICS’04) held in Malaga, Spain, October 2004

- Presented paper in the 4th International Conference on Cryptology in India (INDOCRYPT’03) held in Delhi, India, December 2003

- Presented paper in the 4th Annual Inter Research Institute Student Seminar (IRISS’05) held in Indian Institute of Technology (IIT), Kanpur, April 2005

- Presented paper in the 2nd National Workshop on Cryptology (NWC’02) held in Indian Statistical Institute, Delhi, India, October 2002

- Presented paper in the 3rd National Workshop on Cryptology (NWC’03) held in MIT Campus of Anna University, Chennai, India, October 2003

- Presented paper in the 4th National Workshop on Cryptology (NWC’04) held in Amrita Vishwa Vidyapeetham, Kerala, India, September 2004

- Presented paper in the 5th National Workshop on Cryptology (NWC’05) held in Jawaharlal Nehru National College of Engineering, Shimoga, India, August 2005

- Attended the 3rd International Conference on Cryptology in India (INDOCRYPT’02) held in Hydarabad, India, December 2002

- Attended the 6th International Conference on Cryptology in India (INDOCRYPT’05) held in Indian Institute of Science (IISc), Bangalore, India, December 2005

- Attended the 11th Annual International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT’05) held in Chennai, India, December 2005

- Lectured on “Elliptic curve public key cryptosystems and pairings” in the LACS Seminar held in University of Luxembourg, Luxembourg, May 2006

- Attended the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS’07) held in Singapore, March 2007

• Lectured on “Key agreements protocals” in the staff seminar held in National University of Ireland, Maynooth, April 2008

• Lectured on “Secure and efficient hybrid key agreement schemes in clustered wireless networks” in the staff seminar held in National University of Ireland, Maynooth, November 2008

• Attended Kick-Off Meeting of ECRYPT II held in Katholieke Universiteit Leuven, Belgium, November 2008

• Attended the Claude Shannon Institute Workshop on Coding and Cryptography (CSI WCC’09) held in Cork, Ireland, May 2009

D. Short Academic Visits

• (in 2016) ICISC 2016, Seoul, Korea.
• (in 2014) University of Wollongong, Australia.
• (in 2009) University of York, York, UK.
• (in 2009) University College Cork, Cork, Ireland.
• (in 2008) Department of Electrical Engineering (Division COSIC) at the Katholieke Universiteit Leuven, K. U. Leuven, Department Electrotechniek-Esat, Kasteel Park, Arenberg 10, B- 3001, Heverlee.
• (in 2008) University College Cork, Cork, Ireland.
• (in 2006) UMA-ENSTA, 32 Boulevard Victor, 75739 Paris cedex 15, France.
• (in 2006) University of Luxembourg, Campus Limptersberg, 162A, avenue de la Faiencerie, L-1511, Luxembourg.
• (in 2005) Information Security Institute at the Queensland University of Technology, George Street, Brisbane, Australia.
• (in 2004) Department of Electrical Engineering (Division COSIC) at the Katholieke Universiteit Leuven, K. U. Leuven, Department Electrotechniek-Esat, Kasteel Park, Arenberg 10, B- 3001, Heverlee.

E. Relevant Courses

• Cryptology and Data Security
• Information and Coding Theory
• Discrete Mathematics : Combinatorics, Graph Theory and Logic
• Programming Techniques and Data Structures
• Design and Analysis of Algorithms
• Topics in Algorithmic Graph Theory and Discrete Optimization
• Theory of Automata, Languages, Computability and Complexity

F. Research Interest

• Elliptic Curves and Pairing based Cryptography
• Functional Encryption and Attribute Based Cryptosystems
• Coding Theory and Combinatorial Applications in WSN
• Oblivious Transfer & Private Information Retrieval
• Code-Based Cryptography
• Obfuscation: constructions and applications
• Multilinear maps and their applications
• Lattice-Based Cryptography
• Multivariate Cryptosystems

G. Teaching Interest

- Bachelor’s level: Algebra, Real Analysis, Calculus, Differential Equations, Numerical Analysis, Vector Analysis, Co-ordinate Geometry, Probability, Statistics.

- Master’s level: Complex Analysis, Numerical Analysis, Operations Research, Laplace and Fourier Transforms, Ordinary and Partial Differential Equation, Cryptology and Data Security, Information and Coding Theory, Discrete Mathematics : Combinatorics, Graph Theory and Logic, Programming Techniques and Data Structures, Design and Analysis of Algorithms, Topics in Algorithmic Graph Theory and Discrete Optimization, Theory of Automata, Languages, Computability and Complexity.

- Doctoral Level: Public Key Cryptography, Elliptic Curves, Pairings, Lattice, Multivariate Cryptography, Multilinear Maps and Obfuscators.

H. References

- Prof. Bimal Roy
Applied Statistics Unit
Indian Statistical Institute
Kolkata - 700 108
Tel. (91)(33) 2575-2809, 2575-2501
Fax. (91)(33) 2577-3104, 2577-6037
E-mail: bimal@isical.ac.in

- Prof. Rana Barua
Stat-Math Unit
Indian Statistical Institute
Kolkata - 700 108
Tel. (91)(33) 2575-3410, 2575-3400
Fax. (91)(33) 2577-3071
E-mail: rana@isical.ac.in

- Prof. Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
Kolkata - 700 108
Tel. (91)(33) 2575-3244
Fax. (91)(33) 2577-3104
E-mail: subho@isical.ac.in

- Prof. Tom Dowling
Claude Shannon Institute
Department of Computer Science
National University of Ireland, Maynooth
Co. Kildare, Ireland
Tel. (353)-1-708 4526
Fax. (353)-1-708 3848
E-mail: tdowling@cs.nuim.ie

- Prof. Gary McGuire
Claude Shannon Institute
UCD CASL

University College Dublin
Dublin 4, Ireland
Tel. (353)-1-716-2238 (UCD), (353)-1-716-5319 (CSI)
E-mail: gary.mcguire@ucd.ie

- Prof. Ee-Chien Chang
School of Computing
National University of Singapore
3 Science Drive 2, Singapore 117543
Tel.(65) 6516 6168
Fax.(65) 6779 4580
E-mail: changec@comp.nus.edu.sg