

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:

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 % (Ranked 2nd).
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 % (Ranked 55th).
5. Passed Madhyamik Examinations in 1991 from 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 full time Professor from October 2025.
2. Worked as associate Professor, Department of Mathematics, IIT Kharagpur during April 2016 - October 2025.
3. Worked as Assistant Professor, Department of Mathematics, IIT Kharagpur during December 2009-March 2016.
4. 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.
5. 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.
6. 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.

7. 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.
8. 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.
9. 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:

1. Cryptography and Security Issues (Jul-Dec 2011, 2014, 2019, 2020, 2022, 2023, 2024, **2025**)
2. Information and Coding Theory (Jan-May 2010-13, 2015, 2016, 2019, 2020, 2024)
3. Design & Analysis of Algorithms (Jul-Dec 2011, 2012)
4. Data Structure and Algorithms (Jan-May 2011, 2014, 2019)
5. Design & Analysis of Algorithms Lab (Jul-Dec 2011)
6. Mathematics-II (Jan-May 2010-13)
7. Mathematics-I (Jul-Dec 2013-19)
8. Switching & Finite Automata (Jan-May 2014-18, 2020)
9. Graph Theory & Algorithms (Jul-Dec 2012, 2013)
10. Number Theory (Jul-Dec 2015-18, Aug-Nov 2021)
11. Discrete Mathematics (Jan-May 2017, 2018, 2021)
12. Advanced Calculus (Dec 2020-Mar 2021, Dec 2021-Mar 2022, Nov 2022-Mar 2023)
13. Theory of Computation (Jan-Apr 2022, 2024, 2025)
14. Modern Algebra (Jan-Apr 2023)
15. Optimization Techniques (Jul-Dec 2023, 2024, **2025**)
16. Improper Integral, Vector Calculus and Complex Analysis (Jan-May 2025)

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 (NTRON), Govt. of India, New Delhi, 2007.
12. Offered Senior Lectureship, 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 (Single guidance):

1. Y Sreenivasa Rao (Completed in 2015). Currently Assistant Professor at Department of Mathematics, National Institute of Technology, Warangal, Telangana, INDIA.
Dissertation: Design and Analysis of Attribute-Based Cryptosystems using Bilinear Pairings
2. Vandana (Completed in 2015). Currently Assistant Professor at National Institute of Advanced Manufacturing Technology, Ranchi, INDIA.
Dissertation: Designs of Universally Composable Secure Adaptive Oblivious Transfer Protocols
3. Sumit Kumar Debnath (Completed in 2017). Currently Assistant Professor at Department of Mathematics, National Institute of Technology, Jamshedpur, Jharkhand, INDIA.
Dissertation: Design of Privacy Preserving Secure Set Intersection Protocols
4. Kamallesh Acharya (Completed in 2018). Currently Assistant Professor at NIT Rourkela, INDIA.
Dissertation: Secure and Efficient Constructions of Broadcast Encryption Protocols
5. Mriganka Mandal (Completed in 2020). Currently Assistant Professor at ISI Kolkata, INDIA.
Dissertation: Design and Analysis of Optimal Trace and Revoke Systems in Broadcast Encryption
6. Tapas Pal (Completed in 2021). Currently Group Leader KASTEL-C&C@KIT, Germany.
Dissertation: Designing Provably Secure Advanced Cryptographic Primitives: Witness Encryption, Fully Homomorphic Encryption and Functional Encryption
7. Chinmoy Biswas (Completed in 2022). Currently postdoc at University of Calgary, Canada.
Dissertation: Design and Analysis of Post-Quantum Cryptographic Primitives and Key Predistribution Scheme
8. Jayashree Dey (Completed in 2024). Currently postdoc at IIT Chennai, INDIA.
Dissertation: A Study on Secure Post-Quantum Cryptographic Primitives from Error Correcting Codes and Multivariate Polynomials

10. Surbhi Shaw (Completed 2024). Currently postdoc at IISc Bangalore, INDIA.
Dissertation: Towards Designing Provably Secure Advanced Cryptographic Primitives from Isogenies for Post-quantum Era

Significant Advisory Role:

1. Subhranil Dutta (Completed PhD in 2024). Currently postdoc at University of St. Gallen, Switzerland
[Advisor: Sourav Mukhopadhyay](#), Department of Mathematics, Indian Institute of Technology, Kharagpur.
Dissertation: Selected Constructive Approaches towards Linear Functional Encryption with Advanced Features for Cloud Computing.
2. Anushree Belel (Completed PhD in 2024). Currently postdoc at ROVIRA I VIRGILI UNIVERSITY, SPAIN.
[Advisor: Sourav Mukhopadhyay](#), Department of Mathematics, Indian Institute of Technology, Kharagpur.
Dissertation: A Study of Provably Secure Advanced Encryption Techniques Using Pairing-Based Cryptography
3. Meenakshi Kansal (Completed PhD in 2020). Currently Assistant Professor at Rashtriya Raksha University, Gandhinagar, Gujrat, INDIA.
[Advisor: Sourav Mukhopadhyay](#), Department of Mathematics, Indian Institute of Technology, Kharagpur.
Dissertation: Design and Analysis of Lattice Based Group Signature, Nominative Signature and Multisignature.
4. Pratish Datta (Completed PhD in 2017). Currently Research Scientist at NTT Research, Inc., Palo Alto, California, USA
[Advisor: Sourav Mukhopadhyay](#), Department of Mathematics, Indian Institute of Technology, Kharagpur.
Dissertation: Design and Analysis of Expressive and Secure Functional Encryption, Signcryption and Constrained Pseudorandom Function.
5. Sarbari Mitra (Completed PhD in 2014), Currently Professor at Fort Hays State University, USA.
[Advisor: Sourav Mukhopadhyay](#), Department of Mathematics, Indian Institute of Technology, Kharagpur.
Dissertation: A Study on Key Pre-distribution in Wireless Sensor Networks.

Ongoing: 6 Research scholars

Master's and Bachelor's Thesis Guidance:

Completed: 16 M.Tech. students, 32 M.Sc. student, 37 B.Tech. students
Ongoing: 1 M.Sc. student, 5 B.Tech student

Reviewed Papers Published/ Accepted:

Journal: 48; Conference: 89

Sponsored Projects/ Consultancies:

Completed: 9; In Progress: 3; Approved: 1

Industry Collaboration:

1. Sumanta Sarkar, Research Scientist, TCS Innovation Labs, Hyderabad, India (2019-2020)
2. Nikhil Rathod, Arqanum Technologies, Pune, India (2022-2023)

Academic Collaboration:

1. Katsuyuki Takashima, Professor, Waseda University, Japan (2025), joint proposal submitted under LOTUS Program (<https://www.jst.go.jp/program/india/en/call/>)
2. Ludovic Perret, Professor, EPITA/LRE, Paris (2025), joint proposal submitted under the Indo-French call for proposals CEFIPRA (<https://www.cefipra.org/PgmIA.aspx?p=IR>)
3. Sumanta Sarkar, Lecturer, Universty of Esseex, UK (2025)
4. Cong Zuo, Associate Professor, School of Cyberspace Science and Technology, Beijing Institute of Technology, Beijing, China (2024)
5. Gulshan Gupta, Scientist, Space Applications Centre, Indian Space Research Organization (ISRO), Dept. of Space, Govt. of INDIA (2021-2025)
6. Rohit Tyagi, Scientist, Space Applications Centre, Indian Space Research Organization (ISRO), Dept. of Space, Govt. of INDIA (2021-2025)
7. Deval Mehta, Scientist, Space Applications Centre, Indian Space Research Organization (ISRO), Dept. of Space, Govt. of INDIA (2016-2018)

Professional Activities:

1. **Program Co-Chairs:** [Indocrypt 2025, the 26th International Conference on Cryptology in India](#), Bhubaneswar, Orissa, India, December 14 - 17, 2025.

2. Institute level:

- a) Warden, Gokhale Hall (Jan 2017-Jan 2021)
- b) Acting Warden, Gokhale Hall (Feb 2016-April 2016)
- c) Assistant Warden, Gokhale Hall (Nov 2015-Jan 2017)
- d) Assistant Warden, Sam Hall (Oct 2013-Oct 2015)

3. Departmental level:

- a) Faculty Advisor for Mathematics and Computing(1st year of BS-MS), July 2025-June 2026
- b) Departmental Examination In-Charge (Professor-in-Charge), July 2024-June 2025
- c) Faculty Advisor (M.Tech CSDP), July 2023-June 2025
- d) Laboratory in-charge (Computer Laboratory) (Apr 2019-till date)
- e) Department Faculty Recruitment Committee (Jun 2023-till date)
- f) Subject Co-ordinator (Advanced Calculus) (Aug 2022-Jul 2023)
- g) Department Administrative Committee (Apr 2015-June 2024)
- h) Department PG&R Academic (Apr 2016-till date)
- i) Department Computer Committee (Apr 2016-till date)
- j) Faculty Advisor (2nd year of 2 years M.Sc.- Ph.D), July 2021-June 2022
- k) Faculty Advisor (5th year of 5 years M.Sc. Maths & Computing), July 2020-June 2021
- l) Faculty Advisor (4th year of 5 years M.Sc. Maths & Computing, July 2019-June 2020
- m) Faculty Advisor (M.Tech CSDP), July 2017-June 2019
- n) Library-in-charge (Central) (Apr 2011-June 2017)
- o) Social & Culture (Apr-2012-Mar 2016)
- p) Faculty Advisor (2 years M.Sc.- Ph.D), July 2013-June 2015

4. Workshop organized: India Post Quantum-Crypto Workshop-2020, a two-day workshop organized by IIT Kharagpur and TCS Hyderabad in virtual/online mode, November 17-18, 2020
5. Seminar organized (Details are in <https://www.kgpmathcrypto.com/>):
 - a) Prof. Steven Galbraith, Head, Department of Mathematics, University of Auckland, New Zealand, August 26, 2020
 - b) Prof. Frederik Vercauteren, Research Group COSIC, KU Leuven, Belgium, October 29, 2020
6. 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.
7. *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.*
8. 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.
9. *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.*
10. *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.*
11. 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.
12. Representative of Claude Shannon Institute for European framework 7 E-crypt projects (eCrypt-2 MAYA Working Group)
13. Co-supervised Ph.D. students at Claude Shannon Institute.
14. 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 and many more.
15. Reviewer of papers for conferences Asiacrypt, PKC, ACISP, ACNS, Indocrypt, Inscrypt, ICC, ICISS, and many other international and conferences.
16. 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)

17. Program Committee Member of the 24th International Conference on Cryptology in India (Indocrypt 2022-2024)

18. Program Committee Member of the Cryptography and Security track of the 25th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2023)

19. Chairperson, Technical Evaluation Committee for Quantum Encryption Algorithm (QEA), Telecom Technology Development Fund (TTDF), Ministry of Communications, Department of Telecommunications, Government of India, 2025

Member of Professional Bodies:

Life member of Cryptology Research Society of India (CRSI)

A. List of Publications:

(Citations - 3149, h-index – 27, i10-index- 70)

Journal:

1. Surbhi Shaw and Ratna Dutta: Post-quantum secure compact deterministic wallets from isogeny-based signatures with rerandomized keys. Theoretical Computer Science (TCS) Journal, Vol. 1035: 115127, Elsevier, 2025. <https://doi.org/10.1016/j.tcs.2025.115127>, Impact Factor: 1.0, SCIE.
2. Subhranil Dutta, Ratna Dutta and Sourav Mukhopadhyay: Securing Data in the Cloud Using Pairing-free Inner Product Functional Encryption with Unbounded Vector Size. Theoretical Computer Science (TCS) Journal, Vol. 1031: 11508, Elsevier, 2025. <https://doi.org/10.1016/j.tcs.2025.115085>, Impact Factor: 1.0, SCIE.
3. Jayashree Dey and Ratna Dutta: Privacy Enhanced Secure Compact Attribute-Based Signature from MQ Problem for Monotone Span Program. Theoretical Computer Science (TCS) Journal, Vol. 1020: 114929, Elsevier, 2024. <https://doi.org/10.1016/j.tcs.2024.114929> , Impact Factor: 1.0, SCIE.
4. Subhranil Dutta, Tapas Pal and Ratna Dutta, Reinforcing Privacy in Cloud Computing via Adaptively Secure Non-zero Inner Product Encryption and Anonymous Identity-based Revocation in Unbounded Setting. Theoretical Computer Science (TCS), Vol. 995: 114502, Elsevier, 2024. <https://doi.org/10.1016/j.tcs.2024.114502>, Impact Factor: 1.0, SCIE.
5. 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, Vol. 83(33): 78827-78859 Springer, 2024. DOI:[10.1007/s11042-024-18626-w](https://doi.org/10.1007/s11042-024-18626-w). Impact Factor: 3.6. SCIE.
6. Surbhi Shaw and Ratna Dutta, Quantum Resistant Multi-user Signcryption scheme featuring Key Invisibility for Internet of Things. Journal of Information Security and Applications, Vol 76, 103549, Elsevier, 2023. <https://doi.org/10.1016/j.jisa.2023.103549>, Impact Factor: 5.6, Q1, SCIE.

7. Surbhi Shaw and Ratna Dutta, Forward secure offline assisted group key exchange from isogeny-based blinded key encapsulation mechanism. *IEEE Transactions on Information Theory*, Vol 69, Issue 7, pp. 4708-4722, IEEE 2023. **DOI:** [10.1109/TIT.2023.3260005](https://doi.org/10.1109/TIT.2023.3260005), Impact Factor: 2.5, Q1, SCIE.
8. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Short attribute-based signatures for arbitrary Turing machines from standard assumptions. *Designs, Codes and Cryptography*, Vol 91, pp. 1845-1872, Springer 2023. <https://doi.org/10.1007/s10623-022-01163-8>, Impact Factor: 1.6, Q1, SCIE.
9. Chinmoy Biswas, Ratna Dutta and Sumanta Sarkar, An Efficient Post-Quantum Secure Dynamic EPID Signature Scheme using Lattices, *Multimedia Tools and Applications*, Springer, 2023. <https://doi.org/10.1007/s11042-023-15737-8>, Impact Factor: 3.6, Q2, SCIE.
10. Jayashree Dey and Ratna Dutta, Progress in Multivariate Cryptography: Systematic Review, Challenges and Research Directions. *ACM Computing Surveys*, Vol 55, Issue 12, Article no. 246, pp. 1-34, ACM, 2022. <https://doi.org/10.1145/3571071>, Impact Factor : 16.6, Q1, SCIE.
11. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay, Communication-friendly Threshold Trapdoor Function from Weaker Assumption for Distributed Cryptography. *Annals of Telecommunications*, Vol. 78, pp. 221-233, Springer, 2022. <https://doi.org/10.1007/s12243-022-00937-4>, Impact Factor : 1.9, Q2, SCIE.
12. Amit Kumar Singh, Kamallesh Acharya and Ratna Dutta, Cloud Assisted Semi-static Secure Accountable Authority Identity-based Broadcast Encryption Featuring Public Traceability without Random Oracles. *Annals of Telecommunications*, Vol 78, pp. 79-90, Springer, 2022. <https://doi.org/10.1007/s12243-022-00925-8>, Impact Factor : 1.9, Q2, SCIE.
13. Jayashree Dey and Ratna Dutta, Post-quantum Secure Fully-dynamic Logarithmic-size Deniable Group Signature in Code-based Setting, *Advances in Mathematics of Communications*, American Institute of Mathematical Sciences, 2022. doi: 10.3934/amc.2022077, Impact Factor : 0.9, Q2, SCIE.
14. Surbhi Shaw and Ratna Dutta, Post-quantum secure Id-based identification and identity-based signature achieving forward secrecy. *Journal of Information Security and Applications*, Vol 69, 103275, Elsevier, July 2022. <https://doi.org/10.1016/j.jisa.2022.103275>, Impact Factor: 5.6, Q1, SCIE.
15. Chinmoy Biswas and Ratna Dutta, Secure and Efficient Multi-Key FHE Scheme Supporting Multi-bit Messages from LWE Preserving Non-Interactive Decryption. *Journal of Ambient Intelligence and Humanized Computing*, Springer, 2022. doi: 10.1007/s12652-022-03864-3, Impact Factor: 3.662, Q1
16. Mriganka Mandal, Ratna Dutta, Identity-Based Outsider Anonymous Cloud Data Outsourcing with Simultaneous Individual Transmission for IoT Environment. *Journal of Information Security and Applications*, Vol. 60, 102870, Elsevier, 2021. <https://doi.org/10.1016/j.jisa.2021.102870>, Impact Factor: 5.6, Q1, SCIE.
17. Meenakshi Kansal, Amit Kumar Singh, and Ratna Dutta, Efficient Multi-Signature Scheme using Lattice. *Comput. J.* 65(9): 2421-2429, Oxford Academic, 2021. doi: 10.1093/comjnl/bxab077, Impact Factor: 1.4, Q2, SCIE.
18. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay, Lattice based Nominative Signature using Pseudorandom Function. *IET Inf. Secur.* 15(4): 317-332, Wiley, 2021. doi: 10.1049/ise2.12022, Impact Factor : 1.4, Q2, SCIE.
19. Chinmoy Biswas and Ratna Dutta, Dynamic Multi-Key FHE in Symmetric Key Setting from LWE without using Common Reference Matrix. *Journal of Ambient Intelligence and*

- Humanized Computing, Vol 13, pages 1241-1254, Springer, 2021. <https://doi.org/10.1007/s12652-021-02980-w>, Impact Factor: 3.662, Q1
20. Kamalesh Acharya and Ratna Dutta, Constructing Provable Secure Broadcast Encryption Scheme with Dealership. *Journal of Information Security and Applications*, Vol. 58, 102736, Elsevier, 2020. <https://doi.org/10.1016/j.jisa.2020.102736>, Impact Factor: 5.6, Q1, SCIE.
 21. Kamalesh Acharya and Ratna Dutta, Ternary Subset Difference Revocation in Public Key Framework Supporting Outsider Anonymity. *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, pages 2183-2206, Springer, 2020. doi: 10.1007/s12652-020-02319-x, Impact factor: 3.662, Q1
 22. Chinmoy Biswas and Ratna Dutta, Implementation of Key Predistribution Scheme in WSN based on Binary Goppa Codes and Reed Solomon Codes with Enhanced Connectivity and Resiliency. *Journal of Ambient Intelligence and Humanized Computing*, Vol 14, pp. 5801-5816 Springer, 2023 (accepted in 2020). doi:10.1007/s12652-020-01869-4, Impact factor: 3.662, Q1
 23. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay, Group Signature from Lattices preserving Forward Security in Dynamic setting. *Advances in Mathematics of Communications* 14(4), pp. 535-553, American Institute of Mathematical Sciences, 2020. doi: 10.3934/amc.2020027, 2020. Impact factor: 0.9, Q2, SCIE.
 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, Vol. 48, 2019. <https://doi.org/10.1016/j.jisa.2019.06.009>, Impact factor: 5.6, Q1, SCIE.
 25. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Constrained Pseudorandom Functions for Turing Machines Revisited: How to Achieve Verifiability and Key Delegation. *Algorithmica* 81(9), pp. 3245-3390, Springer, 2019. <https://doi.org/10.1007/s00453-019-00576-7>, Impact factor: 1.1, Q1, SCIE.
 26. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Functional Signcryption. *Journal of Information Security and Applications*, Vol. 42, pp. 118-134, Elsevier, 2018. <https://doi.org/10.1016/j.jisa.2018.08.004>, Impact factor: 5.6, Q1, SCIE.
 27. 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. <https://doi.org/10.1016/j.tcs.2016.12.030>, Impact factor: 1.1, Q2, SCIE.
 28. Pratish Datta, Ratna Dutta and Sourav Mukhopadhyay, Strongly Full-Hiding Inner Product Encryption. *Theoretical Computer Science (TCS)*, Vol. 667, pp. 16-50, Elsevier, 2017. <https://doi.org/10.1016/j.tcs.2016.12.024>, Impact factor: 1.1, Q2, SCIE.
 29. 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. <https://doi.org/10.1016/j.ins.2016.07.039>, Impact factor: 8.1, Q1, SCI.
 30. 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. <https://doi.org/10.1080/00207160.2015.1037838>, Impact factor: 1.97, Q2, SCIE.
 31. 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. Impact factor: 2.53, Q2
 32. 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. Impact factor: 2.53, Q2

33. 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. Impact factor: 3.2, Q2, SCIE.
34. 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. Impact factor: 2.53, Q2
35. 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. Impact factor: 5.6, Q1, SCIE.
36. Vandana Guleria and Ratna Dutta, Universally Composable Issuer-Free Adaptive Oblivious Transfer with Access Policy. In *Security and Communication Networks*, Vol. 8, NO. 18, pp. 3615-3683, Wiley, 2015. Impact factor: 2.53, Q2
37. 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.
38. 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. Impact factor: 2.2, Q2, SCIE.
39. 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. Impact factor: 2.2, Q2, SCIE
40. 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. Impact factor: 0.45
41. 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. Impact factor: 0.45
42. 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. Impact factor: 0.45
43. 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. Impact factor: 4.8, Q1, SCIE.
44. 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. Impact factor: 4.8, Q1, SCIE.
45. 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. Impact factor: 0.63
46. 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. Impact factor: 2.5, Q1, SCIE.
47. 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. Impact factor:1.494

48. 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>. Impact factor:0.64, Q2

Conference:

1. Pratima Jana and Ratna Dutta: CPAKE : An Identity-binding Password Authenticated Key Exchange from Quasi-Cyclic Codes. In the Proceedings of the 25th International Conference on Cryptology in India (Indocrypt 2024), LNCS 15496, pp. 180-200, Springer-Verlag, Chennai, India, 18 - 21 December, 2024.
2. Pratima Jana, Ratna Dutta: Quantum Safe Computation-friendly Identity-binding Password Authenticated Key Exchanges. In the Proceedings of the 18th International Conference on Provable and Practical Security (ProvSec 2024), LNCS 14904, pp. 298-309, Springer-Verlag, Gold Coast, Australia, 25 - 27 September, 2024.
3. Anushree Belel and Ratna Dutta: Attribute-Based Inner Product Functional Encryption in Key-Policy Setting from Pairing. In the proceeding of the 19th International Workshop on Security (IWSEC 2024), Springer-Verlag, LNCS 14977, pp. 101-121 Kyoto, Japan, September 17-19, 2024.
4. Pratima Jana, Surbhi Shaw and Ratna Dutta: Compact Adaptor Signature from Isogenies with Enhanced Security. In the Proceeding of the 23th International Conference on Cryptology and Network Security (CANS 2024), Springer-Verlag, LNCS 14905, pp. 77-100, University of Cambridge, UK, 24-27 September, 2024.
5. Surbhi Shaw and Ratna Dutta: Compact Identity-based Signature and Puncturable Signature from SQISign. In the Proceeding of the 26th Annual International Conference on Information Security and Cryptology (ICISC 2023), LNCS 14561, pp. 282-305, Springer-Verlag, Seoul, Korea, 2023.
6. Surbhi Shaw and Ratna Dutta: Compact Stateful Deterministic Wallet from Isogeny-based Signature featuring Uniquely Rerandomizable Public Keys. In the Proceeding of the 22nd International Conference on Cryptology and Network Security (CANS 2023), LNCS 14342, pp. 392-413, Springer-Verlag, October 31st to November 2nd, 2023, Augusta, Georgia, USA.
7. 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 14310, pp. 274-288, Springer-Verlag, 2-4 October 2023, New Jersey, USA.
8. Pratima Jana and Ratna Dutta: Post-quantum Secure Stateful Deterministic Wallet from Code-based Signature featuring Uniquely Rerandomized Keys. In the Proceeding of the 25th International Symposium on Stabilization, Safety and Security of Distributed Systems (SSS 2023), LNCS 14310, pp. 568-582, Springer-Verlag, 2-4 October 2023, New Jersey, USA.
9. 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 13809, pp. 102-116,

Bucharest, Romania, Springer-Verlag, 8-9 December, 2022.

https://doi.org/10.1007/978-3-031-32636-3_6

10. Jayashree Dey and Ratna Dutta: Code-based Key Encapsulation Mechanism Preserving Short Ciphertext and Secret key. In the Proceeding of the 19th International Conference on Security and Cryptography (SECRYPT 2022), Vol 1, pp. 349-356, Lisbon, Portugal, July 11-13, 2022. DOI: 10.5220/0011273900003283
11. 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), Vol 1, pp. 374-381, Lisbon, Portugal, July 11-13, 2022. DOI: 10.5220/0011271600003283
12. Anushree Belel, Ratna Dutta and Sourav Mukhopadhyay: Trapdoor Function from Weaker Assumption in the Standard Model for Decentralized Network. In the proceedingd of thr 8th International Cryptology and Information Security Conference 2022 (CRYPTOLOGY2022), Port Dickson, Malaysia, July 26-28, 2022.
13. 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 Third International Conference on Emerging Information Security and Applications (EISA 2022), Communications in Computer and Information Science, Vol. 1641, pp. 108-125, Wuhan, China, 29-30 October, 2022.
https://doi.org/10.1007/978-3-031-23098-1_7
14. Surbhi Shaw and Ratna Dutta: Key-oblivious encryption from isogenies with application to accountable tracing signature. In the Proceeding of 22nd International Conference on Cryptology in India (Indocrypt 2021), LNCS 13143, pp. 362-386, Springer-Verlag, Jaipur, India, 13-15 December, 2021.
15. Surbhi Shaw and Ratna Dutta: Identification Scheme and Forward-Secure Signature in Identity-Based Setting from Isogenies. In the Proceedings of the 15th International Conference on Provable and Practical Security (ProvSec 2021), LNCS 13059, pp. 309-326, Springer-Verlag, Guangzhou, China, 5 - 8 November, 2021.
16. Subhranil Dutta, Tapas Pal and Ratna Dutta: Fully Secure Unbounded Zero Inner Product Encryption with Short Ciphertexts and Keys. In the Proceedings of the 15th International Conference on Provable and Practical Security (ProvSec 2021), LNCS 13059, pp. 241-258, Springer-Verlag, Guangzhou, China, 5 - 8 November, 2021.
17. Ratna Dutta, Sumit Kumar Debnath and Chinmoy Biswas: Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem. In the Proceeding of the 18th International Conference on Security and Cryptography (SECRYPT 2021), July 6-8, 2021.
18. Tapas Pal, Ratna Dutta: Chosen Ciphertext Secure Functional Encryption from Constrained Witness PRF. In the Proceedings of the 26th Australasian Conference on Information Security and Privacy (ACISP 2021), LNCS 13083, pp. 254-274, Springer-Verlag, Perth, Australia, December 1-3, 2021.
19. Tapas Pal, Ratna Dutta: CCA Secure Attribute-Hiding Inner Product Encryption from Minimal Assumption. In the Proceedings of the 26th Australasian Conference on Information Security and Privacy (ACISP 2021), LNCS 13083, pp. 24-45, Springer-Verlag, Perth, Australia, December 1-3, 2021.
20. Tapas Pal and Ratna Dutta: Attribute-Based Access Control for Inner Product Functional Encryption from LWE. In the Proceedings of the 7th International Conference on Cryptology and Information Security in Latin America (Latincrypt 2021), LNCS 12912, pp. 127-148, Springer-Verlag, Bogota, October 6-8, 2021.

21. Tapas Pal, Ratna Dutta: Chosen-Ciphertext Secure Multi-Identity and Multi-Attribute Pure FHE. In the Proceeding of the 19th International Conference on Cryptology and Network Security (CANS 2020), LNCS 12579, pp. 387-408, Springer-Verlag, Vienna, Austria, 2020.
22. Tapas Pal, Ratna Dutta: Semi-Adaptively Secure Offline Witness Encryption from Puncturable Witness PRF. In the Proceeding of the 14th International Conference on Provable and Practical Security (Provsec 2020), LNCS 12505, pp. 169-189, Springer-Verlag, Singapore, 2020.
23. Meenakshi Kansal and Ratna Dutta: Round Optimal Secure Multisignature Schemes from Lattice with Public Key Aggregation and Signature Compression. In the Proceeding of the 12th International Conference on Cryptology, AFRICACRYPT 2020, LNCS 12174, pp. 281-300, Springer-Verlag, Cairo, Egypt, 2020.
24. 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 11975, pp 175-193, Springer-Verlag, Seoul, Korea, 2019.
25. 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.
26. Tapas Pal, Ratna Dutta.: Offline Witness Encryption from Witness PRF and Randomized Encoding in CRS model. In the Proceedings of the 24th Australasian Conference on Information Security and Privacy (ACISP 2019), LNCS 11547, pp. 78-96, Springer-Verlag, Christchurch, New Zealand, 2019.
27. Meenakshi Kansal, Ratna Dutta and Sourav Mukhopadhyay: Construction for a Nominative Signature Scheme from Lattice with Enhanced Security. In the Proceedings of International Conference on Codes, Cryptology and Information Security (C2SI 2019), LNCS 11445, pp. 72-91, Springer-Verlag, Rabat – Morocco, 2019.
28. Kamallesh 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 11124, pp. 495-515, Springer-Verlag, Naples, Italy, 2018.
29. 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 11449, pp. 468-489, Springer-Verlag, Fuzhou, China, 2018.
30. 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.
31. Kamallesh 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 10779, pp. 191-213, Springer-Verlag, Seoul, Korea, 2017.
32. Kamallesh 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.
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** 10175, pp. 463-493, Springer-Verlag, Amsterdam, The Netherlands, 2017.
34. 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.
 35. 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.
 36. 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.
 37. 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.
 38. 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.
 39. 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.
 40. 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.
 41. 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.
 42. 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.
 43. 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.
 44. 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.
 45. 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.

46. 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.
47. 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.
48. 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.
49. 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.
50. 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.
51. 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.
52. 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.
53. 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.
54. 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.
55. 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.
56. 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.
57. 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>.
58. 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.
59. 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.
 60. 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.
 61. 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.
 62. 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.
 63. 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.
 64. 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.
 65. 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.
 66. 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.
 67. 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.
 68. 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.
 69. 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.
 70. 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.
 71. 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.
 72. 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.

73. 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.
74. 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.
75. 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.
76. 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.
77. 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.
78. 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.
79. 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.
80. 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.
81. 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.
82. Ratna Dutta and Sourav Mukhopadhyay, 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 Communications Society Press**, 2007.
83. 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.
84. 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.
85. 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.
86. Ratna Dutta and Rana Barua, Constant Round Dynamic Group Key Agreement. In proceedings of ISC'05, **LNCS** 3650, pp. 74-88, Springer-Verlag, 2005.

87. 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>.
88. 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>.
89. 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. [Nabanita Chakraborty](#), Ratna Dutta: Identity-Based Ring Signature from Quantum Token. *IACR Cryptol. ePrint Arch. 2025*: 788 (2025)
2. [Pratima Jana](#), Ratna Dutta: UPKE and UKEM Schemes from Supersingular Isogenies. *IACR Cryptol. ePrint Arch. 2025*: 1010 (2025)
3. [Maria Leslie](#), Ratna Dutta: A Traceable Threshold Asmuth-Bloom Secret Sharing Scheme. *IACR Cryptol. ePrint Arch. 2025*: 1561 (2025)
4. Tapas Pal, Ratna Dutta: Attribute-Based Access Control for Inner Product Functional Encryption from LWE. *IACR Cryptol. ePrint Arch. 2021*: 178 (2021)
5. [Surbhi Shaw](#), Ratna Dutta: Key-Oblivious Encryption from isogenies and its application to Accountable Tracing Signatures. *IACR Cryptol. ePrint Arch. 2021*: 494 (2021)
6. Tapas Pal, Ratna Dutta: Chosen Ciphertext Secure Functional Encryption from Constrained Witness PRF. *IACR Cryptol. ePrint Arch. 2021*: 512 (2021)
7. [Jayashree Dey](#), Ratna Dutta: Secure Code-Based Key Encapsulation Mechanism with Short Ciphertext and Secret Key. *IACR Cryptol. ePrint Arch. 2021*: 881 (2021)
8. [Chinmoy Biswas](#), Ratna Dutta: Secure and Efficient Multi-Key FHE Scheme Supporting Multi-bit Messages from LWE Preserving Non-Interactive Decryption. *IACR Cryptol. ePrint Arch. 2021*: 1431 (2021)
9. Tapas Pal, Ratna Dutta: Chosen-Ciphertext Secure Multi-Identity and Multi-Attribute Pure FHE. *IACR Cryptol. ePrint Arch. 2020*: 1382 (2020)
10. Tapas Pal, Ratna Dutta: Puncturable Witness Pseudorandom Functions and its Applications on Witness Encryption. *IACR Cryptol. ePrint Arch. 2020*: 479 (2020)
11. Tapas Pal, Ratna Dutta: Chosen-Ciphertext Secure Attribute-Hiding Non-Zero Inner Product Encryptions and Its Applications. *IACR Cryptol. ePrint Arch. 2020*: 1085 (2020)
12. Tapas Pal, Ratna Dutta: Non-zero Inner Product Encryptions: Strong Security under Standard Assumptions. *IACR Cryptol. ePrint Arch. 2019*: 817 (2019)

13. Meenakshi Kansal, Ratna Dutta, Sourav Mukhopadhyay: Efficient Construction of Nominative Signature Secure under Symmetric Key Primitives and Standard Assumptions on Lattice. IACR Cryptol. ePrint Arch. 2019: 1232 (2019)
14. Jayashree Dey, Ratna Dutta: Secure Key Encapsulation Mechanism with Compact Ciphertext and Public Key from Generalized Srivastava code. IACR Cryptol. ePrint Arch. 2019: 1388 (2019)
15. Mriganka Mandal, Ratna Dutta: Cost-Effective Private Linear Key Agreement With Adaptive CCA Security from Prime Order Multilinear Maps and Tracing Traitors. IACR Cryptol. ePrint Arch. 2018: 508 (2018)
16. Tapas Pal, Ratna Dutta: Constructing Witness PRF and Offline Witness Encryption Without Multilinear Maps. IACR Cryptol. ePrint Arch. 2018: 587 (2018)
17. Vandana Guleria, Ratna Dutta: UC Secure Issuer-Free Adaptive Oblivious Transfer with Hidden Access Policy. CoRR abs/1711.10751 (2017)
18. Kamalesh Acharya, Ratna Dutta: Adaptively Secure Recipient Revocable Broadcast Encryption with Constant size Ciphertext. IACR Cryptol. ePrint Arch. 2017: 59 (2017)
19. Kamalesh Acharya, Ratna Dutta: Enhanced Outsider-anonymous Broadcast Encryption with Subset Difference Revocation. IACR Cryptol. ePrint Arch. 2017: 265 (2017)
20. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Attribute-Based Signatures for Turing Machines. IACR Cryptol. ePrint Arch. 2017: 801 (2017)
21. Meenakshi Kansal, Ratna Dutta, Sourav Mukhopadhyay: Forward Secure Efficient Group Signature in Dynamic Setting using Lattices. IACR Cryptol. ePrint Arch. 2017: 1128 (2017)
22. Sumit Kumar Debnath, Ratna Dutta: Fair mPSI and mPSI-CA: Efficient Constructions in Prime Order Groups with Security in the Standard Model against Malicious Adversary. IACR Cryptol. ePrint Arch. 2016: 216 (2016)
23. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Verifiable and Delegatable Constrained Pseudorandom Functions for Unconstrained Inputs. IACR Cryptol. ePrint Arch. 2016: 784 (2016)
24. Kamalesh Acharya, Ratna Dutta: Secure and Efficient Construction of Broadcast Encryption with Dealership. IACR Cryptol. ePrint Arch. 2016: 844 (2016)
25. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Succinct Predicate and Online-Offline Multi-Input Inner Product Encryptions under Standard Static Assumptions. IACR Cryptol. ePrint Arch. 2016: 904 (2016)
26. Sumit Kumar Debnath, Ratna Dutta: How to Meet Big Data When Private Set Intersection Realizes Constant Communication Complexity. IACR Cryptol. ePrint Arch. 2016: 1180 (2016)
27. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Fully Secure Unbounded Revocable Attribute-Based Encryption in Prime Order Bilinear Groups via Subset Difference Method. IACR Cryptol. ePrint Arch. 2015: 293 (2015)
28. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: General Circuit Realizing Compact Revocable Attribute-Based Encryption from Multilinear Maps. IACR Cryptol. ePrint Arch. 2015: 884 (2015)
29. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Functional Signcryption: Notion, Construction, and Applications. IACR Cryptol. ePrint Arch. 2015: 913 (2015)
30. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Compact Attribute-Based Encryption and Signcryption for General Circuits from Multilinear Maps. IACR Cryptol. ePrint Arch. 2015: 1188 (2015)
31. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Functional Encryption for Inner Product with Full Function Privacy. IACR Cryptol. ePrint Arch. 2015: 1255 (2015)

32. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Universally Composable Efficient Priced Oblivious Transfer from a Flexible Membership Encryption. IACR Cryptol. ePrint Arch. 2014: 584 (2014)
33. Pratish Datta, Ratna Dutta, Sourav Mukhopadhyay: Fully Secure Self-Updatable Encryption in Prime Order Bilinear Groups. IACR Cryptol. ePrint Arch. 2014: 940 (2014)
34. Ratna Dutta, Sugata Sanyal: Collusion resistant self-healing key distribution in mobile wireless networks. CoRR abs/1206.6285 (2012)
35. Ratna Dutta, Rana Barua: Dynamic Group Key Agreement in Tree-Based Setting. IACR Cryptol. ePrint Arch. 2005: 131 (2005)
36. Ratna Dutta, Rana Barua: Constant Round Dynamic Group Key Agreement. IACR Cryptol. ePrint Arch. 2005: 221 (2005)
37. Ratna Dutta, Rana Barua, Palash Sarkar: Provably Secure Authenticated Tree Based Group Key Agreement Protocol. IACR Cryptol. ePrint Arch. 2004: 90 (2004)
38. Rana Barua, Ratna Dutta, Palash Sarkar: Extending Joux's Protocol to Multi Party Key Agreement. IACR Cryptol. ePrint Arch. 2003: 62 (2003)
39. Ratna Dutta and Rana Barua, Group Key Agreement Immune to Dictionary Attacks. In proceedings of National Workshop on Cryptology 2005, Shimoga, India, August 2005.
40. 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.
41. Ratna Dutta, [Rana Barua](#), [Palash Sarkar](#): Pairing-Based Cryptographic Protocols : A Survey. [IACR Cryptol. ePrint Arch. 2004](#): 64 (2004)
42. Ratna Dutta, [Rana Barua](#): Overview of Key Agreement Protocols. [IACR Cryptol. ePrint Arch. 2005](#): 289 (2005)

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 Fast 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 and Multivariate Cryptosystems from Hidden Field Equations	Mathematical Research Impact Centric Support (MATRICS) to the Science and Engineering Research Board (SERB)	Rs. 6.60 Lakhs	2021	Complete
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	Complete
8	Principal Investigator	Quantum Resistant Cryptographic Protocols for Cloud computing	ISRO, IIT Kharagpur CELL Space Technology Cell	Rs. 23.76 Lakhs	2022	In progress
9	Co-Investigator	Cryptographic hash algorithm based on quantum paradigm	ARQANUM TECHNOLOGIES PRIVATE LIMITED	Rs. 53.1 Lakhs	2023	Complete
10	Principal Investigator	Development of QVPN	The Indian ARMY	Rs. 150 Lakhs	2023	In progress
11	Co-Investigator	Towards designing cryptographic primitives to support secure decentralized protocols	CSIR	Rs. 15.16 Lakhs	2023	In progress
12	Principal Investigator	Design and analysis of post-quantum cryptographic primitives from error correcting codes	Core Research Grant to the Science and Engineering Research Board (SERB)		2023	Approved
13	Principal Investigator	Construction of Privacy Preserving Cryptographic Protocols for Blockchain based applications in Military and Defence Organizations	DRDO under the Vertical: Cognitive Technologies		2025	Lab Approved, GC Approved, Financial sanction pending

C. Conferences Attended

- Invited talk on Post-quantum cryptography- Lattice-based approach in the National Symposium on Mathematical Innovations for Industrial Advancement (NSMIIA 2025), BIT Mesra, Ranchi, India, August 8-10, 2025
- Invited talk on Lattice-based cryptography in the Workshop on Post Quantum Cryptography II, IIT (ISM) Dhanbad, India, in virtual/online mode, June 25-28, 2025
- Invited lecture series on Post-quantum cryptography in the Lodha Genius Programme 2025, Ashoka University, Haryana, India, June 1-10, 2024
- Chair a session in the 25th International Conference on Cryptology in India (INDOCRYPT'24) held in Chennai, India, December 18-21, 2024
- Invited to attend the 30th International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt 2024) held in Kolkata, India, December 9-13, 2024
- Invited talk on Post-Quantum Secure MFHE and IPFE in unbounded setting for Untrusted Cloud Environment – Instantiation and Implementation in the International Conference on Security and Privacy (ICSP - 2024), NIT, Jamshedpur, India, November 20-21, 2024
- Invited talk on Isogeny-based Cryptography in the International Conference on Recent Advances in Mathematics and Data Science (ICRAMDS - 2024), MNIT, Bhopal, India, June 27-28, 2024
- Invited to the C.R.Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS), Hederabad, India, June 10, 2024
- Invited to the Center for Security, Theory and Algorithms (CSTAR), IIIT Hederabad, India, June 8, 2024
- Invited talk on Isogeny-based Cryptography in the Society for Electronic Transactions and Security (SETS), Chennai, India, May 06, 2024
- Invited to the Department of Computer Science and Engineering, IIT-Roorkee India, May 16-20, 2024
- Invited talk on Quantum Resistant Cryptographic Protocols for Cloud Computing at SAC Annual Sponsored ReseArch Review (SAC-ASAR) 2023, ISRO, Ahmedabad, India, in virtual/online mode, November 20-November 24, 2023
- Invited talk on Post-Quantum Cryptography in the International Workshop on Quantum Algorithms, Machine Learning and Control at School of Engineering, Trinity College Dublin (TCD), Dublin, in virtual/online mode, June 22-23, 2023
- Invited talk on Post-Quantum Cryptography in 2 days Workshop on Computer Networks and Security at Department of Computer Science and Engineering, Sri Jayachamarajendra College of Engineering, JSS Science and Technology University, Mysuru, India, June 1-2, 2023
- Invited talk on Quantum Resistant Cryptographic Protocols for Cloud Computing at SAC Annual

Sponsored ReseArch Review (SAC-ASAR) 2022, ISRO, Ahmedabad, India, in virtual/online mode, November 9-November 22, 2022

- Invited talk on Post-quantum cryptography in the Online Workshop on High Performance Computing with Application to AI and Cryptography, Organized by IIT Kharagpur and National Technological Research Organization Under the aegis of National Supercomputing Mission Kharagpur, India, in virtual/online mode, September 8, 2022
- Invited talk on Post-quantum cryptography in the C-DAC Technology Conclave (Quantum computing session), Pune, India, in virtual/online mode, July 28-29, 2021
- Invited talk on Quantum Resistant Cryptographic Protocols for Cloud Computing at SAC Annual Sponsored ReseArch Review (SAC-ASAR) 2021, ISRO, Ahmedabad, India, in virtual/online mode, November 23-December 2, 2021
- Invited talk on Lattice-based Cryptosystems in the International Conference on Security & Privacy (ICSP 2020) organized by NIT-Jamsedpur, India, in virtual/online mode, November 05-06, 2020
- Invited talk on Isogeny-based Cryptosystems in the webinar organized by the Department of Mathematics, Abhedananada Mahavidyalaya, Sainthia, Birbhm, September 14-15, 2020
- Invited Talk on Presented progress in Group Monitoring Workshop (GMW) of SERB PAC (MS), IIT Madras, India, March 2020
- Invited talk on Post-Quantum Cryptography at IIT Madras, India, March 2020
- Invited talk on Multivariate Cryptosystems at Chennai Mathematical Institute (CMI), India, March 2020
- 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
- Invited to attend the 3rd International Conference on Cryptology in India (INDOCRYPT'02) held in Hyderabad, India, December 2002
- Invited to attend the 6th International Conference on Cryptology in India (INDOCRYPT'05) held in Indian Institute of Science (IISc), Bangalore, India, December 2005

- Invited to attend the 11th Annual International Conference on the Theory and Application of Cryptology & Information Security (ASIACRYPT'05) held in Chennai, India, December 2005
- Invited talk on “Elliptic curve public key cryptosystems and pairings” in the LACS Seminar held in University of Luxembourg, Luxembourg, May 2006
- Invited to attend the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS'07) held in Singapore, March 2007
- Invited talk on “Key agreements protocols” in the staff seminar held in National University of Ireland, Maynooth, April 2008
- Invited talk 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
- Invited to attend Kick-Off Meeting of ECRYPT II held in Katholieke Universiteit Leuven, Belgium, November 2008
- Invited to attend 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 Limpstersberg, 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 set intersection
- Obfuscation: constructions and applications
- Multilinear maps and their applications
- Lattice-based cryptography
- Code-based cryptography
- Multivariate public-key cryptosystem
- Isogeny-based cryptography
- Financial cryptography for sharing economy

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: changeec@comp.nus.edu.sg