1. **Full name of the faculty member: Professor Dr. Avishek Adhikari**
2. **Designation: Professor and HOD, Department of Mathematics, Presidency University, Kolkata, India.**
3. **Specialization:** Cryptography, Cryptanalysis of Stream Ciphers and Block Ciphers, Secret Sharing, Quantum Cryptography, Algebra, Graph Theory.
4. **Photograph:**

Brief Introduction: **Professor Dr. AVISHEK ADHIKARI,** M.Sc. **(Gold Medalist)**, a recipient of the **President of India Medal, ISCA Young Scientist Award and NANUM** fund by **International Mathematical Union (IMU), received his** PhD Degree from **Indian Statistical Institute** under the supervision of the former **Director of Indian Statistical Institute and Padma Shree** Awardee **Professor Bimal Roy. Currently Dr Adhikari is a Professor and HOD at the Department of Mathematics, Presidency University, Kolkata.** He was a faculty member at the **Department of Pure Mathematics, University of Calcutta** (July 7, 2006 to January 16, 2019). He is the **founder secretary of IMBIC, India. He was the former Treasurer of Cryptology Research Society of India (2008-2024), Former Eastern Zonal Coordinator for NBHM MSc and PhD Scholarship Examination**, and former member of the NBHM regional library committee (Eastern Region). He was a Post-Doctoral fellow at **INRIA-Rocquencourt, France**, a visiting scientist at **Linkoping University, Sweden** and a visiting scientist at **Indian Statistical Institute, Kolkata**. He visited **Japan (7 times, funded by JSPS, Japan and JST, Japan), Sweden (3 times), France (2 times), England (3 times), Switzerland (2 times), South Korea, Russia, Malaysia (2 times), Thailand, Denmark, Norway, Netherland, Belgium, Italy, Bangladesh, Singapore**. He has published **six basic textbooks** on mathematics including **Basic Modern Algebra with Applications (Springer, 2014), Basic Topology, Vol 1 (Springer, 2022) and Basic Topology, Vol 2 (Springer, 2022)** and edited two research monographs including **Springer Monograph (2017) on Mathematical and Statistical Applications in Life Sciences and Engineering**. He has published more than 70 research articles in reputed international journals, conference proceedings and contributed volumes. He is on the editorial board of several journals. He is one of the investigators of **12** Sponsored Research Projects funded by the agencies like **DRDO, WESEE (Ministry of Defense), DST-SERB, DIT, NBHM** including two International Collaborative Projects supported by **DST-JSPS (Indo-Japan Project) and DST-JST (Indo-Japan) in collaboration with Indian Statistical Institute. Ten** of his PhD students have already obtained Ph.D. Degree.

Three of the Ph.D. scholars are doing their research works under his supervision. He was the **Program Chair of the 22nd International Conference Indocrypt 2021.**

5. Contact information:

Office Address: Department of Mathematics, Presidency University, Kolkata, 86/1 College Street Road, Kolkata 700073, West Bengal, India.
Residential Address: AH 317, Salt Lake, Sector 2, Kolkata 700091, West Bengal, India
e-mail id: avishek.maths@presiuniv.ac.in **&** avishek.adh@gmail.com
website: http://presiuniv.ac.in/web/staff.php?staffid=424

6. Academic qualifications

College/University from which the degree was obtained	Abbreviation of the degree
St. Xavier's College, Kolkata	B.Sc. in Mathematics Hons. **(Stood 2nd in University of Calcutta)** [1999]
Department of Pure Mathematics, Calcutta University	M.Sc. in Pure Mathematics, **Gold Medalist (Stood 1st) [2001]**
Indian Statistical Institute	Ph.D. [2004] under the Supervision of **Professor Bimal Roy, Former Director,** Indian Statistical Institute.

7. Positions held/holding:

1. **Head of the Department of Mathematics, Presidency University, November 1, 2021-till date**
2. **Professor, Department of Mathematics, Presidency University, January 17, 2019-till date**
3. **Assistant Professor, Department of Pure Mathematics, University of Calcutta, July 7, 2006 to January 16, 2019.**
4. **Visiting Scientist, Linkoping University, Sweden, April 2006-June 2006.**
5. **Visiting Scientist, Indian Statistical Institute, December 2005-March 2006.**
6. **Post Doctoral Fellow, INRIA, France, December 2004-December 2005.**
7. **Research Fellow, Indian Statistical Institute, 2001-2004.**

8. Research guidance:

I. Number of scholars awarded **Ph.D. degrees** under my supervision: **10**

I. **Dr Angsuman Das,** *On Some Mathematical Aspects of Security Notions and Constructions of Public Key Cryptosystems and Secret Sharing Schemes***, Degree Awarded in 2014.**

II. **Dr Partha Sarathi Roy,** *On Some Aspects of Secret Sharing Schemes and Oblivious Transfer Protocols Using Mathematical Tools***, Degree Awarded in 2015.**

III. **Dr Sabyasachi Dutta,** *Algebraic And Combinatorial Aspects Of Visual Cryptography***, Degree Awarded in 2016.**

IV. **Dr Ushnish Sarkar,** *On Some Combinatorial Studies of Radio k-coloring Problems of Graphs and Related Issues*, **Degree Awarded in 2017.**

V. **Dr Prakash Dey,** *Algebraic Aspects Of Cryptanalysis On Secret-Key Cryptosystems***, Awarded in 2017.**

VI. **Dr Subarsha Banerjee,** *Spectra of Graphs on Various Algebraic Structures,* **Awarded in 2022.**
VII. **Dr. Jyotirmoy Pramanik,** *Fault Tolerance In Cryptographic Secret Sharing Using Algebraic Techniques,* **Awarded in 2022.**
VIII. **Dr. Kutubuddin Sardar,** *On Some Algebraic Aspects of Secret Image Sharing,* **Awarded in 2023.**
IX. **Dr. Sandip Kumar Mondal,** *Algebraic Aspects of Symmetric-Key Cryptosystems and Their Cryptanalysis,* **Awarded in 2024**.
X. **Dr. Chandan Goswami,** *Mathematical Aspects of Security and Privacy for Internet of Things (IoT)*, **Awarded in 2025.**

II. Currently Number of scholars Submitted Ph.D. Thesis: **0**

III. **Number of Postdoctoral Fellow: 1 (Dr Kumardipta Bose, NBHM Fellow, 2023-)**

IV. Number of researchers pursuing Ph.D. under my supervision: **3**

V. Number of researchers awarded M.Phil. : **1**

I. **Kabita Das,** *Review of some Black and White Visual Cryptographic Schemes for Threshold as well as for General Access Structures.*

9. Projects:

- ***Current projects:***
  i. **Coordinator** of the **DST-FIST Program supported by Department of Science and Technology, Government of India**, for 5 years at the Department of Mathematics, Presidency University, Kolkata, Budget: **Rs 66,00,000/-**

- ***Completed projects*:**
  i. **Principal Investigator of the MATRICS Research Grant for the Research Project entitled "Application of Algebra in Cryptanalysis of Polynomial Based Image Secret Sharing Schemes Under Different Adversarial Models: Few Efficient Remedies in Different Cheating Scenarios" funded by DST-SERB, for three years 2020-2023 with fund Rs 6,60,000/-**
  ii. **Co-Investigator** of the **DST-SERB s**ponsored Core Research Grant project entitled “A study on k-level metric bases for graphs: Theoretic and Algorithmic Approaches” **of Rs 25,69,831/-** for three years (2020-2023) in collaboration with Dr Laxman Saha of Balurghat College.

  iii. **Started the project as Principal Investigator** of the Research Project entitled Detection of an Unknown Stream Cipher and Recovery of its Embedded Keys Through Cryptanalysis of a Class of Iterative Ciphers Using Fault Analysis, of amount **Rs. 21, 24, 000/- for** 2 years from September 12, 2018 funded by DRDO, Ministry of Defense, **Government of India. After joining the Presidency University, Dr Avishek Adhikari become the Co-investigator of the project.**
  iv. **Principal-investigator** of the Research Project entitled Constructions and Analysis of Some Secret Sharing Schemes and Their Applications Using Mathematical and Statistical Tools, of amount **Rs. 13, 09, 900/- (= Rs 11,51,500/- + Rs 1,58,400/- HRA), for** 3 years from January, 2014, funded by

National Board of Higher Mathematics (NBHM), Department of Atomic Energy, Government of India.

v. Co-investigator of the Joint Research Project entitled "Analysis of Cryptographic Algorithms and Evaluation on Enhancing Network Security Based on Mathematical Science", of amount **Rs. 23.00 lakhs** , December 2008- December 2011, under Strategic **Japanese-Indian Cooperative Program supported by JST-DST project.**

vi. Principal Investigator of the Research Project of **Ministry of Communication and Information Technology, Govt. of India**, entitled "Secret Sharing Schemes using DNA Cryptography", of amount **Rs. 22.94 lakhs** at Department of Pure Mathematics, April 2007- March 2009.

vii. Co-investigator of the Joint Research Project entitled Design and development of Pseudo Random Number Generators for use in Key Generation Systems, of amount Rs**. 7.60 lakhs** for 180 days, 2010-2011, funded by **MINISTRY OF DEFENCE, Govt of India** in collaboration with CRYPTOLOGY RESEARCH SOCIETY OF INDIA (CRSI), Applied Statistics Unit, Indian Statistical Institute.

viii. Co-investigator of the Joint Research Project entitled Design and development of Strong Boolean functions with Cryptographic properties, of amount **Rs. 6.30 lakhs** for 180 days, 2010-2011, funded by **MINISTRY OF DEFENCE, Govt of India** in collaboration with CRYPTOLOGY RESEARCH SOCIETY OF INDIA (CRSI), Applied Statistics Unit, Indian Statistical Institute.

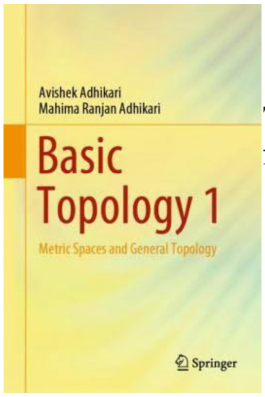
ix. Co-investigator of the Joint Research Project entitled Design and development of Resilient Key Management for Secure Symmetric Implementation, of amount **Rs. 8.75 lakhs**, for 180 days, 2010-2011, funded by **MINISTRY OF DEFENCE, Govt of India** in collaboration with CRYPTOLOGY RESEARCH SOCIETY OF INDIA (CRSI), Applied Statistics Unit, Indian Statistical Institute.

x. Co-investigator of the Joint Research Project entitled For Design and Development of Test Suite for Statistical Analysis of Cipher and Random Number Generators, of amount **Rs. 9.50 lakhs**, for 180 days from October, 2009, funded **by MINISTRY OF DEFENCE, Govt of India**, in collaboration with CRYPTOLOGY RESEARCH SOCIETY OF INDIA (CRSI), Applied Statistics Unit, Indian Statistical Institute.

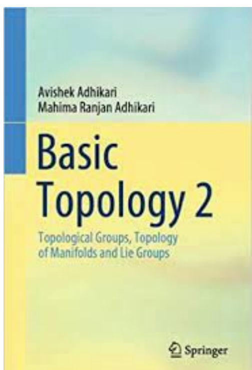
xi. Co-investigator of the Joint Research Project entitled “Computational Aspects of Mathematical Design and Analysis of Secure Communication Systems Based on Cryptographic Primitives”, of amount **Rs. 6.16 lakhs,** 2014-2016, **India-Japan Science Council supported by DST-JSPS Science and Technology Program i**n collaboration with **Indian Statistical Institute, Kolkata and Kyushu University, Japan.**

10. <u>Publications:</u>

A) Books:

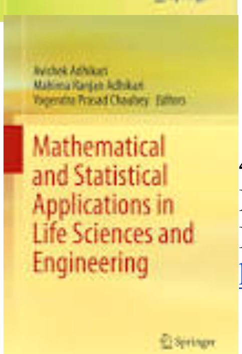


1. **(Avishek Adhikari & M R Adhikari), Basic Topology 1, Springer in 2022. For more details, please visit the website for more details: https://link.springer.com/book/9789811665080**

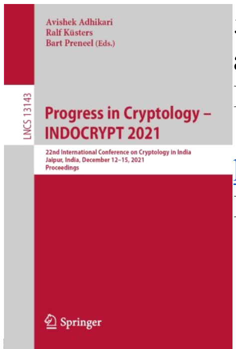


2. **<u>(Avishek Adhikari & M R Adhikari), Basic Topology 2, Springer in 2022. For more details, please visit the website for more details:</u> https://www.amazon.in/Basic-Topology-Topological-Groups-Manifolds/dp/9811665761**

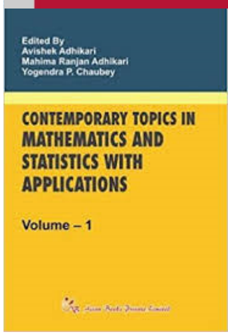
3. <u>(M R Adhikari **& Avishek Adhikari), Basic Modern Algebra with Applications, published by Springer. For more details, please visit the website for more details:**</u> **http://www.springer.com/in/book/9788132215981**



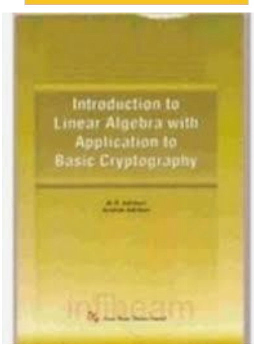
4. Edited Book, (**Avishek Adhikari,** M R Adhikari and Y. P. Chaubey), **Mathematical and Statistical Applications in Life Sciences and Engineering, Springer** in 2017, For more details, please visit the website: http://www.springer.com/in/book/9789811053696
ISBN 978-981-10-5370-2.



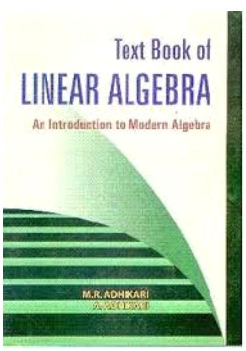
5. Edited Book, (**Avishek Adhikari,** Ralf Küsters and Bart Preneel), Progress in Cryptology – INDOCRYPT 2021 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021, Proceedings. For more details, please visit the website: https://link.springer.com/book/10.1007/978-3-030-92518-5?page=2
ISBN: 978-3-030-92518-5.



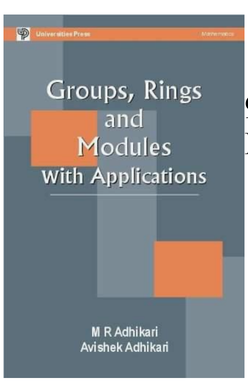
6. Edited Book: (**Avishek Adhikari and** M R Adhikari and Y P Chaubey), Contemporary Topics in Mathematics and Statistics with Applications, **Asian Books Private Limited,** 2012.



7. (**Avishek Adhikari and** M R Adhikari), Introduction to Linear Algebra with Application to Basic Cryptography, Asian Books Private Limited, 2007.



8. (**Avishek Adhikari and** M R Adhikari), Text Book of Linear Algebra : An Introduction to Modern Algebra, **Allied Publishers,** 2004.



9. (**Avishek Adhikari and** M R Adhikari), Groups, Rings and Modules with Applications, **Universities Press,** 2003.

B) Select list of publications:

a) Journals:

1. (with S. K. Mondal, P. Dey, H. S. Roy, and S. Maitra), "Improved Fault Analysis on Subterranean 2.0," in **IEEE Transactions on Computers**, **(Science Citation Index)** 2024, doi: 10.1109/TC.2024.3371784.

2. (with Roy, H.S., Dey, P., Mondal, S.K. et al.) Cryptanalysis of full round FUTURE with multiple biclique structures. **Peer-to-Peer Netw. Appl. (Science Citation Index Expanded)** 17, 397–409 (2024). https://doi.org/10.1007/s12083-023-01600-y

3. (with Mondal, S. K., Rahman, M., Sarkar, S.), Revisiting Yoyo Tricks on AES. **IACR Transactions on Symmetric Cryptology, 2**023(4), 28–57, **(Science Citation Index Expanded).** https://doi.org/10.46586/tosc.v2023.i4.28-57

4. (with Satyam Kumar, Sandip Kumar Mondal, Santanu Sarkar, Takanori Isobe, Anubhab Baksi), Restricted near collision attack on Plantlet. J Cryptogr Eng (2023). **(Science Citation Index Expanded)** https://doi.org/10.1007/s13389-023-00336-y

5. (with J Varghese, K Praveen, S Dutta), A novel approach for long-term secure storage of domain independent videos, Journal of Visual Communication and Image Representation Volume 104 , October 2024, 104279, **(Science Citation Index Expanded),** https://www.sciencedirect.com/science/article/abs/pii/S1047320324002359

6. (with Chandan Goswami, Avishek Adhikari, Suraj Kumar Sahoo, Pinaki Sarkar), Authenticated key agreement for IoT network using HECC and CRT four co-primes, **Peer-to-Peer Netw. Appl.** 17, 2397–2414 (2024). https://doi.org/10.1007/s12083-024-01699-7 **(Science Citation Index Expanded)**

7. (with Md Kutubuddin Sardar and Jyotirmoy Pramanik), (t,k,n) Regional Secret Image Sharing over Finite Fields, Signal Processing, Volume 210, **September 2023,** 109082, **Elsevier Journal, (Science Citation Index).** https://doi.org/10.1016/j.sigpro.2023.109082
8. (with K, P., Dutta, S., Sethumadhavan M.) Proactive visual cryptographic schemes for general access structures. Multimedia Tools Appl **(2023), Springer, (Science Citation Index Expanded)**. https://doi.org/10.1007/s11042-023-14998-7.
9. (with Subarsha Banerjee), On spectra of power graphs of finite cyclic & dihedral groups, **Rocky Mountain Journal of Mathematics**, 53 (2), 341-356, **2023 (Science Citation Index Expanded).**
10. (with P Sarkar, SK Sahoo, C Goswami), Connectivity invariant lightweight resiliency improvement strategies for CRT-subset scheme, to appear in Ad Hoc Networks, **Elsevier Journal,** 2022, **(Science Citation Index**)
11. (with S K Sahoo and S Dutta), Practical attacks on a class of secret image sharing schemes based on Chinese Remainder Theorem, Computers and Electrical Engineering **Elsevier Journal,** Volume 100, May 2022, 107924, **(Science Citation Index).**

12. (with Subarsha Banerjee), On spectra and spectral radius of Signless Laplacian of power graphs of some finite groups, **Asian-European Journal of Mathematics,** Vol. 14, No. 06, 2150090 (2021), **(Emerging Sources Citation Index)**
13. (with Md Kutubuddin Sardar), Essential secret image sharing scheme with small and equal sized shadows, Signal Processing, : Image Communication**, Elsevier Journal,** 2020, 87, 115923, **(Science Citation Index)**
14. (with Md Kutubuddin Sardar), A New Lossless Secret Color Image Sharing Scheme with Small Shadow Size, Journal of Visual Communication and Image Representation, **Elsevier Journal,** 2020. **(Science Citation Index Expanded)**
15. (with Subarsha Banerjee), Signless Laplacian spectrum of power graphs of finite cyclic groups, to appear in **AKCE International Journal of Graphs and Combinatorics, Elsevier Journal,** 2020. **(Emerging Sources Citation Index)**
16. (with Sabyasachi Dutta and Sushmita Ruj), Maximal contrast color visual secret sharing schemes, to appear in **Designs, Codes and Cryptography, Springer Journal. (Science Citation Index Expanded)**
17. (With Prakash Dey and Raghvendra Singh Rohit), Single Key MITM Attack and Biclique Cryptanalysis of Full Round Khudra, J**ournal of Information Security and Applications, Elsevier Journal, Vol 41, pp. 117-123, August 2018. (Science Citation Index Expanded)**
18. (With Ushnish Sarkar), On relationship between Hamiltonian path and holes in L(3,2,1)-coloring of minimum span, **Discrete Applied Mathematics, Elsevier Journal**, Volume 222 Issue C, May 2017, pp. 227-234. **(Science Citation Index Expanded)**
19. (with Sabyasachi Dutta and Raghvendra Singh Rohit), Constructions and Analysis of Some Efficient t-$(k,n)^*$-Visual Cryptographic Schemes Using Linear Algebraic Techniques, **Design, Codes and Cryptography, Springer Journal**, 80(1):165-196(2016),DOI 10.1007/s10623-015-0075-5. **(Science Citation Index Expanded)**
20. (with Santanu Sarkar, Prakash Dey and Subhamoy Maitra), Probabilistic signature based generalized framework for differential fault analysis of stream ciphers, **Cryptography and Communications, Springer Journal**, July 2017, Volume 9, Issue 4, pp 523-543. **(Science Citation Index Expanded)**
21. (with Prakash Dey and Raghvendra Singh Rohit), Full key recovery of ACORN with a single fault, **Journal of Information Security and Applications, Elsevier Journal,** Volume 29, August 2016, Pages 57-64. **(Science Citation Index Expanded)**
22. (With Ushnish Sarkar), A new graph parameter and a construction of larger graph without increasing radio k-chromatic number, **Journal of Combinatorial Optimization, Springer Journal**, Volume 33 Issue 4, May 2017, pp 1365-1377. **(Science Citation Index Expanded)**
23. (with Rita SahaRay), Structural form of a minimal critical set for a latin square representing the elementary abelian 2-group of order 8, **Ars Combinatoria**, 120, 181-191, 2015. **(Science Citation Index Expanded)**
24. (With Ushnish Sarkar), On characterizing radio k-coloring problem by path covering problem, **Discrete Mathematics, Elsevier Journal,** 338 (2015), pp. 615-620, DOI information: 10.1016/j.disc.2014.11.014. **(Science Citation Index Expanded)**
25. (with Angsuman Das and Kouichi Sakurai), Plaintext Checkable Encryption with Designated Checker, **Journal of Advances in Mathematics of Communications,** Volume 9, No. 1, 2015, 37-53, doi:10.3934/amc.2015.9.37. **(Science Citation Index Expanded)**
26. (**single author**), Linear algebraic techniques to construct monochrome visual cryptographic schemes for general access structure and its applications to color images, **Design, Codes and Cryptography, Springer Journal,** December 2014,

Volume 73, Issue 3, pp 865-895, DOI 10.1007/s10623-013-9832-5. **(Science Citation Index Expanded)**

27. (with Partha Sarathi Roy), One-Sided Leakage-Resilient Privacy Only Two-Message Oblivious Transfer, **Journal of Information Security and Applications, Elsevier Journal,** Volume 19, Issues 4-5, November 2014, Pages 295-300. **(Science Citation Index Expanded)**
28. (with Mrinal Nandi and Subrata Parui), Bounds on the Size of the Minimum Dominating Sets of Some Cylindrical Grid Graphs**, International Journal of Combinatorics,** Volume 2014, Article ID 348359, 13 pages, http://dx.doi.org/10.1155/2014/348359.
29. (with Angsuman Das), A note on "On ciphertext undetectability", **Tatra Mountains Mathematical Publications.** Vol. 57, no. 4 (2013), p. 119-121.
30. (with Dong Hao, Xiaojuan Liao, Kouichi Sakurai and Makoto Yokoo), A repeated game approach for analyzing the collusion on selective forwarding in multi hop wireless networks, **Computer Communications, Elsevier Journal,** Volume 35, Issue 17, 1 October 2012, Pages 2125-2137. **(Science Citation Index Expanded)**
31. (with Angsuman Das), An efficient IND-CCA2 secure Paillier-based cryptosystem, **Information Processing Letters, Elsevier Journal,** Volume 112, Issue 22, 30 November 2012, Pages 885-888, http://dx.doi.org/10.1016/j.ipl.2012.08.007. **(Science Citation Index Expanded)**
32. (with Liang Zhao, Di Xiao and Kouichi Sakurai), On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption , **Communications in Nonlinear Science and Numerical Simulation, Elsevier Journal,** http://dx.doi.org/10.1016/j.cnsns.2011.12.015. Volume 17, Issue 8, August 2012, Pages 3303-3327. **(Science Citation Index Expanded)**
33. (with Mrinal Nandi and Subrata Parui), Domination Number of Cylindrical Grids, **Applied Mathematics and Computation, Elsevier Journal,** Volume 217, Issue 10, 15 January 2011, Pages 4879-4889. **(Science Citation Index Expanded)**
34. (with ParthaSarathi Roy), Multi-Use Multi-Secret Sharing Scheme for General Access Structure, Annals of the University of Craiova, Mathematics and Computer Science Series Volume 37(4), 2010, Pages 50-57, ISSN: 1223-6934. **(Emerging Sources Citation Index)**
35. (with Angsuman Das), An efficient multi-use multi-secret sharing scheme based on hash function, **Applied Mathematics Letters, Elsevier Journal,** Volume 23, Issue 9, September 2010, Pages 993-996. **(Science Citation Index Expanded)**
36. (with Chitradeep Dutta Roy, Neel Choudhury, Amrik Chatterjee (during their summer training in 2009)), Verifiable Secret Sharing Scheme on Images using Watermarking , **International Journal of Computer Science and Network Security,** VOL.10 No.2, page 76-81, February 2010. **(Emerging Sources Citation Index)**
37. (with M Bose and Bimal Roy), Applications of Partially Balanced and Balanced Incomplete Block Designs in developing Visual Cryptographic Schemes, **IEICE TRANS. FUNDAMENTALS, Japan,** Vol. E-90A, No. 5, pp. 949-951, May 2007. **(Science Citation Index Expanded)**
38. (Single Author), An overview of black and white Visual Cryptography using mathematics, **J. Calcutta Math. Soc.** 2 (2006), no. 2, 21-52.
39. (with M R Adhikar and Shibopriya Mitra), A generalization of Milnors result, **J. Calcutta Math. Soc**. 2 (2006), no. 1, 55-58.
40. (with R SahaRay and Jennifer Seberry), Critical Sets in Orthogonal Arrays with 7 and 9 Levels, **The Australasian Journal of Combinatorics**, Volume 33, 2005, pp. 109-123. **(Emerging Sources Citation Index)**
41. (with R SahaRay and Jennifer Seberry), Critical Sets for a Pair of Mutually Orthogonal Cyclic Latin Squares of Odd Order Greater than 9, **The Journal of**

Combinatorial Mathematics and Combinatorial Computing, Vol. 55, 2005, pp. 171-185. (**Emerging Sources Citation Index**)

42. (with P K Rana), A Study of Functors Associated With Topological Groups, **Studia Universitatis Babes-Bolyai Mathematica**, Vol XLVI (4), 3-14, 2001. (**Emerging Sources Citation Index**)

43. (with M Bose), A New Visual cryptographic Scheme Using Latin Squares, **IEICE TRANS. FUNDAMENTALS, Japan**, VOL E87-A, NO.5, MAY 2004, pp. 1198-1202. (**Science Citation Index Expanded**)

b) Conference volumes (IEEE or LNCS by Springer):

1. (with K Praveen, GA KS, IG Ray, A Adhikari, S Datta, AK Biswas), On the Design of a Searchable Encryption Protocol for Keyword Search using Proactive Secret Sharing, 2024 IEEE 20th International Conference on e-Science (e-Science), 1-8. Doi: https://ieeexplore.ieee.org/abstract/document/10678696
2. (with Tewary, A., Mandal, S., Chakrabarti, A., Saha, D), Differential Fault Analysis of Trivium Using Artificial Neural Network on SoC Platform. In Emerging Electronic Devices, Circuits and Systems. **Lecture Notes in Electrical Engineering,** vol 1004. **Springer, 2023,** Singapore. https://doi.org/10.1007/978-981-99-0055-8_22)
3. (with Pramanik J.) Evolving Secret Sharing in Almost Semi-honest Model. In: Stănică P., Mesnager S., Debnath S.K. (eds) Security and Privacy. ICSP 2021. Communications in Computer and Information Science, vol 1497. **Springer,** Cham. https://doi.org/10.1007/978-3-030-90553-8_9, 2021.
4. (with Debnath A.) On Determination of φ−1(2apa1). In: Mishra S.R., Dhamala T.N., Makinde O.D. (eds) Recent Trends in Applied Mathematics. Lecture Notes in Mechanical Engineering. **Springer, Singapore**. https://doi.org/10.1007/978-981-15-9817-3_5, 2021
5. (with Dutta S., Bhore T., Sardar M.K., Sakurai K.) Visual Secret Sharing Scheme with Distributed Levels of Importance of Shadows. In: Giri D., Ho A.T.S., Ponnusamy S., Lo NW. (eds) Proceedings of the Fifth International Conference on Mathematics and Computing. Advances in Intelligent Systems and Computing, vol 1170. 19-32, **Springer, Singapore**, 2021 https://doi.org/10.1007/978-981-15-5411-7_2, 2021.
6. (with Sardar M.K.) (2021) A New Lossless Secret Image Sharing Scheme for Grayscale Images with Small Shadow Size. In: Bhattacharjee D., Kole D.K., Dey N., Basu S., Plewczynski D. (eds) Proceedings of International Conference on Frontiers in Computing and Systems. Advances in Intelligent Systems and Computing, vol 1255. 701-709, **Springer, Singapore**. https://doi.org/10.1007/978-981-15-7834-2_65, 2021.
7. (with Pramanik J.) Evolving Secret Sharing with Essential Participants. In: Bhattacharjee D., Kole D.K., Dey N., Basu S., Plewczynski D. (eds) Proceedings of International Conference on Frontiers in Computing and Systems. Advances in Intelligent Systems and Computing, vol 1255. 691-699, **Springer, Singapore**. https://doi.org/10.1007/978-981-15-7834-2_64, 2021.
8. (with Dutta S., Sardar M.K., Ruj S., Sakurai K.) Color Visual Cryptography Schemes Using Linear Algebraic Techniques over Rings. In: Kanhere S., Patil V.T., Sural S., Gaur M.S. (eds) Information Systems Security. ICISS 2020. **Lecture Notes in Computer Science**, vol 12553, 198-217, **Springer, Cham.** https://doi.org/10.1007/978-3-030-65610-2_13, 2020.

9. (with B C Das and Md Kutubuddin Sardar), Efficient Random Grid Visual Cryptographic Schemes having Essential Members, in the Proceedings of the International Conference of ICSP 2020 to be published by Springer**, 2021**.

10. (With Jyotirmoy Pramanik, Partha Sarathi Roy, Sabyasachi Dutta and Kouichi Sakurai), Secret Sharing Schemes on Compartmental Access Structure in Presence of Cheaters, **Springer LNCS,** ICISS 2018: 171-188.
11. (With Partha Sarathi Roy, Sabyasachi Dutta, Kirill Morozov, Kazuhide Fukushima, Shinsaku Kiyomoto and Kouichi Sakurai), Hierarchical Secret Sharing Schemes Secure against Rushing Adversary: Cheater Identification and Robustness, to appear in **Springer LNCS** of the 14th International Conference on Information Security Practice and Experience (ISPEC 2018) will be held in **Tokyo, Japan,** during September 25-27, 2018.
12. (with Sabyasachi Dutta), Contrast Optimal XOR Based Visual Cryptographic Schemes, Information Theoretic Security - 10th International Conference, ICITS 2017, **Hong Kong, China,** November 29 - December 2, 2017, **Springer LNCS**, 10681, 2017, pp. 58-72.
13. (with Sabyasachi Dutta, Partha Sarathi Roy and Kouichi Sakurai), On the Robustness of Visual Cryptographic Schemes, 15th International Workshop, IWDW 2016, **Beijing, China, September** 17-19, 2016, **Springer LNCS,** volume 10082, pp. 251-262.
14. **(with** Kirill Morozov, Satoshi Obana, ParthaSarathi Roy, Kouichi Sakurai and Rui Xu**),** Efficient Threshold Secret Sharing Schemes Secure against Rushing Cheaters, to appear in the **Lecture Notes in Computer Sciences, Springer,** proceedings of the **9th International Conference on Information Theoretic Security,9-12 August 2016, Tacoma, Washington, USA.**
15. (with Prakash Dey, Raghvendra Singh Rohit, Santanu Sarkar), Differential Fault Analysis on Tiaoxin and AEGIS Family of Ciphers. SSCC 2016, **Springer Communications in Computer and Information Science,** 2016, pp. 74-86.
16. (with Angsuman Das), Plaintext Checkable Signcryption, ICISS 2015, Volume 9478, **Lecture Notes in Computer Sciences, Springer, 2015, pp 324-333**.
17. (with Prakash Dey, Abhishek Chakraborty and Debdeep Mukhopadhyay), Improved Practical Differential Fault Analysis of Grain-128, Proceedings of DATE 2015, available at **IEEE Xplore Digital Library or ACM Digital Library.** This year DATE 2015 received 1129 submissions, of which 915 went into the review process (214 were automatically rejected before review for various reasons). Out of the 915 reviewed submissions, 205 papers (= 22.4%) were selected for either "long" or "short" presentation at the conference. Our paper is accepted for "long" presentation at the conference.
18. (with Prakash Dey), Improved Multi-Bit Differential Fault Analysis of Trivium, Progress in Cryptology, INDOCRYPT 2014, **Lecture Notes in Computer Science, Springer, 2014, pp 37-52.**
19. (with ParthaSarathi Roy, Rui Xu, Kirill Morozov and Kouichi Sakurai), An Efficient Robust Secret Sharing Scheme with Optimal Cheater Resiliency,(Space 2014), **Lecture Notes in Computer Sciences, Springer,** Volume 8804, 2014, pp 47-58.
20. (with Sabyasachi Dutta), XOR Based Non-monotone t-$(k,n)^*$-Visual Cryptographic Schemes Using Linear Algebra,(ICICS 2014), **Lecture Notes in Computer Sciences, Springer,** Volume 8958, pp 230-242.
21. (with Angsuman Das and ParthaSarathi Roy), Computationally Secure Robust Multi-Secret Sharing for General Access Structure,(ICMC 2015), Mathematics and Computing, Volume 139 of the series **Springer Proceedings in Mathematics & Statistics,**pp 123-134, 2015.

22. (with ParthaSarathi Roy and Angsuman Das), Computationally Secure Cheating Identifiable Multi-Secret Sharing for General Access Structure,(ICDCIT-2015), in **Lecture Notes in Computer Sciences, Springer,** Volume 8956, pp 278-287, 2015.
23. (withAngsuman Das), Signcryption with Delayed Identification, Proceedings of the International Conference on Mathematics and Computing - 2013, **Springer Mathematics and Statistics Series,** Volume 91, 2014, pp 23-39.
24. (with Angsuman Das), Signcryption from Randomness Recoverable PKE Revisited, to appear in the Proceedings of the 9th International Conference on Information Systems Security (ICISS 13), **Lecture Notes in Computer Science series, Springer,** Volume 8303, pp 78-90.
25. (with Angsuman Das and Sabyasachi Dutta), Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture, The Complete Picture, Proceedings of the Seventh International Conference on Provable Security (ProvSec 2013), Melaka, Malaysia,**Lecture Notes in Computer Science series, Springer, Volume 8209,** pp 104-120.
26. (with Liang Zhao, Takashi Nishide, Kyung-Hyune Rhee and Kouichi Sakurai), Cryptanalysis of Randomized Arithmetic Codes Based on Markov Model , Proceeding of The 7th International Conference, INSCRYPT 2011, November 30-December 3, 2011, Beijing, China,**Lecture Notes in Computer Science series, Springer,** Volume 7537, pp 341-362.
27. (with Dong Hao and Kouichi Sakurai), Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks , Proceeding of The Third International Conference on Trusted Systems, INTRUST 2011, November 27-29, 2011, Beijing, China, **Lecture Notes in Computer Science series, Springer,** pp 239-257.
28. (with Liang Zhao, Di Xiao and Kouichi Sakurai), Security Improvement of a Pixel Bit Based Image Scrambling Encryption Scheme Through the Self-correlation Method. (INSCRYPT 2010 (short paper), Shanghai, China, October 20 to 23, 2010)
29. (with Liang Zhao and Kouichi Sakurai), A New Scrambling Evaluation Scheme based on Spatial Distribution Entropy and Centroid Difference of Bit-plane. (IWDW 2010, 1~3 October 2010, Korea University, Seoul, Republic of Korea), Digital Watermarking, **Lecture Notes in Computer Science, Springer,** 2011, Volume 6526/2011, 29-44, DOI: 10.1007/978-3-642-18405-5_4.
30. (with Liang Zhao, Di Xiao, and Kouichi Sakurai), Cryptanalysis on an Image Scrambling Encryption Scheme Based on Pixel Bit. (IWDW 2010, 1~3 October 2010, Korea University, Seoul, Republic of Korea), Digital Watermarking, **Lecture Notes in Computer Science, Springer,** 2011, Volume 6526/2011, 45-59, DOI: 10.1007/978-3-642-18405-5_5.
31. (with Bimal Roy), On some constructions of monochrome visual cryptographic schemes , Page(s): 1-6, Digital Object Identifier 10.1109/INFTECH.2008.4621609, appeared in the **IEEE Conference Proceedings,** 1st International Conference on Information Technology, Faculty of Electronics, Telecommunications and Informatics Gdansk University of Technology, Poland, May 18-21, 2008.
32. (Single Author) DNA Secret Sharing, **IEEE World Congress on Computational Intelligence,** Vancouver, Canada, July 16-21, 2006.
33. (with Tridib Kumar Dutta and Bimal Roy), A New Black and White Visual Cryptographic Scheme for General Access Structures, **Lecture Notes In Computer Science, Vol 3348, Springer-Verlag,** 399-413, 2004.
34. (with Somnath Sikdar), A New (2,n)-Color Visual Threshold Scheme for Color Images, **Lecture Notes In Computer Science, Vol 2904, Springer-Verlag,** 148-161, 2003.

c) Other publications:

1. **Volume Editor:**
   a. **Proceedings of IMBIC, Volume 8, ISBN 978-81-925832-7-3.**
   b. **Proceedings of IMBIC, Volume 7, ISBN 978-81-925832-6-6.**
   c. **Proceedings of IMBIC, Volume 6, ISBN 978-81-925832-5-9.**
   d. **Proceedings of IMBIC, Volume 5, ISBN 978-81-925832-4-2.**
   e. **Proceedings of IMBIC, Volume 4, ISBN 978-81-925832-3-5.**
   f. **Proceedings of IMBIC, Volume 3, ISBN 978-81-925832-2-8.**
   g. **Proceedings of IMBIC, Volume 2, ISBN: 978-81-925832-1-1.**
   h. **Proceedings of IMBIC, Volume 1, ISBN: 978-81-925832-0-4.**

11. Patents:

Patent application has been filed in 2024 with Indian Patent Office in collaboration with DRDO and University of Calcutta. Patent application No. 202411033941. Patent applied for "Apparatus and method for identification of cryptographic algorithm".

12. Membership of Learned Societies:

1. **Indian Science Congress Association (Life Member)**
2. **Calcutta Mathematical Society (Life Member)**
3. **Founder Secretary and Life Member of Institute for Mathematics, Bioinformatics, Information Technology and Computer Science (IMBIC), Branches: Japan, Sweden**
4. **Cryptology Research Society of India (Life Member).**

13. Invited lectures delivered:

a. Invited Lectures at Foreign Institutes:

1. Invited talk at **Bauman Moscow State Technical University, Russia** on "Visual Cryptography and DNA Secret Sharing: Two Simple ways to Store Secret Information in a Secure Way" on July 6, 2017.
2. Invited talk at the **University of Nagasaki, Japan** on "India and Indian Mathematics: A Brief Overview" on June 22, 2016.
3. Invited talk at the **Tokyo Institute of Technology, Japan** on "On a Complete Characterization of Optimal XOR Based Visual Cryptographic Schemes for Non-monotone General Access Structures" on June 23, 2016.
4. Invited to **University of Putra Malaysia (UPM), Malaysia** and delivered a talk on "COLOR VISUAL CRYPTOGRAPHIC SCHEMES USING STATISTICAL DESIGNS" on May 28, 2014 at the International Conference and Workshop on Mathematical Analysis 2014 (ICWOMA2014), 27-30 May 2014**), Malaysia**.
5. Invited talk on "Design Theory and Visual Cryptographic Schemes" at Graduate School of Mathematical Sciences, **University of Tokyo, Japan,** during November 3-6, 2013 at the JSPS-DST Asian Academic Seminar, 2013 on Discrete Mathematics & its Applications.
6. Visited University of Kyushu, Japan August 26-30, 2013 as an invited speaker of the International Conference entitled "Algebraic constructions as a fundamental keystone ofa safe and secure society: Mathematics for guaranteeing the reliability of the cyber security"

organized by the **Institute of Mathematics for Industry (IMI), Kyushu University, Japan** during August 26-30, 2013.

The Title of the three invited talks are:

a. Connections among Algebra, Statistical Designs and Secret Sharing Schemes (on August 27, 2013).
b. Applications of Algebraic Structure in Visual Cryptography (on August 28, 2013).
c. Plaintext Checkable Encryption with Designated Checker (on August 29, 2013).

7. Invited talk on Applications of Mathematics, Statistics in DNA Micro Array and Secret Sharing Schemes **at Meijo University, Japan** on June 4, 2012.

8. Invited talk on A Brief Introduction about Kolkata and University of Calcutta, India at the Department of Computer Science and Communication Engineering, University **of Kyushu, Japan** on June 1, 2012.

9. Invited talk on Color Visual cryptographic Scheme for General Access Structure at the **Department of Computer Science and Communication Engineering,** University of **Kyushu, Japan on** May31, 2012.

10. Invited talk on Some Secret Sharing Schemes and Further Studies at the **Department of Industrial Mathematics, University of Kyushu, Japan** on May 29, 2012.

11. Invited talk on Cryptography: An Art of Secret Writing at the **Department of Computer Science and Communication Engineering, University of Kyushu, Japan** on August 12, 2011.

12. Invited talk on Indian Education System at the **Department of Computer Science and Communication Engineering, University of Kyushu, Japan** on June 29, 2010.

13. Invited talk on Information theoretic discussions on perfectly secure multi-use multi-secret sharing scheme at **KDDI, Japan** on July 7, 2010.

14. Invited talk on Interdisciplinary Secret Sharing Schemes at **Tokyo Institute of Technology, Japan** on July 5, 2010.

15. Invited talk on On DNA Secret Sharing at **Tokyo University, Japan** on July 7, 2010.

16. Invited talk on Constructions of some Multi-Secret Sharing Schemes at the INDO-JAPAN Workshop at **AIST, Japan** on July 7, 2009.

17. Invited talk on DNA secret sharing scheme and two multi-secret multi use secret sharing schemes for general access structure at the **Department of Computer Science and Communication Engineering, University of Kyushu, Japan** on June 5, 2009.

18. Invited talk on Visual cryptographic Scheme: A different type of Secret Sharing Scheme at the **Department of Computer Science and Communication Engineering, University of Kyushu, Japan** on May 27, 2009.

19. Invited talk on "Visual Cryptography and DNA Secret Sharing" at the Recent Advances in Cryptography in **Paris, June** 11-13, 2007 organized by **Indo-French Centre for Promotion of Advanced Research.**

20. Invited talk on "Application of Mathematics in DNA Secret Sharing" at the **University of Rajsahi, Bangladesh** on June 14, 2007.

21. Invited talk on DNA Secret Sharing and its Application to Cryptography at the Conference DNA and its Related Topics, May 19, 2006, organized by **University of Linkoping, Sweden.**

22. Invited talk on Applications of Mathematics in Developing Visual Cryptographic Schemes at the seminar Laprochaine session du sminaire se tiendra le vendredi November 4, 2005, organized **by ENSTA, France**.

23. Invited talk on Application of Mathematics in Cryptography at the conference Mathematics and Its Applications, 2005, June 22, 2005 organized by **University of Karlstad, Sweden.**

b. Selective Invited Lectures at Indian Institutes (Last Updated in 2019):

1. Invited talk at the **13th International Conference of IMBIC** on "Mathematical Sciences for Advancement of Science and Technology" **(MSAST 2019) organized by the Institute for Mathematics, Bioinformatics, Information Technology and Computer Science (IMBIC),** Kolkata on "**Cryptanalysis on Polynomial Based Image Encryption Schemes**" on December 22, 2019.
2. Invited talk on "**Fun with Numbers and Their Applications to Real Life**" at the **Department of Mathematics, Gurudas College** on November 8, 2019.
3. Invited as a Resource Person to deliver Invited Talk on "**Algebra and Its Applications**" (November 28, 2019) at the **Refresher Course for University and College teachers under UGC-HRDC** of Jadavpur University (November 18 – 30, 2019) at the **Department of Mathematics, Jadavpur University.**
4. Invited as a **Resource Person** to deliver Invited Talks on **"A Special Type of Secret Sharing Scheme: Visual Cryptography and Few Related Open Issues"** on September 27, 2019 at the National Workshop on Cryptology (September 19-26, 2019) organized by the **Presidency University, Bangalore.**
5. Invited as a **Resource Person** to deliver Invited Talks on **"Fun with Numbers and Their Applications to Cyber Security"** on September 20, 2019 at the Taki Ramkrishna Mission High School in the Two Day Workshop on Science (September 20-21, 2019) organized by the **VVM in collaboration with Vigyan Prasar, DST, Government of India.**
6. Invited as a **Resource Person** to deliver Invited Talks on:
   (i) "Applications of Groups, Rings, Fields and Number Theory in the Digital World" (August 3, 2019).
   (ii) "Linear Algebraic Aspects of Visual Cryptography: Few Open Issues" (August 4, 2019) at the **Refresheres Course** organized by the **Department of Mathematics, University of North Bengal (August 1-14, 2019).**
7. Invited talk at the **National workshop on "Current state of affairs in cyber security & cryptology"** during September 13-14, 2019 at NIT Durgapur, West Bengal organized by the **Vivekanand Vigyan Mission (VVM) and NIT Durgapur**. Title of the Invited Talk: "Various Aspects of Secret Sharing: Few Open Issues" on September 13, 2019.
8. Invited talk on "Modern Cryptography: Recent Trends and Applications" at the Applied Sciences Departments, DIATM, Durgapur on August 14, 2019.
9. Invited talk at the **2-Day Workshop on Cryptology (July 11-12, 2019)** organized by the **Department of Mathematics, Barasat State University,** in collaboration with **Indian Statistical Institute (ISI, Kolkata). Title of the invited talk: "Concepts of Secret Sharing: An Important Cryptographic Primitive" on June 6, 2019.**
10. Invited as a Recourse Person to deliver Invited Talks on
    (a) "Different Aspects of Secret Sharing: An Important Cryptographic Primitive" **(on July 5, 2019)** &
    (b) "Primality Testing: Dealing with Big Primes" **(on July 6, 2019)** in the **Short Term Course on Introduction to Modern Cryptography (July 1-6, 2019)** organized by the **Department of Mathematics, NIT Jamshedpur.**
11. Invited as a Resource Person to deliver Invited Talks on
    a. Applications of Linear Algebra to Secret Sharing: An Important Branch of Cryptography"
    b. "Applications of Abstract Algebra in Finding Large Prime Numbers" on **June 15, 2019** at the **National Level Workshop on Advanced Mathematics (WAM-2019, June 13-22, 2019)** organized by the **Calcutta Mathematical Society.**

12. Invited talk at the Workshop on “Mathematics and Cryptology” organized by the **East Calcutta Girls’ College** in collaboration with **R C Bose Centre for Cryptology and Security, ISI Kolkata on “Understanding Basic Mathematics towards Learning Cryptography” on April 30, 2019.**
13. Invited talk on “**Internet and Mathematics**” at the Workshop organized by the Department of Mathematics, **Victoria Institution (College)**, Kolkata on March 30, 2019.
14. Invited talk at the Short Term Course on Basic Cryptography and Cryptanalysis organized by the **Department of Mathematics, IIT-KGP** on “Secret Sharing: Visual Cryptography and DNA Secret Sharing” on March 28, 2019.
15. Invited talk at the **12th International Conference of IMBIC** on "Mathematical Sciences for Advancement of Science and Technology" **(MSAST 2018) organized by the Institute for Mathematics, Bioinformatics, Information Technology and Computer Science (IMBIC),** Kolkata on “Introduction to Cryptography and Cryptanalysis: Few Important Issues” on December 22, 2018.
16. Invited as a Resource Person to deliver Invited Series of Lectures on Introduction to Algebra to the **“Balurghat College Mathematics Camp (October 21 to November 10, 2018)”** scheduled during October 21st to October 24, 2018 organized by the **Balurghat College, Dakshin Dinajpur, West Bengal.**
17. Invited talk at the Workshop on “Mathematics-Statistics-Cryptology-Computer Science” organized by the **East Calcutta Girls’ College** in collaboration with **R C Bose Centre for Cryptology and Security, ISI Kolkata on “Understanding Basic Mathematics towards Learning Cryptography” on September 13, 2018.**
18. Invited talk at the **Amity University, Kolkata** on the topic “Secure Digital Communication using Mathematical and Statistical Tools” on September 26, 2018.
19. Invited talk at the Workshop on “Mathematics-Statistics-Cryptology-Computer Science” organized by the **East Calcutta Girls’ College** in collaboration with **R C Bose Centre for Cryptology and Security, ISI Kolkata on “Introduction to Mathematical Cryptology: An Overview” on July 20, 2018.**
20. Invited as an Invited Speaker at the **105th Indian Science Congress in Mathematical Science Section (including Statistics)** held at Imphal, Manipur during March 16-20, 2018 and delivered an invited talk on “Digital Data Security: Mathematical Aspects of Cryptography" on March 18, 2018.
21. Invited as a resource person at the Faculty Development Programme on Cryptography and Networking Security (FDPCNS-2018) organized by the Dept. of Computer Science & Engineering, **Jalpaiguri Govt. Engineering College** and delivered an invited talk on “Secret Sharing Scheme: An Important Primitive for Cryptography" on March 14, 2018.

22. Invited as an invited Speaker at the Annual Seminar Lecture organized by the **Department of Mathematics, Serampore College,** and delivered an invited talk on “Applications of Algebra and Number Theory in Secure Digital Communications" on January 13, 2018.
23. Invited as a resource person at the Two-Day National Seminar on Contemporary Research in Theoretical and Applicable Mathematics organized, held during September 8-9, 2017 organized by the The **Bhawanipur Education Society College** and delivered the invited lecture on Algebraic Aspects of Cryptology and its Application to Modern Cyber Security on September 9, 2017.
24. Invited as a resource person at the “Short Term Course on Fundamental Algorithms: Design and Analysis" organized by the **Department of Mathematics, IIT Kharagpur** and delivered an invited talk on “Cryptographic Algorithms" on February 11, 2017.
25. Invited as a resource person at the Workshop on “Communications and Multimedia Security” organized by the **Department of Computer Science and Engineering of**

IIT(ISM), Dhanbad and delivered an invited lecture on “Visual Cryptography: A Different Secret Sharing Scheme" (on February 10, 2017).

26. Invited as a resource person at the **“TEQIP-II sponsored short term course on "Introduction to Cryptography"** during 27-31 January, 2017 organized by the Department of Mathematics, IIT Kharagpur and delivered two invited talks on January 28, 2017. The title of the talks are:

- ❖ Evaluation of Secret Sharing Schemes.
- ❖ Visual Cryptography: A Different Approach.

27. Invited as a resource person at the Tutorial of the **“Third International Conference on Mathematics and Computing (ICMC 2017)"** during January 17-21, 2017 at Haldia, India organized by the Haldia Institute of Technology, Haldia and delivered an invited lecture on ``Few Aspects of Secret Sharing Schemes" (on January 18, 2017).

28. Delivered a special lecture on “Applications of Mathematics in Securing Digital Data” on 14-12-2016 at the **City College**, Kolkata.

29. Delivered a special lecture on “Securing Digital World Through Mathematics” on 02-12-2016 at the **Bhairab Ganguly College**, Kolkata

30. Invited as a resource person at the Faculty Development Programme on “Preparing for Challenges in Higher Education Institutions" during September 23-29, 2016, organized by the **Bhawanipur Education Society College** and delivered an invited lecture on “Cryptology and Reading Numerical Codes" (on September 28, 2016).

31. Invited as a resource person at the UGC-Sponsored Seminar on “Basic Mathematics and its Applications" organised by **RKMVC College, Rahara,** Kolkata on September 21, 2016 and delivered an invited lecture on “Applications of Groups, Rings, Fields and Linear Algebra in Digital World" (on September 21, 2016).

32. Three invited lectures under UGC-SAP (DRS-II) at the Department of **Mathematics and Statistics, University of Himachal Pradesh, Himachal**. The Title of the talks are as follows:

a. Symmetric and Asymmetric Key Cryptography. (on May 28, 2016)
b. Applications of Cryptography. (on June 3, 2016)
c. Visual Cryptography.(on June 4, 2016)

33. Invited talk on “Algebraic Aspects of A Special Type of Secret Sharing Scheme: Visual Cryptography” at the **Department of Mathematics, Shiv Nadar University, Uttar Pradesh,** on May 26, 2016.

34. Invited talk on “Linear Algebraic Aspects of Visual Cryptography: Few Open Issues" at the **Department of Mathematics, Cochin University of Science and Technology, Kochi, Kerala** on March 15, 2016.

35. Invited talk on “Future Prospects in Mathematics after UG and PG Courses in India and Foreign Countries" organized by the Career and Counseling Cell of **Barasat Govt. College, West Bangal,** on February 2, 2016.

36. Two invited talks on ``Number theory and Algebra" at **Lady Brabourne College,** West Bangal, on October 23 and 30, 2015.

37. Invited talk on “Applications of Groups, Rings and Fields in the Digital World Through Cryptography" at the UGC Sponsored National Seminar on Recent Trends on Pure and Applied Mathematics, August 14, 2015, organized by the **Uluberia College, West Bangal.**

38. Invited as a resource person to the National Workshop on Cryptology 2014, during September25-27, 2014, organized by **PDPM IIITDM Jabalpur** and delivered the invited talk "OR-Based Monotone and XOR-Based Non-Monotone Visual" on September 25, 2014.

39. Invited as a resource person to the short term course entitled "A Short Term Course on Cryptography" from 18th May, 2014 to 24th May, 2014 organized by the **Department of Mathematics, IIT Kharagpur** and delivered the following two invited talks on

   a. Introduction to Secret Sharing.
   b. Visual Cryptography and DNA Secret Sharing.

40. Invited as a resource person to the workshop entitled "Instructional Workshop On Graph Theory And Its Applications To Visual Cryptography", during March 10-15, 2014, organized by the **National Centre for Advanced Research in Discrete Mathematics (n-CARDMATH), Kalasalingam University, Madurai** and delivered the followingfour invited talks on

   a. Introduction to Visual Cryptography: A Very Different Cryptographic Scheme. (on March10, 2014)
   b. Mathematical and Statistical Tools to Study (2,n)-VCS (on March 10, 2014)
   c. Cumulative Array and Linear Algebraic Techniques to Construct VCS for General AccessStructure. (on March 11, 2014)
   d. Color VCS and Future Direction of Research. (on March 11, 2014)

41. Invited as a resource person to annual Program entitled "Analytica 2013", on September 25, 2013,organized **by St Xavier's College, Kolkata** delivered the invited talk on "Introduction to AlgebraicCryptography".

42. Invited talk on "An Introduction to Mathematical Cryptography at the Department of Mathematics", **at Lady Brabourne College, Kolkata** on May 17, 2012.

43. Invited talk on "Some Secret Sharing Schemes With Emphasis on Visual Cryptography" at the Seminar on Cryptography organized by the **Barasat State University,** on September 30, 2011.

44. Invited talk on "Some Secret Sharing Schemes and Further Studies" on July 16, 2011 at the Tutorial Workshop on Cryptology, July 16-17, 2011, organized by University of Calcutta and **COEC,ISI Kolkata**.

45. Invited as a resource person to deliver an invited talk on "Cryptography is the science of analyzing and deciphering codes, ciphers and cryptograms" at the Engineer, Golden Jubilee Edition Technical Symposium of **NITK Surathkal,** during 29 October to 1 November 2009.

46. Invited as a resource person to deliver an invited talk on "Introduction to Secret Sharing and Some Interesting Secret Sharing Schemes" at the CRSI-IMSc Joint Workshop on Teaching Cryptology at Undergraduate level during June 15-19, 2009 at the **Indian Statistical Institute, Kolkata.**

47. Invited talk on "Changing Faces of Terrorism and Importance of Cryptography" on the occasion of the Celebration of National Science Day, February 28, 2009, organized by **Indian Science Congress Association.**

48. Invited as a resource person to deliver an invited talk on "Visual and DNA cryptography" at the Workshop on Cryptography, December 5-6, 2008, organized by **Institute of Mathematics and Applications, Bhubaneswar**.

49. Invited as a resource person to deliver an invited talk on "Changing Faces of Terrorism and Secret Message Transmission" at the UGC sponsored Seminar on Changing Faces of Terrorism, a 21stCentury Perspective, organized by **Gokhale Memorial Girls College, Kolkata.**

12.Awards:

1. **"Young Scientist Award" Recipient in Mathematical Science Section (including Statistics)** for the year 2007-08, awarded by **Indian Science Congress Association**.
2. **"President of India Medal for General Proficiency, 2002",** awarded by University of Calcutta.
3. **"Dr B B Datta Memorial Scholarship" in recognition of securing highest marks in the B.Sc (Maths Hons)** of **1999 amongst the prosecuting students of PG Course in Pure Mathematics from University of Calcutta.**
4. **Recipient of the "NANUM 2014" travel grant to Seoul ICM 2014, Korea.**
5. **National Scholarship, Govt of India for Secondary, Higher Secondary and BSc.**
6. **Gold Medalist, 1st Class 1st in MSc, Calcutta University.**
7. **Awarded numerous medals in Sports and Paintings in different competitions organized by school, institute and some organizations.**

13.Other notable activities:

	Founder Secretary of the International Institute IMBIC, having branches in Japan and Sweden
	Former Treasurer of Cryptology Research Society of India (2008-2024)
	Former members of the NBHM regional library committee (Eastern Region).
	Worked as the Easter Zonal coordinator for NBHM, Department of Atomic Energy, Government of India, for MSc and PhD Scholarship Examinations
	Worked as the Managing Editor of the Journal of Pure Mathematics, University of Calcutta.
	Visited Japan (7 times), UK (3 times), Sweden (3 times), Switzerland (2 times), France (2 times), Belgium, Holland, Norway, Denmark, Italy, Korea, Malaysia (2 times), Singapore, Bangladesh, Bhutan, Russia, Thailand.
	Volume Editor of all the 18 Proceedings of the International Conferences MSAST 2007-2024.
	Convener of the Annual Event of the International Conference MSAST organized by the International Institute for Mathematics, Bioinformatics, Information Technology and Computer Science, with branches in Japan and Sweden.
	Worked as a paper setter, moderator, examiner of different examinations organized by different Universities and Institutes.
	Worked as Thesis Reviewer of PhD Thesis of different Universities, IITs and ISI
	Worked as an external expert member of the PhD Entrance/Thesis Viva organized by different Universities, Institutes like Indian Statistical Institute, IITs, IIEST etc.
	Worked as reviewers of leading journals such as AMS Mathscinet, Discrete Mathematics, Discrete Applied Mathematics, Design Codes and Cryptography, IEEE journals, IEICE, many other Springer and Elsevier Journals etc
	Worked as external Committee member of interview for the recruitment of Project Linked personnel at Indian Statistical Institute.
	Worked as External Member for the M.Tech (CS) and M.Math Dissertation of Indian Statistical Institute.

	Former/current Member of Board of Studies of Mathematics: 1. St Xaviers' College, 2. Ramakrishna Mission Vivekananda Centenary College (UG & PG unit), 3. Adamas University (former), 4. Dumdum Motijheel College (PG Unit), 5. APC College, New Barrackpore (PG Unit) (former), 6. Sister Nivedita University
	Program Chair, 22nd International Conference on Cryptology in India, Jaipur, India, December 12–15, 2021 and Volume Editor of the Springer Proceedings "Progress in Cryptology – INDOCRYPT 2021" with Ralf Küsters (Germany) and Bart Preneel **(Belgium)**
	Chairman: Vetting Committee for the purpose of vetting of various Cyber Security courses under CDP program of CCPTR of MAKAUT (Vide letter No. MAKAUT-WB-Regis./IT.WB/013/2021-22 dated 25.10.2021) constituted by **Cyber Security Centre of Excellence, Govt. of West Bengal**
	Chairman: PhD Committee of the Department of Mathematics, Presidency University (since 2019), Chairman: PhD Committee of the Department of Statistics, Presidency University (since 2019), External Member of the PhD Committee of the Department of Pure Mathematics, University of Calcutta (since 2019)